IBM System/36

System Security Guide

IBM System/36

System Security Guide

Program Numbers: 5727-SS1
5727-SS6

File Number
S36-36

Order Number
SC21-9042-4

| **Fifth Edition (October 1986)**

| This major revision makes obsolete SC21-9042-3. See "About This Manual" for a summary of major changes to this edition. Changes or additions to the text are indicated by a vertical line to the left of the change or addition.

| This edition applies to Release 5, Modification Level 0, of IBM System/36 System Support Program Products (Program 5727-SS1 for the 5360 and 5362 System Units, and Program 5727-SS6 for the 5364 System Unit), and to all subsequent releases and modifications until otherwise indicated.

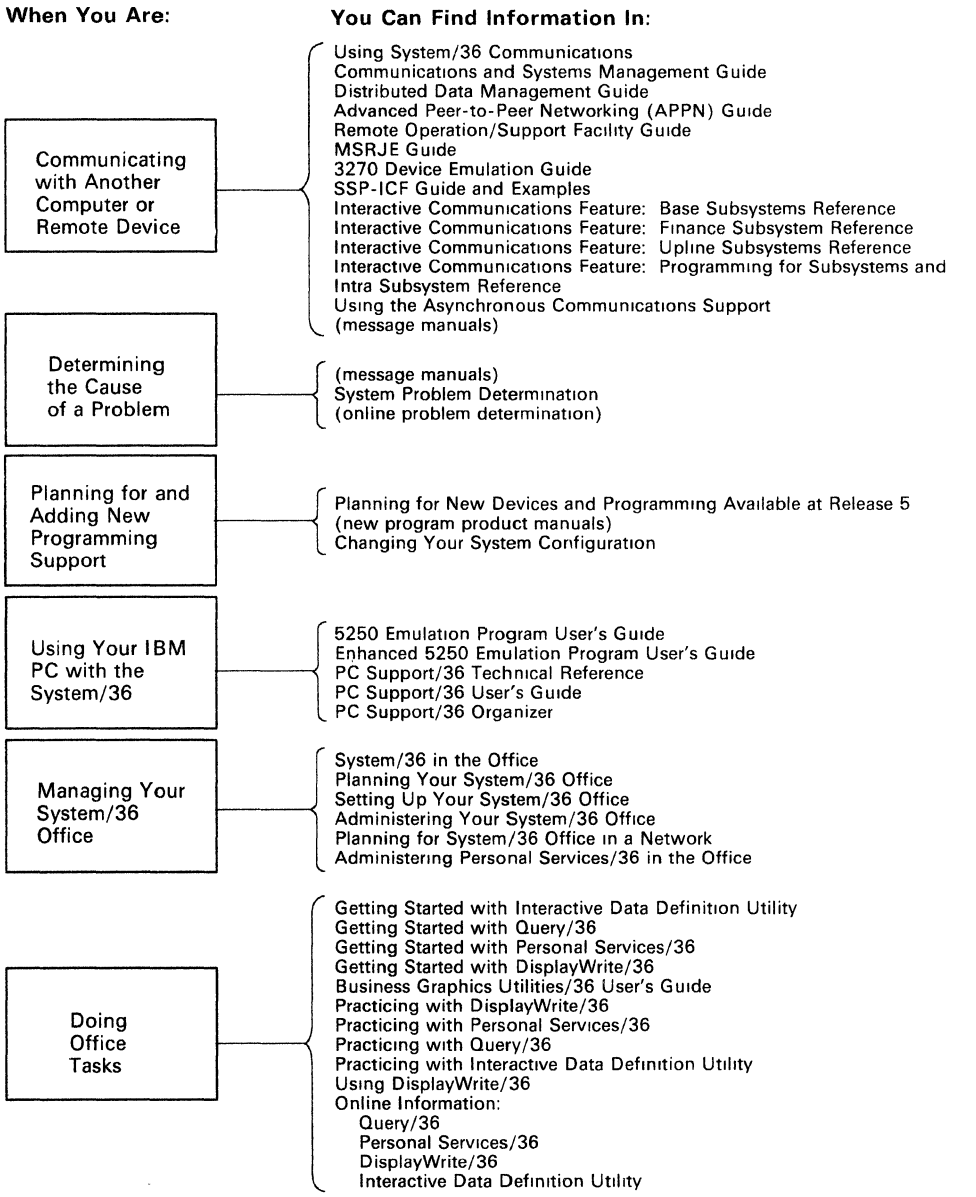
This publication contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

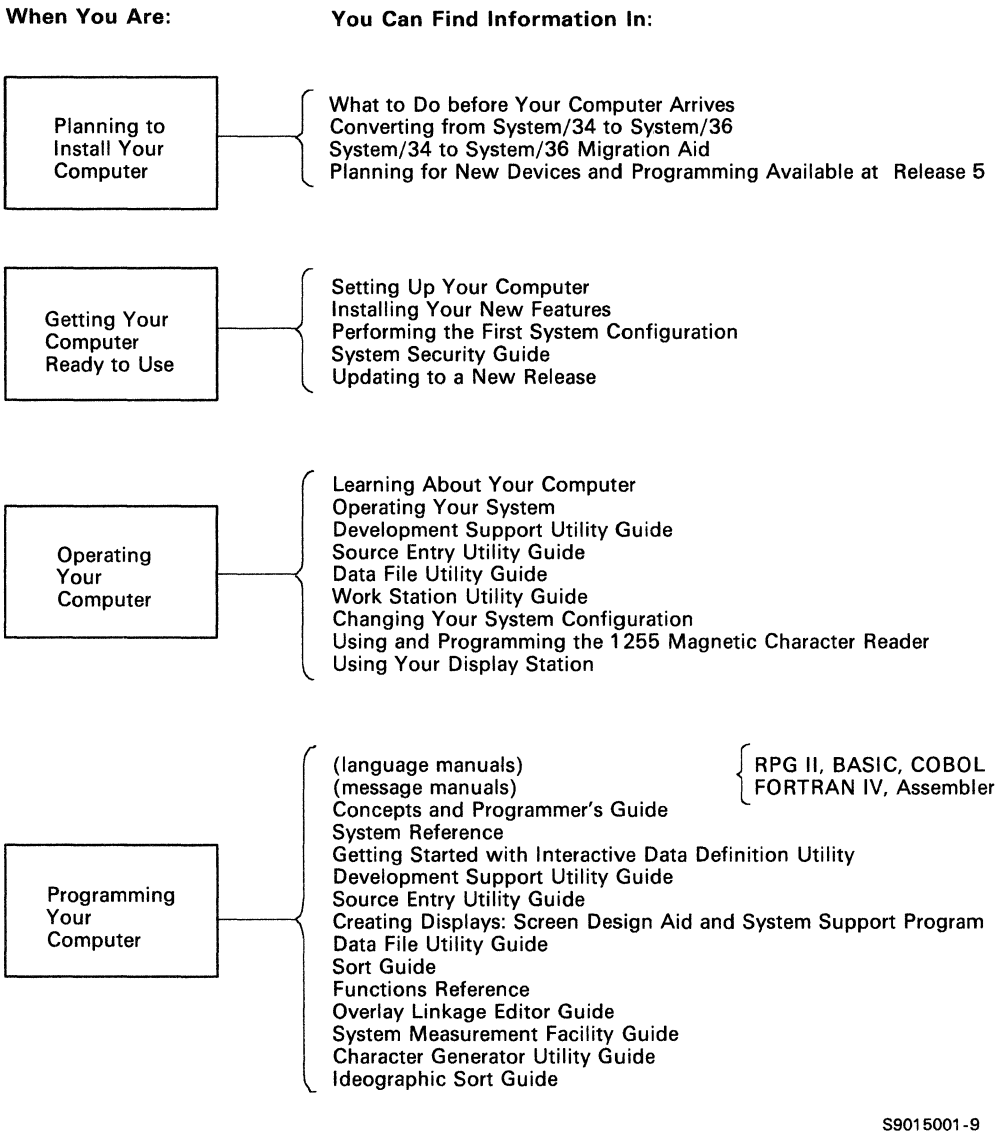
References in this publication to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM licensed program in this publication is not intended to state or imply that only IBM's licensed program may be used. Any functionally equivalent program may be used instead.

The numbers at the bottom right of illustrations are publishing control numbers and are not part of the technical content of this manual.

Publications are not stocked at the address given below. Requests for IBM publications should be made to your IBM representative or to your IBM-approved remarketer.

This publication could contain technical inaccuracies or typographical errors. A form for readers' comments is provided at the back of this publication. If the form has been removed, comments may be addressed to IBM Corporation, Information Development, Department 245, Rochester, Minnesota, U.S.A. 55901. IBM may use or distribute whatever information you supply in any way it believes appropriate without incurring any obligation to you.


When You Are:
You Can Find Information In:
Communicating with Another Computer or Remote Device
Using System/36 Communications
Communications and Systems Management Guide
Distributed Data Management Guide
Advanced Peer-to-Peer Networking (APPN) Guide
Remote Operation/Support Facility Guide
MSRJE Guide
3270 Device Emulation Guide
SSP-ICF Guide and Examples
Interactive Communications Feature: Base Subsystems Reference
Interactive Communications Feature: Finance Subsystem Reference
Interactive Communications Feature: Upline Subsystems Reference
Interactive Communications Feature: Programming for Subsystems and Intra Subsystem Reference
Using the Asynchronous Communications Support
(message manuals)
Determining the Cause of a Problem
(message manuals)
System Problem Determination
(online problem determination)
Planning for and Adding New Programming Support
Planning for New Devices and Programming Available at Release 5
(new program product manuals)
Changing Your System Configuration
Using Your IBM PC with the System/36
5250 Emulation Program User's Guide
Enhanced 5250 Emulation Program User's Guide
PC Support/36 Technical Reference
PC Support/36 User's Guide
PC Support/36 Organizer
Managing Your System/36 Office
System/36 in the Office
Planning Your System/36 Office
Setting Up Your System/36 Office
Administering Your System/36 Office
Planning for System/36 Office in a Network
Administering Personal Services/36 in the Office
Doing Office Tasks
Getting Started with Interactive Data Definition Utility
Getting Started with Query/36
Getting Started with Personal Services/36
Getting Started with DisplayWrite/36
Business Graphics Utilities/36 User's Guide
Practicing with DisplayWrite/36
Practicing with Personal Services/36
Practicing with Query/36
Practicing with Interactive Data Definition Utility
Using DisplayWrite/36
Online Information:
Query/36
Personal Services/36
DisplayWrite/36
Interactive Data Definition Utility
S9015015-9


When You Are:
You Can Find Information In:
Planning to Install Your Computer
What to Do before Your Computer Arrives
Converting from System/34 to System/36
System/34 to System/36 Migration Aid
Planning for New Devices and Programming Available at Release 5
Getting Your Computer Ready to Use
Setting Up Your Computer
Installing Your New Features
Performing the First System Configuration
System Security Guide
Updating to a New Release
Operating Your Computer
Learning About Your Computer
Operating Your System
Development Support Utility Guide
Source Entry Utility Guide
Data File Utility Guide
Work Station Utility Guide
Changing Your System Configuration
Using and Programming the 1255 Magnetic Character Reader
Using Your Display Station
Programming Your Computer
(language manuals)
RPG II, BASIC, COBOL
FORTRAN IV, Assembler
(message manuals)
Concepts and Programmer's Guide
System Reference
Getting Started with Interactive Data Definition Utility
Development Support Utility Guide
Source Entry Utility Guide
Creating Displays: Screen Design Aid and System Support Program
Data File Utility Guide
Sort Guide
Functions Reference
Overlay Linkage Editor Guide
System Measurement Facility Guide
Character Generator Utility Guide
Ideographic Sort Guide
S9015001-9

Contents

About This Manual ix
Who should use this manual . . . ix
How this manual is arranged . . . ix
What you should know . . . x
If you need more information . . . x
How this manual has changed . . . xi

Chapter 1. Introduction to System Security 1-1
Physical Security 1-1
Limit Access to the System Room 1-1
Limit Access to the System Unit 1-2
Securing Diskettes and Tapes 1-3
Data Security 1-3
Password Security 1-4
Menu Security 1-5
Badge Security 1-7
Communications Security 1-9
Resource Security 1-9

Chapter 2. User Identification File 2-1
Introduction 2-1
User Profiles 2-1
Password Security Information 2-2
Badge Security Information 2-5
Location Profiles 2-6
Communications Security Information 2-6
Creating the User Identification File 2-7
Activating Password Security 2-10
Starting the Password Date Checking Function 2-16
Activating Badge Security 2-20
Entering Profiles into the User ID File 2-23
Entering User Profiles 2-23
Entering Location Profiles 2-30
Changing Information in the User ID File 2-34
Changing User Profiles 2-34
If You Are a Master Security Officer or Security Officer 2-35
If You Are a System Console Operator, Subconsole Operator, or Display Station Operator 2-40
Changing Passwords 2-42
Changing Location Profiles 2-44
Listing the User ID File 2-46
Listing User Profiles 2-46
Sample Printout of User Profiles with Passwords Listed 2-49

Sample Printout of User Profiles when Password Security Is Not Active 2-51
Description of User Profile Entries on the User ID File Printouts 2-52
Listing Location Profiles 2-54
Sample Printout of Location Profiles 2-55
Description of Location Profile Entries on User ID File Printout 2-56
Saving the User ID File 2-57
Saving Copies on Diskette 2-57
Example of Copying the User ID File on Diskette 2-59
Saving Copies on Tape or Tape Cartridge 2-60
Example of Copying the User ID File on Tape 2-62
Saving Copies on Disk 2-63
Example of Copying the User ID File to Another Area on Disk 2-63
Restoring the User ID File 2-64
Restoring Copies from Diskette 2-64
Example of Restoring the User ID File from Diskette 2-67
Restoring Copies from Tape or Tape Cartridge 2-68
Example of Restoring the User ID File from Tape 2-72
Restoring Copies from Disk 2-73
Example of Restoring the User ID File from a Disk File 2-74
Changing the Size of the User ID File 2-75
Deactivating Password Security 2-76
Stopping the Password Date Checking Function 2-80
Deactivating Badge Security 2-83
Removing the User ID File from Disk 2-86

Chapter 3. Resource Security File 3-1
Introduction 3-1
Securing Files, Libraries, and Groups 3-1
Access Levels 3-1
Parent and Child Concept 3-3
Special Resource Types 3-6
Securing Folders, Subdirectories, and Folder Members 3-10
Authorization Lists 3-11
Access Levels 3-15
Creating the Resource Security File 3-18
Activating Resource Security 3-22
Entering Information into the Resource Security File 3-26
Entering Information for Files and Libraries 3-26
Entering Information for Authorization Lists, Folders, Subdirectories, and Folder Members 3-32
Creating an Authorization List 3-37
Securing Folders 3-41
Securing a Subdirectory 3-45
Securing Folder Members 3-50
Changing Information in the Resource Security File 3-54
Changing Information for Files, Libraries, and Groups 3-54
Changing Information for Authorization Lists, Folders, Subdirectories, and Folder Members 3-59
Changing an Authorization List 3-60
Changing Folder Security Information 3-65
Changing Subdirectory Security Information 3-70
Changing Folder Member Security Information 3-75
Listing the Resource Security File 3-79

Listing File, Library, and Group Security Information 3-79
Sample Printout of Files, Libraries, and Groups by Resource Name 3-82
Sample Printout of Files, Libraries, and Groups by User ID 3-86
Sample Printout of Files, Libraries, and Groups by Owner ID 3-90
Listing Folder Security Information 3-93
Sample Printout of Folders, Subdirectories, and Authorization Lists by Resource Name 3-96
Sample Printout of Folders, Subdirectories, and Authorization Lists by User ID 3-100
Sample Printout of Folders, Subdirectories, and Authorization Lists by Owner ID 3-103
Saving the Resource Security File 3-106
Saving Copies on Diskette 3-106
Example of Copying the Resource Security File on Diskette 3-109
Saving Copies on Tape or Tape Cartridge 3-109
Example of Copying the Resource Security File on Tape 3-111
Saving Copies on Disk 3-112
Example of Copying the Resource Security File to Another Area on Disk 3-112
Restoring the Resource Security File 3-113
Restoring Copies from Diskette 3-113
Example of Restoring the Resource Security File from Diskette 3-116
Restoring Copies from Tape or Tape Cartridge 3-116
Example of Restoring the Resource Security File from Tape 3-119
Restoring Copies from Disk 3-120
Example of Restoring the Resource Security File from a Disk File 3-121
Changing the Size of the Resource Security File 3-122
Deactivating Resource Security 3-124
Removing the Resource Security File from Disk 3-127

Appendix A. Required Access Levels for Using the System Programming A-1
Access Levels for User Programs A-1
OCL Statements and Procedure Control Expressions A-2
Procedures and Commands A-3

Appendix B. Planning Forms for the Security Files B-1

Appendix C. Converting System/34 Security Files to System/36 Security Files C-1
Using the SECCONV Procedure C-1

Appendix D. Security Procedures D-1
PASSWORD Procedure D-1
SECDEF Procedure (User Identification File) D-2
SECDEF Procedure (Resource Security File) D-3
SECEDIT Procedure D-3
SECLIST Procedure (User Identification File) D-4
SECLIST Procedure (Resource Security File) D-4
SECREST Procedure D-5
SECSAVE Procedure D-5

Appendix E. Generating Random Hexadecimal Location Passwords E-1

Glossary G-1

Index X-1

About This Manual

Who should use this manual . . .

This manual provides information about establishing, activating, and maintaining your system security. The system manager (or someone who is assigned the responsibilities of a master security officer) should read this manual for an introduction to system security, and use it later for detailed reference. If you have read *Planning for System Security*, SA21-9445, which is Workbook 6 of *What to Do Before Your Computer Arrives* (SBOF-4773 for the 5360 System Unit or SBOF-4778 for the 5362 System Unit), you are already familiar with system security and have established a security plan for your system. If so, you can skip certain portions of this manual, but you might like to read those sections for a brief review.

Most of the information in this manual is intended for a master security officer. However, the sections "Changing User Profiles" and "Changing Passwords" are for all users.

This manual will help you use the system security support to:

- Protect your system and your data from being used by people who do not have the proper authorization
- Protect your data from intentional or unintentional damage or destruction
- Keep the information in your security files up to date

How this manual is arranged . . .

Chapter 1 of this manual introduces you to system security. It discusses the system security support you can use to limit access to the system and to your data. Use this chapter to begin planning your system security. Even if you already have a security plan, you might want to review Chapter 1.

Chapter 2 describes the user identification file.

Chapter 3 describes the resource security file.

Appendix A describes the minimum security levels required to run programs and procedures that use secured files and libraries. Use this appendix when you secure the files and libraries that contain your data.

Appendix B contains planning forms you can use to help you prepare your system security.

Appendix C describes the procedure you can use to convert your System/34 security files to System/36 security files if you are converting from System/34 to System/36.

Appendix D contains the security procedures and their parameters. You may want to refer to this appendix once you have become familiar with the security procedures. You can use the security procedures to bypass the system help menus and displays.

Appendix E contains one method of manually generating random hexadecimal passwords for location profiles.

This manual also contains a glossary. Use the glossary to find a definition for a word or term you do not understand.

What you should know . . .

Planning for System Security, SA21-9445, which is Workbook 6 of *What to Do Before Your Computer Arrives* (SBOF-4773 for the 5360 System Unit or SBOF-4778 for the 5362 System Unit), describes how to plan for your system security. You might want to read that manual before reading this one.

If you need more information . . .

If you know how to operate the system, you should be able to use only this manual to prepare, activate, and maintain your system security. However, if you do need additional information, the following system manuals are available:

- *Operating Your System*, SC21-9452 for the 5360 and 5362 System Units, and SC21-9453 for the 5364 System Unit. These manuals contain detailed information about how to operate the system. To activate your system security, it is necessary to perform at least one initial program load (IPL). *Operating Your System* tells you how to perform IPL.

- *Using Your Display Station*, SC21-9455. This manual contains detailed information about how to operate your display station.

- *System Reference*, SC21-9020. This manual contains a description of all the procedures and commands you can use on the system. When you prepare for your system security, you might want to obtain a listing of the files and libraries on your system. *System Reference* tells you how to get such a listing.

How this manual has changed . . .

The following changes were made since the previous edition:

- SECEDIT OFFICE procedure changed to SECEDIT RESFLDR in Chapter 3, "Resource Security File."
- SECLIST OFFICE procedure changed to SECLIST RESFLDR in Chapter 3, "Resource Security File."
- Information on securing paths to subdirectories was added in Chapter 3, "Resource Security File."

Changes made since the previous edition of the manual are indicated by a vertical bar to the left of the change.

Chapter 1. Introduction to System Security

This chapter introduces system security, a part of the System Support Program Product (SSP). System security includes two types of security:

- Physical security
- Data security

If you already have read *Planning for System Security*, which is Workbook 6 of *What to Do Before Your Computer Arrives*, you can skip this chapter. You might, however, want to read it for a quick review.

If you have not read Workbook 6, Chapter 1 can help you learn about the security measures you might consider.

Physical Security

Physical security involves protecting the devices against damage and destruction and protecting the system from being used by people who do not have the proper authorization. The following are a few of the things you might consider when deciding how to physically secure your system.

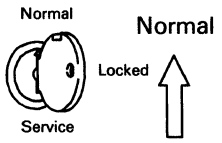
Note: If you have a 3180 Model 2 Display Station attached to your System/36, be advised that it is possible for a user to use record mode to record and play back security information. Be aware that there could be a security exposure if you have a 3180 Model 2 installed in your system configuration.

Limit Access to the System Room

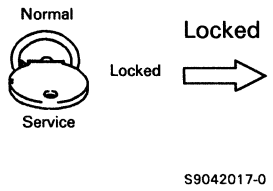
You can limit access to your system by placing it in a special room behind locked doors. This is an effective start at securing your system.

Limit Access to the System Unit

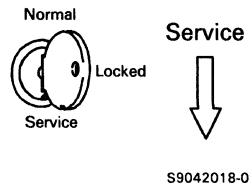
You can limit the use of the entire system by using the keylock feature on the system control panel. The keylock has three positions: Normal, Locked, and Service.



Normal: When the keylock is in the Normal position, the system can be turned on and operated normally. The SSP-provided security functions described later in this manual operate normally. Certain service and diagnostic functions that are performed from the system control panel are not allowed. For example, you cannot use the system control panel to display and alter storage.



Locked: When the keylock is in the Locked position, the system *cannot* be turned on but can be operated normally if it was previously turned on. The SSP-provided security functions, described later in this manual, operate normally. Certain service and diagnostic functions that are performed from the system control panel are not allowed.



Service: When the keylock is in the Service position, the system can be turned on and operated normally. In addition, certain service and diagnostic functions are allowed by anyone with a security classification of system console operator or higher.

When the keylock is in the Service position, *any* operator can use the system control panel to perform some functions that alter or display secured areas of storage, and *any* operator can perform some diagnostic functions that you might not want them to do. Therefore, do not leave the keylock in the Service position. Use the Service position of the keylock *only* when you perform service and diagnostic procedures.

In any of the three positions, the key can be removed from the keylock to keep the keylock in that position.

You can also limit the use of one or more of your display stations with an optional lock. That type of lock prevents the use of a particular display station unless it is unlocked with a key.

Securing Diskettes and Tapes

Information that is stored on diskettes or tapes cannot be secured. Therefore, the diskettes or tapes themselves should be kept in a secure place.

Data Security

Data security helps you prevent unauthorized people from signing on your system and from gaining access to information in the system. The types of data security include:

- Password security
- Menu security
- Badge security
- Communications security
- Resource security

When you put into effect password, menu, badge, or communications security, you enter security information in the user identification file. The user identification file is described in Chapter 2, "User Identification File."

When you put into effect resource security, you enter security information in the resource security file. The resource security file is described in Chapter 3, "Resource Security File."

Password Security

Password security helps prevent an unauthorized person from signing on to the system.

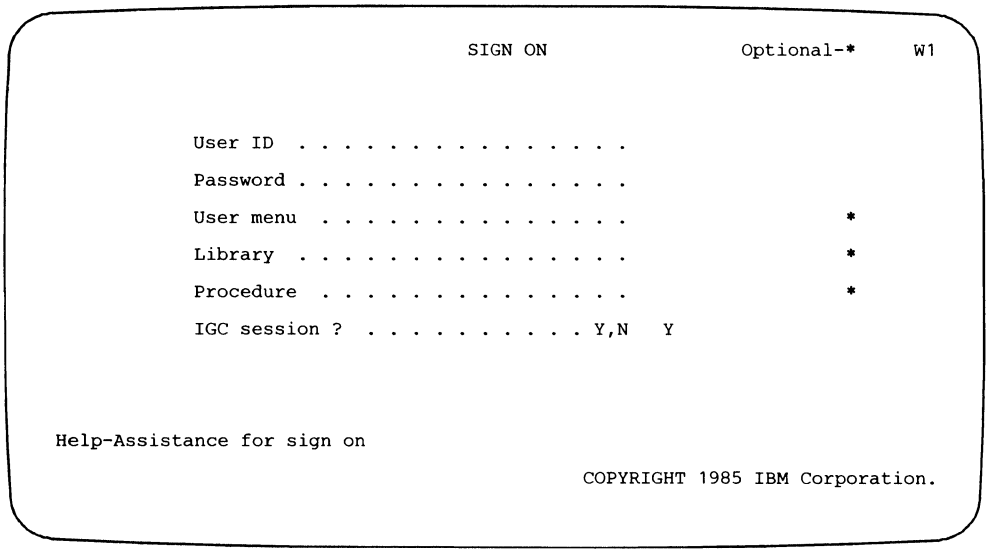
When password security is active (that is, you have specified that password information should be checked and verified), a person must enter a password, in addition to a user ID (user identification), to sign on to the system. If the correct combination of user ID and password is entered on the sign-on display, the person is allowed on the system.

A user ID can be any combination of up to 8 characters; the first character must be 0 through 9, A through Z, #, @, or $. The remaining characters can be any character of the alphabet, any number, or any special character except a comma. Also, the user ID cannot contain any blanks between the characters.

A password must be 4 characters. Any letter of the alphabet, any number, or any special character except a blank can be used.

When password security is not active, anyone can sign on to the system by entering any user ID (such as a name) from 1 to 8 characters.

A sample Sign On display is shown in Figure 1-1.



Notes:

1. *The password prompt appears only if password security is active.*
2. *The IGC session prompt appears only if you have the ideographic version of the SSP.*

Figure 1-1. Sample Sign On Display with Password Security Active

Menu Security

Password security must be active to use menu security.

Menu security allows you to restrict a user to using a single menu or chain of menus. When menu security is in effect, the menu that you specify in the user profile as the mandatory default user menu appears after the user signs on. Unless an option on the mandatory menu causes another option menu, help menu, or help prompt to appear, a user cannot use another menu or the system help.

When menu security is in effect, the user does not have to enter a menu name in the menu field on the Sign On display. Once the default menu is displayed, the user can only:

- Select the options on that menu
- Enter the MSG and OFF control commands

Figure 1-2 (Accounts Receivable and Invoicing: Main Menu) and Figure 1-3 (Accounts Receivable and Invoicing: Transactions Menu) are examples of two menus. Option 1 of the Accounts Receivable Main Menu calls the Accounts Receivable Transactions Menu.

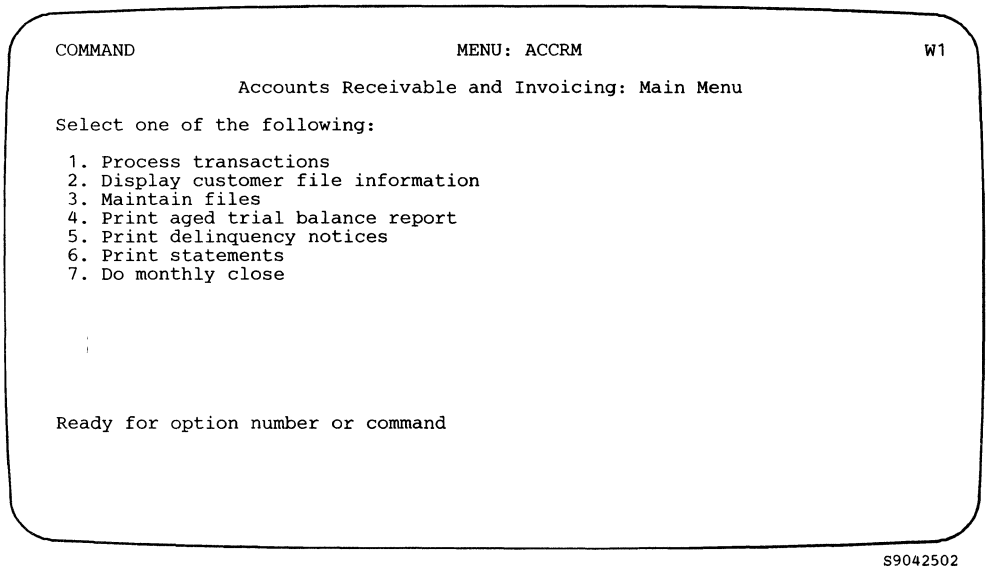


Figure 1-2. Accounts Receivable and Invoicing: Main Menu

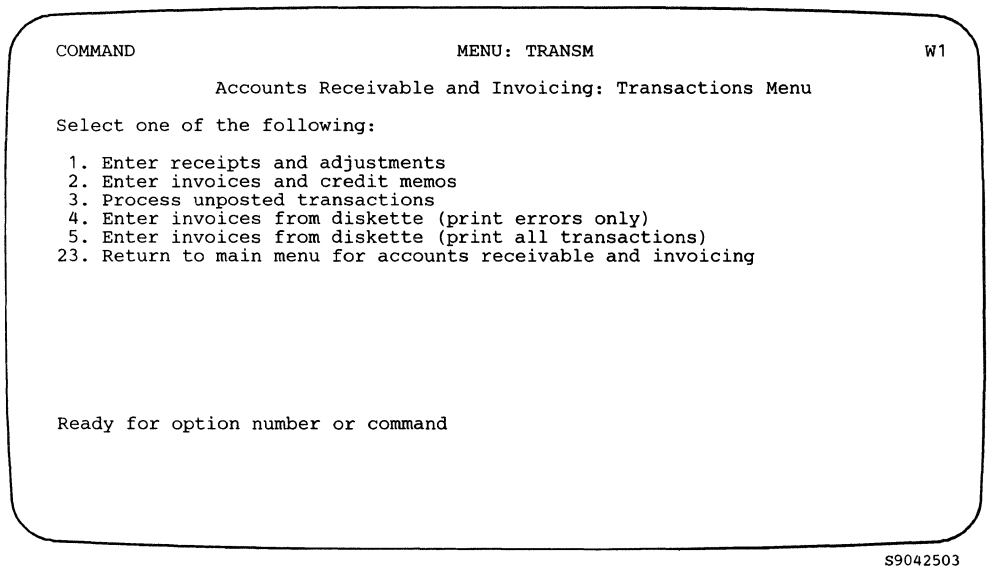
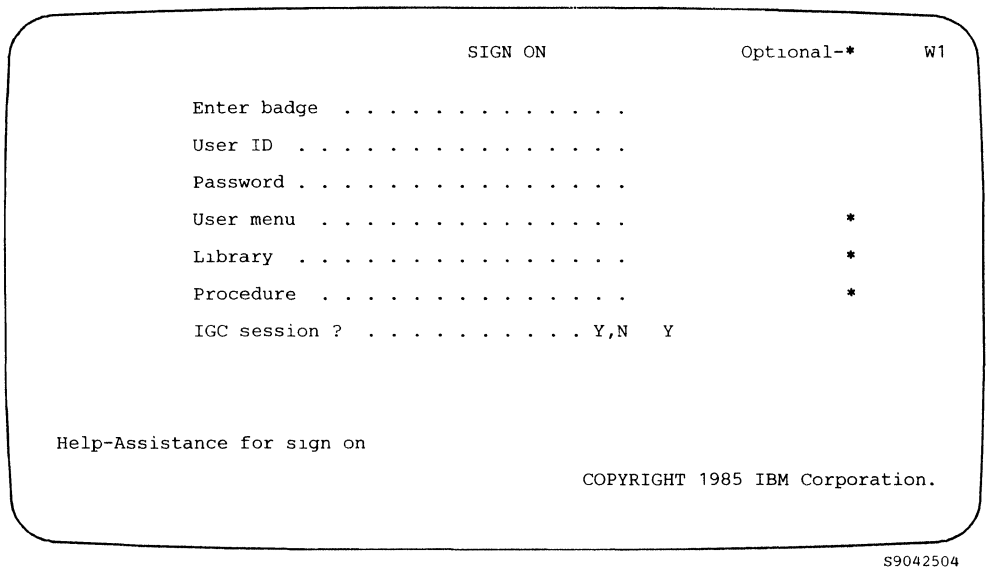


Figure 1-3. Accounts Receivable and Invoicing: Transactions Menu

Badge Security

If password security is active, you can use another type of security called badge security. Badge security prevents unauthorized users from signing on to a display station that has a magnetic stripe reader configured. When badge security is active, the display station configured with a magnetic stripe reader has an *Enter badge* prompt on the Sign On display. Figure 1-4 shows the Sign On display with the *Enter badge* prompt:



Note: The IGC session prompt appears only if you have the ideographic version of the SSP.

Figure 1-4. Sample Sign On Display with Badge Security Active

The user must move a badge through the magnetic stripe reader as well as supply the other information needed during sign-on. The badge has a magnetic stripe with specially coded data. Consult your local IBM branch office for information about obtaining badges and magnetic stripe readers, and about coding the information needed on the magnetic stripe.

If the person does not have a badge or uses a badge with the wrong information, that person is unable to sign on at that display station. Figure 1-5 shows a magnetic stripe reader and a badge being passed through the reader.

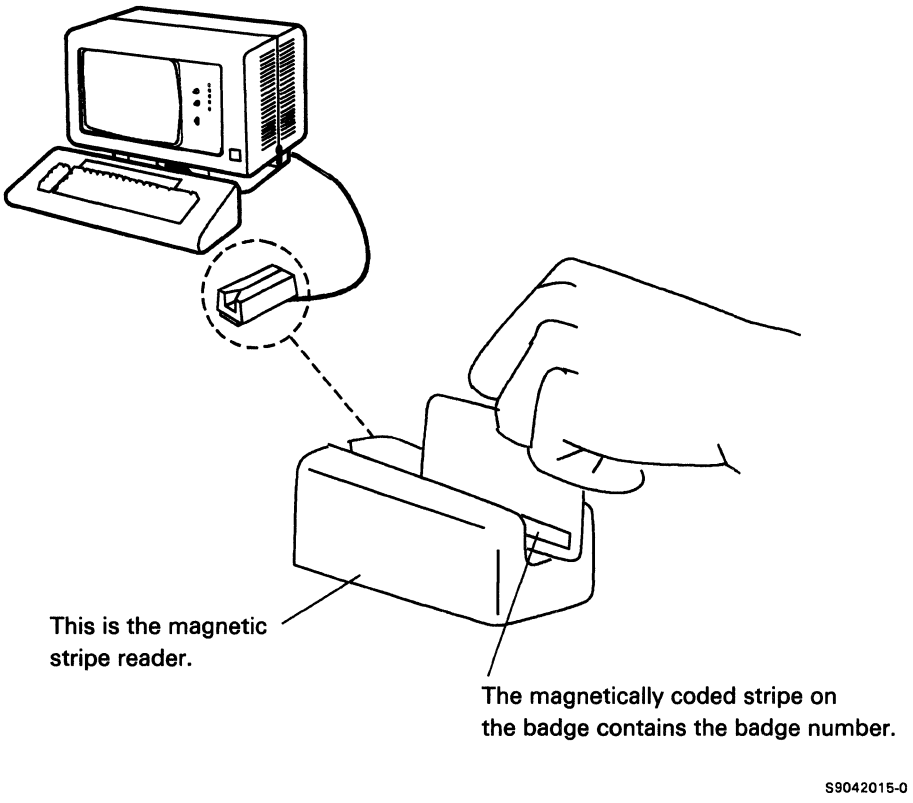


Figure 1-5. Magnetic Stripe Reader and Badge

Badge security requires a magnetic stripe reader at a display station and the hardware support for connecting the reader to the display station. The display stations with badge readers are identified during system configuration.

Not every display station needs a magnetic stripe reader; a person with a badge can still sign on at a display station without a magnetic stripe reader. You might decide to install magnetic stripe readers only at those display stations that are far away from your central data processing center.

Communications Security

In order to use communications security, password security must be active.

Communications security is only valid with the APPC (advanced program-to-program communications) subsystem. APPC is the communications support that allows System/36 to communicate with other systems having compatible support.

Communications security allows you to verify a remote location's identity before you allow it to run programs on your system. When communications security is in effect, the local and remote locations must send and receive the same location password to start an APPC session.

If both systems have communications security in effect, they verify each other's identity, by exchanging location passwords, before an APPC session can be started.

If neither system has communications security and password security, a user on one system can access any resources that are not secured and any secured resources he is authorized to access on the other system.

If one system has password security and the other system does not, a user ID of *NULL allows users on the system that is not secured to access (start a procedure on), via APPC, the secured system. The secured system must create a user profile with a user ID of *NULL. The user ID of *NULL and an access level should be entered for the resources on your system that you will allow the system that is not secured to access.

Required entries for the *NULL user profile are described in the section "Entering User Profiles" in Chapter 2. Refer to the section "Location Profiles" in Chapter 2 for more information on communications security.

Note: Do not create a location profile for a remote location that does not use communications security.

Resource Security

Resource security helps prevent unauthorized access to disk files, libraries, folders, and folder members on your system.

When resource security is not active, anyone who can sign on to the system can use any file, library, or folder on the system.

*Note: Diskette and tape files **cannot** be secured using resource security.*

Resource security is a good way of ensuring that only the people that you have authorized to use certain files, libraries, and folders can do so. You can, for example, allow only the employees responsible for the payroll to update the personnel files and to run the payroll programs.

Chapter 2. User Identification File

Introduction

The user identification file (called the user ID file) is made up of records called user profiles and location profiles. Each user profile contains security information about someone who is allowed to sign on to your system. Each location profile contains security information about a remote location that is allowed to access your system via advanced program-to-program communications (APPC).

User Profiles

Each user profile contains information about someone who is allowed to sign on to your system. The information that can be included in a user profile includes:

- User ID
- Password
- Date the password last changed
- Security classification
- Service aid authority
- Default user menu
- Mandatory menu
- Default sign-on procedure
- Mandatory procedure
- Default library
- Beginning help menu
- Comment
- Badge number

Part of this information is used only when password security is active and the other part (user ID, default user menu, default sign-on procedure, default library, beginning help menu, and comment) is used whether password security is active or not active.

The following describes the information contained in each user profile.

Password Security Information

User ID: The user ID identifies the user signing on to your system. Each user must have a unique user ID. A user ID is also useful for tracing the activity of a particular user on the system. For example, when a job is logged into the history file, the user ID identifies the user who is running it.

Password: The password is used to verify a user's identity. If password security is active, the password is checked and verified when the user signs on to your system.

Although it is not required, it is suggested that passwords be unique to each individual. Passwords should be random and meaningless groups of characters.

Date the Password Last Changed: This is the date on which the user last changed his or her password. This field in the user profile is updated each time the user changes his or her password (using the PASSWORD procedure or SECEDIT procedure) or when the master security officer or security officer changes the user's password. The date can also be set to the current date by the RESTORE procedure.

Security Classification: The security classification determines the amount of control a user has over the jobs that are run on the system and the output that the system prints. Security classifications are listed in highest to lowest levels of authority. Each security classification also has all the authority of all the lower classifications.

The security classifications are:

- M (master security officer)

  In addition to what is listed for a security officer, a system console operator, a subconsole operator, and a display station operator, a master security officer can:

  - Change, remove, list, or add any security information
  - Activate or deactivate all types of system security
  - Create and remove the security files
  - Save or restore information contained in the security files

- S (security officer)

  In addition to what is listed for a system console operator, a subconsole operator, and a display station operator, a security officer can:

  - Change, remove, list, or add security information about himself or herself, system console operators, subconsole operators, and display station operators
  - Change, remove, add, or list any information about resource security
  - Edit, delete, print, restore, or save network resource directory

- O (system console operator)

  In addition to what is listed for a subconsole operator and a display station operator, a system console operator can:

  - From the system console, run certain procedures not allowed at other display stations
  - Run procedures not allowed by users with lower security classifications
  - Control all jobs run on the system and their printed output
  - Use the system console

- C (subconsole operator)

  In addition to what is listed for a display station operator, a subconsole operator can:

  - Control the running of his or her own jobs
  - Control the printing of output for the printers controlled by a subconsole
  - Use a subconsole

- D (display station operator)

  A display station operator can:

  - Control the running of only his or her own jobs and their printed output
  - Use the security procedures to list security information about the secured resources that he or she is authorized to use
  - Use the security procedures to change security information about the secured resources that he or she owns
  - Secure his or her own files, libraries, folders, and folder members
  - Use a subconsole in command mode

Service Aid Authority: Service aid authority indicates whether the user can run the following service aid procedures to diagnose and correct problems on the system:

- DFA: Gets selected information from a dump file (a copy of all or part of storage), formats the information, and either prints or displays the information.

- DUMP: Prints or displays selected storage areas on disk.

- PATCH: Displays selected areas on disk or diskette and allows you to change the data in those areas.

- PTF (PATCH parameter only): Changes a library member.

Master security officers automatically receive service aid authority; this authorization cannot be changed.

A user must have service aid authority to apply a change to or rebuild the master configuration record (options 12 and 13 on the CNFIGSSP Main Menu).

Default User Menu: The default user menu is the menu that appears after the user signs on. When you specify a default menu for a user, the user does not have to enter the name of the menu in the menu field on the Sign On display.

Notes:

1. *A user can change his or her default menu by displaying a different menu and pressing command key 23. The displayed menu then becomes the default menu and the current library becomes the default library. If password security is not active and the user does not have a user profile in the user ID file, a user profile is created for the user when he or she presses command key 23. The default menu can also be changed using SECEDIT USERID.*

2. *The user cannot change the default menu if the default menu is specified as the user's mandatory menu.*

Mandatory Menu: The default user menu can also be specified as the user's mandatory menu. The user is then restricted to selecting options from the default user menu and entering the MSG and OFF commands.

Note: If the user is restricted to a mandatory menu, the PASSWORD procedure must be an option on the mandatory menu or the user cannot change his or her password.

Default Sign-On Procedure: The default sign-on procedure is the procedure that runs after the user presses the Enter key on the sign-on display and before the command display is shown. This procedure must exist in the user's default library or in #LIBRARY.

Note: A user can change his or her default sign-on procedure using the SECEDIT USERID procedure. A user cannot change the default sign-on procedure if the procedure is specified as the user's mandatory sign-on procedure. A user can enter a 0 in the default sign-on procedure prompt to sign on without running his or her default sign-on procedure as long as it is not mandatory.

Mandatory Procedure: The default sign-on procedure can also be specified as the user's mandatory procedure. The procedure you specify as the default sign-on procedure will run each time the user signs on the system. The user cannot change his or her mandatory sign-on procedure. If the procedure is mandatory, it must be completed successfully. If the user receives a system message because an error was detected, the procedure may not complete successfully, and the user cannot sign on.

Default Library: The default library is the name of the library that becomes the session library after the user signs on. The default user menu and default sign-on procedure must be in this library or in #LIBRARY. If either the menu or the procedure is mandatory, the user cannot change the default library.

Beginning Help Menu: The beginning help menu is the first system help menu displayed when the user enters the word HELP on a command display. The beginning help menu is displayed after the user signs on if a default user menu is not specified. If a user is restricted to a mandatory menu, the beginning help menu cannot be displayed unless help is started by a menu option. If you do not specify a beginning help menu, the Main Help menu is displayed when the user types in HELP and presses the Enter key. You can obtain a printout of most of the help menus by entering HELP MENUNAME at a command display. The SSP-supplied help menus and their purposes are described in the manuals, *Operating Your System* and *Using Your Work Station*.

Note: A user can change his or her beginning help menu by displaying a different help menu and pressing command key 24. The displayed help menu then becomes the user's beginning help menu. If password security is not active and the user does not have a user profile in the user ID file, a user profile is created for the user when he or she presses command key 24. The beginning help menu can also be changed using SECEDIT USERID.

Comment: An area within each user profile is set aside for you to include information about the user. For example, the user's name, telephone number, or department number could be included. This area is not checked by the system, but is there for your convenience in identifying a particular user.

Badge Security Information

Badge Number: Badge number is the number coded on the magnetic stripe of the user's badge.

Location Profiles

Each location profile contains information about a remote location that you want to communicate with in a secured environment. The following describes the information contained in each location profile.

Communications Security Information

Remote Location Name: The remote location name identifies the remote location you want to communicate with. Each remote location must have a unique remote location name.

Location Password: The location password is used to verify a location's identity. The local and remote locations must exchange the same location password to start an APPC session.

A null location password (*NULL) can be used in a location profile. Using a null location password can reduce processing time during session initiation. Use the null location password only in a physically secure environment.

User Password Required: User password required indicates whether a remote system must send a valid user password with the user ID before it can start a procedure on your system.

Comment: An area within each location profile is set aside for you to include information about the remote location. For example, the location's name, address, and telephone number could be included. This area is not checked by the system, but is there for your convenience in identifying a particular remote location.

Creating the User Identification File

The following steps and the system displays help you to create the user ID file. For information about signing on to the system and about entering procedures, see the manuals, *Operating Your System* and *Using Your Display Station.*

1. Sign on to the system console. Because password security is not yet active, you can use any user ID; however, if you are going to be a master security officer, it is suggested that you enter the user ID that you plan to use.

2. On a command display at the system console, do one of the following:

   a. Type SECDEF and press the Help key.
   b. Type HELP SECDEF and press the Enter key.

   Either method allows you to run the SECDEF procedure. SECDEF is the security procedure you need to use to create the user ID file.

   For either method, the following display appears:

```
                              SECDEF PROCEDURE

            Creates or removes the user identification file; creates
            or removes the resource security file; or activates
            or deactivates password, resource, or badge security.

Security type . . . . . . . . . . . . . . . . . USERID,RESOURCE  USERID




Cmd3-Previous menu                                        COPR IBM Corp. 1985
```

S9042505

Notes:

a. The security procedures described in this guide can also be used by typing the name of the procedure followed by one or more parameters. The security procedures and parameter values are described in Appendix D.

b. Only one security procedure that uses the user ID file can be run at a time. For example, one user cannot be editing the user ID file (SECEDIT USERID procedure) while another user is listing the file (SECLIST USERID procedure). The second user trying to use the user ID file receives an error message with options to try again or cancel the request.

3. You do not have to enter the security file type. USERID (the default value) indicates that the user ID file is to be created.

   Press the Enter key.

   The following display appears:

```
                              SECDEF PROCEDURE

            Creates or removes the user identification file; creates
            or removes the resource security file; or activates
            or deactivates password, resource, or badge security.

Security type . . . . . . . . . . . . . . . . . . USERID,RESOURCE  USERID

Option  . . . . . . . . . . . . . . . . . . . . . ACTBDG,ACTPW,CREATE
                      DEACTBDG,DEACTPW,DELETE,STRTDATE,STOPDATE          *




Cmd2-Page back                                          COPR IBM Corp. 1985
```

S9042506

4. Using the display shown in step 3, you can choose one of several tasks:

   Activate badge security
   Activate password security
   Create the user ID file
   Deactivate badge security
   Deactivate password security
   Delete the user ID file
   Start the date checking function
   Stop the date checking function

   Because you want to create the user ID file, type CREATE, and press the Enter key.

   The following display appears:

```
                SECDEF: Create the user identification file                W1

           The user identification file does not currently exist.
           To create the file enter the following value:

Number of user and location profiles . . . . . 18 - 3998        18




           Press the Enter key to create the user identification file.



Cmd3-Display previous menu          Cmd7-End              COPR IBM Corp. 1985
```

S9042507

5. Using the display shown in step 4, specify the size of the user identification file. Each user profile counts as one record. Each location profile counts as one record. The number 18 (already displayed) is the minimum number of records (user profiles and location profiles) allowed for the user ID file; 3998 is the maximum number allowed.

   Type the number of users and remote locations you plan to have use your system. For example, if you have completed the user ID file planning forms for 35 of your employees and 1 remote location, type the number 36.

   The actual size of the user ID file created by the system might be slightly larger than the size that you specify. That is because the system rounds the number of users you specify to the next greatest multiple of 20 and then subtracts 2. For example, if you specify 36 users, the actual number of records in the file will be 38 (that is, 40 - 2).

6. If you decide not to create the user ID file, press command key 7. The SECDEF procedure does not create the user ID file, and the procedure ends.

   If you decide to create the user ID file, press the Enter key. The user ID file is created on disk. Press command key 3 or the Enter key to complete the SECDEF procedure.

Activating Password Security

To enter password security information into the user ID file, you must first activate password security.

If you do not want to activate password security but do want to specify user IDs, default user menus, default sign-on procedures, default libraries, and beginning help menus, skip this section and the section on activating badge security and go to the section "Entering Profiles into the User ID File."

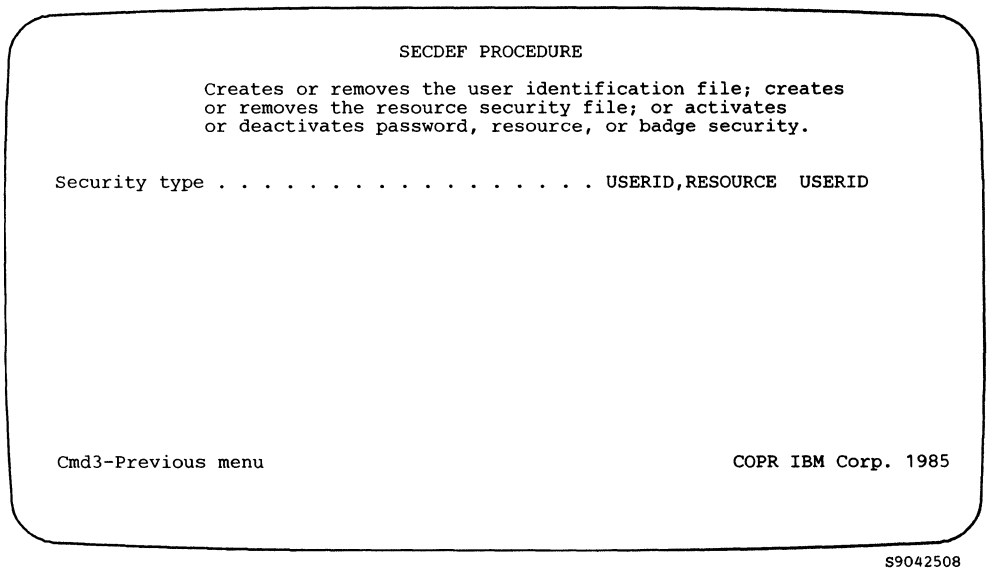
To activate password security, do the following:

1. On the command display at the system console, type the following:

   ```
   SECDEF
   ```

   Press the Help key.

   The following display appears:



S9042508

2. On the display shown in step 1, the system asks you for the type of security file that you want to work with. The system has already filled in USERID for the security file type. Because password security uses the user ID file, press the Enter key.

   The following display appears:

```
                              SECDEF PROCEDURE

            Creates or removes the user identification file; creates
            or removes the resource security file; or activates
            or deactivates password, resource, or badge security.


Security type . . . . . . . . . . . . . . . . . USERID,RESOURCE  USERID

Option  . . . . . . . . . . . . . . . . . . . . ACTBDG,ACTPW,CREATE
                    DEACTBDG,DEACTPW,DELETE,STRTDATE,STOPDATE              *









Cmd2-Page back                                          COPR IBM Corp. 1985
```

S9042509

3. Using the display shown in step 2, you can choose one of several tasks:

   Activate badge security
   Activate password security
   Create the user ID file
   Deactivate badge security
   Deactivate password security
   Delete the user ID file
   Start the date checking function
   Stop the date checking function

   Because you want to activate password security, type ACTPW, and press the Enter key.

   The following display appears:

```
                    SECDEF: Activate password security                    W1

            Type any changes and press the Enter key to schedule
            password security to be activated at the next IPL.

 Master security officer user ID . . . . . . . . . . . . . . . . . LAG535

 Master security officer password  . . . . . . . . . . . . . . .

 Override user ID  . . . . . . . . . . . . . . . . . . . . . . . .

 Override password . . . . . . . . . . . . . . . . . . . . . . . .

 Maximum invalid sign-on attempts  . . . . . . . . . . . 3 - 25  10

 Start password date checking to
   require users to change passwords?  . . . . . . . . . .   Y,N  Y

      Press the Enter key to schedule password security to be activated.

Cmd3-Display previous menu          Cmd7-End              COPR IBM Corp. 1985
```

S9042510

4. The user ID that you entered when you created the user ID file is already displayed. The system assumed this is the user ID of a master security officer. You can change your user ID at this time if you want to. Type your password, too.

5. Type an override user ID and an override password. You will need the override user ID and override password if the user ID file is removed or destroyed or if the master security officer forgets his or her user ID and password. The override user ID and override password can only be used on the IPL Sign On display.

   Notes:

   a. *The override user ID and override password are not stored in the user ID file. Be sure to keep a record of the override user ID and the override password.*

   b. *After password security is active, you can change the override user ID, the override password, and the maximum invalid sign-on attempts by typing* `SECDEF USERID,ACTPW` *and pressing the Enter key. A display appears on which you can change the override user ID, the override password, and the maximum invalid sign-on attempts.*

6. Type the maximum invalid sign-on attempts. Valid values are any number from 3 through 25. The system default is 10. The value you enter is:

   - The maximum number of times you will allow a user to enter an incorrect user ID or password during sign on. If a user enters an incorrect user ID or password this maximum number of times consecutively, the display station at which the incorrect user ID or password was entered is varied offline.

   - The maximum number of times you will allow a user to enter his or her current password incorrectly when changing his or her password. If a user enters his or her current password incorrectly this maximum number of times consecutively, the user is signed off the system.

   - The maximum number of times a user can attempt to start an Interactive Communications Feature (SSP-ICF) procedure with an invalid user ID or password. If a user attempts to start an SSP-ICF procedure using an incorrect user ID or password this maximum number of times consecutively, your location is disabled and must be enabled again before it can start procedures. For information on how to enable and disable, see the ENABLE and DISABLE procedures in the *System Reference* manual.

7. Type Y (yes) or N (no) to indicate whether or not to start the password date checking function. You can use the password date checking function to require users to change their passwords within a specified number of days.

8. If you decide to activate password security and start the password date checking function (ACTPW in step 3, Y in step 7), press the Enter key. The following display appears:

```
                        SECDEF : Password date checking                    W1

                         Start password date checking

Maximum number of days user may
 keep current password . . . . . . . . . . . . . . . . . . 1 - 366  60

Number of days user will be warned
 before password expires . . . . . . . . . . . . . . . . . 1 - 366  14

          Type any changes and press the Enter key to schedule
          password date checking to start.  Password security
          and password date checking will be scheduled to be
          activated at the next IPL.  If password security is
          active, password date checking is started immediately.




Cmd3-Display previous menu          Cmd7-End              COPR IBM Corp. 1985
```

S9042600

a. Type the maximum number of days users are allowed to keep their passwords. Valid values are any number from 1 through 366; the system default is 60.

b. Type the number of days you want users to receive a warning message before their passwords expire. Users receive a warning message each time they sign on until they change their password or their password expires.

c. Press the Enter key. A message is displayed telling you password security and date checking will be started after the next initial program load (IPL) of the system.

d. Press command key 3 or the Enter key to complete the SECDEF procedure. If you decide to change these values, type SECDEF USERID,STRTDATE. The current values are displayed and can be changed. The new values become effective immediately.

If you decide not to activate password security and not start the password date checking function, press command key 7. The SECDEF procedure does not activate password security or start the password date checking function, and the procedure ends.

If you decide to activate password security and not start the password date checking function (ACTPW in step 3, N in step 7), press the Enter key. A message is displayed that indicates that password security will be activated at the next IPL. Press command key 3 or the Enter key to complete the SECDEF procedure.

Note: Before you perform an IPL, you should follow the steps in the section "Activating Badge Security" if you also want to have badge security active on your system.

9. Perform an IPL of the system. To activate password security, you *must* perform an IPL. For information about how to IPL, see the manual, *Operating Your Computer.*

Notes:

1. *After the IPL is complete, the only user IDs and passwords that the system recognizes are the user IDs and passwords specified in steps 4 and 5.*

2. *After the IPL is complete, you should run the SECEDIT procedure to define the other users to the system. See the section "Entering Profiles into the User ID File" later in this chapter.*

3. *Once password security is active and you have entered the other user profiles into the user ID file, menu security will also be active for those users who have mandatory menus.*

Starting the Password Date Checking Function

The password date checking function is an SSP option that requires users to change their passwords within a specified number of days. Once this function is started, all users are required to change their own passwords within the number of days you specify. You can also specify the number of days you want users to receive a message warning them that their password is about to expire. You must be a master security officer to activate the password date checking function.

Note: If a user is restricted to a mandatory menu, the PASSWORD procedure must be an option on the mandatory menu or the user will not be able to change his or her password.

To start the password date checking function, password security must already be active or scheduled to be active at the next IPL.

Note: You may already have told the system you wanted to start the password date checking function when you performed the steps in the previous section, "Activating Password Security." If you did, and you do not want to change any of the values you specified, you can skip this section.

If password security is already active on your system, you can start the password date checking function by performing the following steps.

1. Type the following on the command display:

   ```
   SECDEF
   ```

   Press the Help key.

   The following display appears:

```
                              SECDEF PROCEDURE

            Creates or removes the user identification file; creates
            or removes the resource security file; or activates
            or deactivates password, resource, or badge security.

Security type . . . . . . . . . . . . . . . . . USERID,RESOURCE  USERID




Cmd3-Previous menu                                        COPR IBM Corp. 1985
```

S9042601

2. On the display shown in step 1, the system asks you for the type of security file that you want to work with. The system has already filled in USERID for the security file type. Because the password date checking function uses the user ID file, press the Enter key.

   The following display appears:

```
                              SECDEF PROCEDURE

            Creates or removes the user identification file; creates
            or removes the resource security file; or activates
            or deactivates password, resource, or badge security.


Security type . . . . . . . . . . . . . . . . . USERID,RESOURCE  USERID

Option  . . . . . . . . . . . . . . . . . . . . ACTBDG,ACTPW,CREATE
                    DEACTBDG,DEACTPW,DELETE,STRTDATE,STOPDATE              *









Cmd2-Page back                                          COPR IBM Corp. 1985
```

S9042602

3. Using the display shown in step 2, you can choose one of several tasks:

   Activate badge security
   Activate password security
   Create the user ID file
   Deactivate badge security
   Deactivate password security
   Delete the user ID file
   Start the date checking function
   Stop the date checking function

   Because you want to start the date checking function, type STRTDATE, and press the Enter key.

   The following display appears:

```
                        SECDEF : Password date checking                    W1

                         Start password date checking

Maximum number of days user may
 keep current password . . . . . . . . . . . . . . . . . 1 - 366  60

Number of days user will be warned
 before password expires . . . . . . . . . . . . . . . . 1 - 366  14

          Type any desired changes and press the Enter key to
          start password date checking.  No IPL is necessary
          if password security is already active.




Cmd3-Display previous menu          Cmd7-End              COPR IBM Corp. 1985
```

S9042603

4. Type the maximum number of days you want to allow users to keep their passwords. Valid values are 1 through 366 days. The default is 60 days.

5. Type the number of days you want users to be warned before their passwords expire. Valid values are 1 through 366 days. The default is 14 days.

6. If you decide not to start the password date checking function, press command key 7. The SECDEF procedure ends without starting password date checking.

   If you decide to start the password date checking function, press the Enter key. A message is displayed that indicates that password date checking has started. This also puts the current date in each user profile in the *Date password last changed* field. Press command key 3 or the Enter key to complete the SECDEF procedure.

   If you decide later that you want to change these values, enter SECDEF USERID,STRTDATE again. A display shows the current values. These values can be changed to any number, 1 through 366, with the number of warning days less than the maximum number of days a user may keep a password. If you decrease the maximum number of days a user may keep a password, the *Password was changed on* date is reset in some users' profiles. If the user's password was valid with the current maximum, but would be expired with the new maximum, the date is reset so the password would expire in the number of days set for the user to be warned.

   For example, let's say the maximum number of days a user may keep a password is set to 60 days, and the number of days a user is to be warned is 14. If the user changed the password on 07/01/85, the warning would begin on 08/16/85, and the password would expire on 08/30/85. On 08/23/85 the user's password is 53 days old. If the master security officer changes the maximum number of days a user can keep a password from 60 to 30, that user's password would be expired with the new maximum of 30. The user's password will be reset to expire on 09/06/85, which is 14 days from 08/23/85. The *Password was changed on* date in that user's profile is reset to 08/07/85 which makes it appear that the password is 16 days old.

Activating Badge Security

To activate badge security, password security must already be active or scheduled to be active at the next IPL. For information about activating password security, see "Activating Password Security" earlier in this chapter. Once badge security is activated, badge number information must be in the user ID file for a user to sign on to a display station with a magnetic stripe reader. For information about entering badge number information, see "Entering Profiles into the User ID File" later in this chapter.

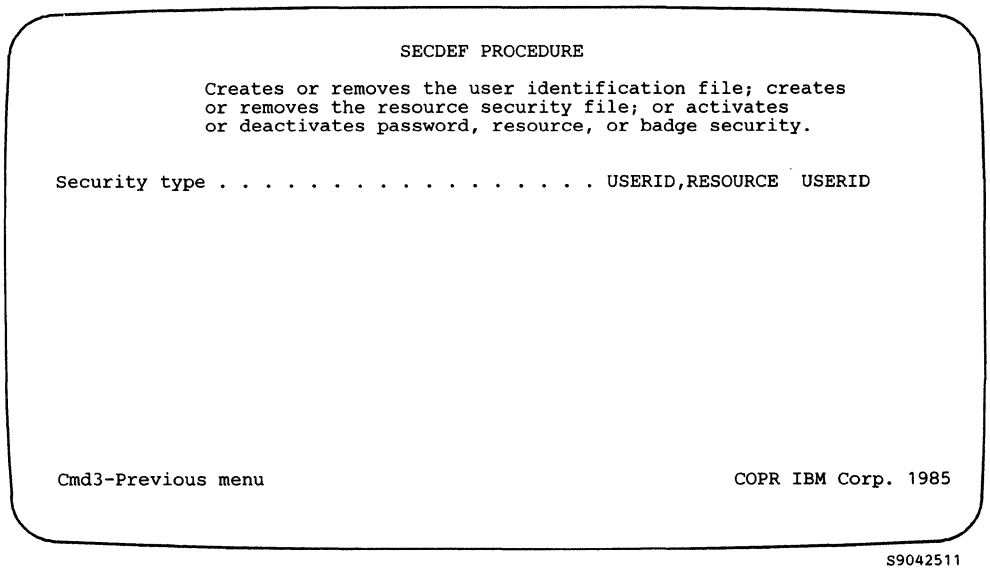
If password security is already active, you must be a master security officer to activate badge security. The following steps can be performed at any display station. If password security is not active but is scheduled to be active at the next IPL, you do not have to be a master security officer, but you must perform the following steps from the system console.

1. Type the following on the command display:

   ```
   SECDEF
   ```

   Press the Help key.

   The following display appears:



S9042511

2. On the display shown in step 1, the system asks you for the type of security file that you want to work with. The system has already filled in USERID for the security file type. Because badge security uses the user ID file, press the Enter key.

   The following display appears:

```
                              SECDEF PROCEDURE

            Creates or removes the user identification file; creates
            or removes the resource security file; or activates
            or deactivates password, resource, or badge security.


Security type . . . . . . . . . . . . . . . . . USERID,RESOURCE  USERID

Option  . . . . . . . . . . . . . . . . . . . . ACTBDG,ACTPW,CREATE
                    DEACTBDG,DEACTPW,DELETE,STRTDATE,STOPDATE                *









Cmd2-Page back                                          COPR IBM Corp. 1985
```

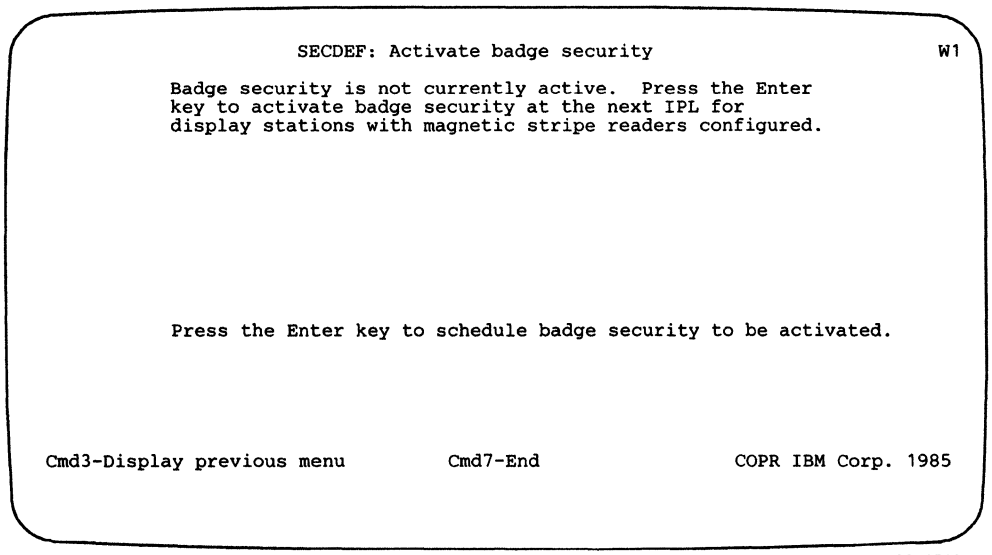
S9042512

3. Using the display shown in step 2, you can choose one of several tasks:

   Activate badge security
   Activate password security
   Create the user ID file
   Deactivate badge security
   Deactivate password security
   Delete the user ID file
   Start the date checking function
   Stop the date checking function

   Because you want to activate badge security, type ACTBDG, and press the Enter key.

   The following display appears:



S9042513

4. If you decide not to activate badge security, press command key 7. The SECDEF procedure does not activate badge security, and the procedure ends.

   If you decide to activate badge security, press the Enter key. A message is displayed that indicates that badge security will be activated at the next IPL. Press command key 3 or the Enter key to complete the SECDEF procedure.

5. Perform an IPL of the system. To activate badge security, you *must* perform an IPL. If password security is not already active but is scheduled to be active, both password security and badge security are activated when you perform an IPL.

Entering Profiles into the User ID File

Now that you have created the user ID file, you are ready to enter information into that file. It is not necessary to have password and badge security active to enter information into the user ID file.

Entering User Profiles

If you filled out a planning form (User Identification Form O) for each user of your system, you can use the completed forms when you enter user profiles into the user ID file. If you did not fill out a planning form for each user of your system, you can still enter user profiles into the user ID file. However, you might want to jot down some notes about each user before you begin to do the actual entry work.

The following illustration shows a completed Form O and those entries being entered into the user ID file using the SECEDIT USERID procedure.

Note: If you have not activated password security, the only user profile information you can enter is:

User ID
Default user menu
Default sign-on procedure
Default library
Beginning help menu
Comment

User Identification Form

Customer Name _____
Customer Number _____

Name Paul Hanson
Position Department Supervisor
Responsibilities ordering supplies, tracking departments
production and workload

Optional=*
User ID PHDEPT51
Password 143L
Security classification? D
(M, S, O, C, D)
Service aid authority? N
(Y, N)
*Default sign-on procedure PLANTP
Procedure mandatory? N
(Y, N)
*Default user menu PLANTM
Menu mandatory? Y
(Y, N)
*Default library PLANTLIB
Beginning help menu MAIN
(MAIN)
*Comment PAUL HANSON
DEPT SUPERVISOR
MANUFACTURING DEPT51
*Badge number
(00000000-99999999)

M = Master security officer
S = Security officer
O = System console operator
C = Subconsole operator
D = Display station operator

S9042002-3

```
                              SECEDIT USERID                              W1
                                                                  Optional-*
          Edit the user profiles in the user identification file

     Mode:  Add - Key in profile information and press Enter

User ID . . . . . . . . . . . . . . . . . . . . . . . . . . . . PHDEPT51

Password . . . . . . . . . . . . . . . . . . . . . . . . . . . 143L

Security classification . . . . . . . . . . . . . . . M,S,O,C,D  D

Service aid authority ? . . . . . . . . . . . . . . . . . Y,N  N

Badge number . . . . . . . . . . . . . . . . 00000000-99999999          *

Comment . . . . . . . . . . . . . . . . . . . . . . PAUL HANSON         *
                                                    DEPT SUPERVISOR
                                                    MANUFACTURING DEPT51

Roll keys-Page          Cmd2-Scan           Cmd3-Restart
Cmd4-Remove             Cmd5-Add mode       Cmd6-Show passwords
Cmd7-End                Cmd9-Additional information
                                                  COPR IBM Corp. 1985
```

S9042514

```
                              SECEDIT USERID                              W1
                                                                  Optional-*
          Edit the user profiles in the user identification file

User ID      PHDEPT51

     Mode: Add - Key in profile information and press Enter

Default user menu . . . . . . . . . . . . . . . . . . . . . . . PLANTM     *
  Menu mandatory? . . . . . . . . . . . . . . . . . . . . Y,N  Y

Default sign-on procedure . . . . . . . . . . . . . . . . . . . PLANTP     *
  Procedure mandatory? . . . . . . . . . . . . . . . . . Y,N  N

Default library . . . . . . . . . . . . . . . . . . . . . . . . PLANTLIB   *
Beginning help menu . . . . . . . . . . . . . . . . . . . . . . MAIN       *

Comment . . . . . . . . . . . . . . . . . . . . . . PAUL HANSON         *
                                                    DEPT SUPERVISOR
                                                    MANUFACTURING DEPT51

Roll keys-Page       Cmd2-Scan       Cmd3-Restart       Cmd4-Remove
Cmd5-Add mode        Cmd7-End        Cmd10-Previous information
                                                  COPR IBM Corp. 1985
```

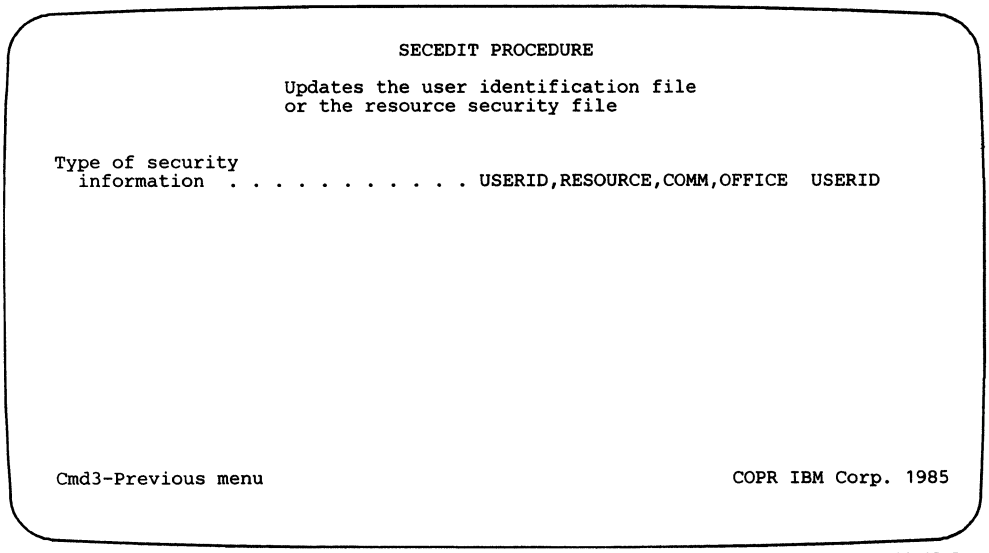
S9042612

1. To enter user profiles into the user ID file, type:

   ```
   SECEDIT USERID
   ```

   Press the Help key.

   The following display appears:



S9042515

2. Press the Enter key.

   Note: The next display you see contains the user ID that you entered when you activated password security (see "Activating Password Security" earlier in this chapter). The password you entered when you activated password security is not displayed. You can use command key 6 to display your password. At this time, you should follow applicable steps 3 through 13 to complete your own user profile, then press the Enter key.

   If you did not activate password security and badge security, the next display you see shows only the user ID, default user menu, default sign-on procedure, default library, beginning help menu, and comment prompts. This is the only user profile information you can enter when password security and badge security are not active.

   If you did activate password security and badge security, the following display appears:

```
                              SECEDIT USERID                              W1
                                                                  Optional-*
          Edit the user profiles in the user identification file

     Mode: Add - Key in profile information and press Enter

User ID . . . . . .

Password . . . . . .

Security classification . . . . . M,S,O,C,D   D

Service aid authority ? . . . . . Y,N   N

Badge number . . . . . 00000000-99999999                              *

Comment . . . . . .                                                   *


Roll keys-Page              Cmd2-Scan             Cmd3-Restart'
Cmd4-Remove                 Cmd5-Add mode         Cmd6-Show passwords
Cmd7-End                    Cmd9-Additional information
                                                  COPR IBM Corp. 1985
```

S9042516

3. Type the user ID of the user. A user ID can be any combination of up to 8 characters; the first character must be 0 through 9, A through Z, #, @, or $. The user ID of *NULL, valid only during an APPC session, is the only exception. The remaining characters can be any character of the alphabet, any number, or any special character except a comma. Also, the user ID cannot contain any blanks between the characters.

4. Type the 4-character password of the user. Use any letter of the alphabet, any number, or any special character except a blank.

5. Type the security classification of the user. Security classifications are:

   M Master security officer
   S Security officer
   O System console operator
   C Subconsole operator
   D Display station operator

   Security classifications are described in detail in the "Introduction" earlier in this chapter.

6. Type Y (yes) or N (no) to indicate whether the user can run the service aid procedures.

7. If the user has a badge, type the badge number.

8. A comment of up to 60 characters can be entered here.

   Press command key 9 or the Enter key to show the additional user profile information on the next display. The following display appears:

```
                                SECEDIT USERID                          W1
                                                                  Optional-*
          Edit the user profiles in the user identification file

User ID:

     Mode: Add - Key in profile information and press Enter

Default user menu . . . . . . . . . . . . . . . . . . . . . .           *
  Menu mandatory? . . . . . . . . . . . . . . . . . . . . . . Y,N   N

Default sign-on procedure . . . . . . . . . . . . . . . . . .           *
  Procedure mandatory? . . . . . . . . . . . . . . . . . . . Y,N   N

Default library . . . . . . . . . . . . . . . . . . . . . . .           *
Beginning help menu . . . . . . . . . . . . . . . . . . . . .   MAIN    *

Comment . . . . . . . . . . . . . . . . . . . . .                       *


Roll keys-Page       Cmd2-Scan        Cmd3-Restart       Cmd4-Remove
Cmd5-Add mode        Cmd7-End         Cmd10-Previous information
                                                  COPR IBM Corp. 1985
```

S9042604

   For your convenience, the user ID you entered on the previous display is displayed again. You cannot type over the user ID. It is displayed for your information only.

   *Note: If a user ID of *NULL is entered on the first screen, the **Beginning help menu** field is blank because a *NULL user ID cannot have a beginning help menu.*

   The comment you entered on the previous display is also displayed again. You can, however, change the comment field on this display.

9. Type the default user menu for this user. This menu name can be up to 6 characters.

10. *Menu mandatory?* specifies whether the user is (Y) or is not (N) restricted to selecting options from the default user menu that you specified in step 9.

11. Type the default sign-on procedure for this user. This procedure name can be up to 8 characters.

12. *Procedure mandatory?* specifies whether or not (Y or N) the default sign-on procedure must run successfully each time this user signs on.

13. Type the name of the default library that contains the default user menu and sign-on procedure. The library name can be up to 8 characters. If you do not specify a default library, #LIBRARY becomes the user's session library when the user signs on.

14. Type the name of this user's beginning help menu. The beginning help menu is the first help menu displayed when the user enters the word HELP on a command display.

15. Press the Enter key. The next blank user profile is displayed. Continue entering user profiles for each user of your system. Press command key 7 to end the SECEDIT USERID procedure.

A null user profile can be entered for communications security. The user ID in this user profile is *NULL. The *NULL user ID cannot be entered when a user signs on at a display station. The *NULL user ID is valid only when transmitted during an APPC session. The *NULL password is not checked for expiration; it is always a valid password.

When your secured system is communicating with a system that is not secured or a secured system that sends a null user ID, your system substitutes the *NULL user ID for the null user ID it received.

A user profile with the *NULL user ID must exist in your user ID file at the time of the transmission. Otherwise, the remote system cannot start procedures on your system.

When you enter a user profile with *NULL as the user ID, you must enter the following information:

User ID: *NULL

Password: (leave blank)

Security classification: D

Service aid authority: N

Badge number: (leave blank)

Default user menu: (leave blank)

Menu mandatory: N

Default sign-on procedure: (leave blank)

Procedure mandatory: N

Default library: (leave blank)

Beginning help menu: (leave blank)

Comment: Up to 60 characters (optional)

Entering Location Profiles

If you filled out a planning form (Location Identification Form S) for each remote location you want to communicate with using APPC, you can use the completed forms when you enter location profiles into the user ID file. If you did not fill out a planning form for each remote location you want to access your system, you can still enter location profiles into the user ID file. However, you might want to jot down some notes about each remote location before you begin to do the actual entry work.

The following illustration shows a completed Form S and those entries being entered into the user ID file using the SECEDIT COMM procedure.

Password security must be active to run the SECEDIT COMM procedure. The SECEDIT COMM procedure can be run from any display station but only by a master security officer.

S Location Identification Form	Name of Local System S36DEN Local Location Name DENVER	Customer Name Customer Number

Name of remote system S36AUS Remote location name AUSTIN Location password 3B963C562FA7CAC7 Require user passwords to start procedure? (Y,N) Y Comment Programming Center Hilton Bldg. Austin, Texas	Name of remote system Remote location name Location password Require user passwords to start procedure? (Y,N) Comment
Name of remote system Remote location name Location password Require user passwords to start procedure? (Y,N) Comment	Name of remote system Remote location name Location password Require user passwords to start procedure? (Y,N) Comment
Name of remote system Remote location name Location password Require user passwords to start procedure? (Y,N) Comment	Name of remote system Remote location name Location password Require user passwords to start procedure? (Y,N) Comment
Name of remote system Remote location name Location password Require user passwords to start procedure? (Y,N) Comment	Name of remote system Remote location name Location password Require user passwords to start procedure? (Y,N) Comment
Name of remote system Remote location name Location password Require user passwords to start procedure? (Y,N) Comment	Name of remote system Remote location name Location password Require user passwords to start procedure? (Y,N) Comment

S9042004-0

```
                         SECEDIT COMM                              W1
          Edit location profiles in the user identification file

      Mode: Add - Key in profile information and press Enter

                                                          Optional-*
  Remote location name . . . . . . . . . . . . . . . . . . . . AUSTIN

  Location password  . . . . . . . . . . . . . . . . . 3B963C562FA7CAC7

  Require user password to start each procedure? . . . . . . . . . Y,N  Y

  Comment  . . . . . . . . . . . . . . . . . . . . . PROGRAMMING CENTER     *
                                                      HILTON BLDG.
                                                      AUSTIN, TEXAS



  Roll keys-Page        Cmd2-Scan        Cmd3-Restart        Cmd4-Remove
  Cmd5-Add mode         Cmd6-Create password                 Cmd7-End
                                                               COPR IBM Corp. 1985
```

S9042517

1. To enter location profiles into the user ID file, type:

   ```
   SECEDIT COMM
   ```

   Press the Help key.

   The following display appears:

```
                          SECEDIT PROCEDURE

                  Updates the user identification file
                  or the resource security file


Type of security
  information  . . . . . . . . . . . USERID,RESOURCE,COMM,OFFICE  COMM









Cmd3-Previous menu                                   COPR IBM Corp. 1985
```

S9042518

2. Press the Enter key. The following display appears, which shows a blank location profile in the user ID file.

```
                                SECEDIT COMM                              W1

          Edit location profiles in the user identification file

   Mode: Add - Key in profile information and press Enter

                                                                  Optional-*
Remote location name . . . . . . . . . . . . . . . . . . . .

Location password  . . . . . . . . . . . . . . . . . . . . .

Require user password to start each procedure? . . . . . . . . . . Y,N  Y

Comment  . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . *









Roll keys-Page          Cmd2-Scan        Cmd3-Restart     Cmd4-Remove
Cmd5-Add mode           Cmd6-Create password              Cmd7-End
                                                           COPR IBM Corp. 1985
```

S9042519

3. Type the location name of the remote location you want to communicate with using APPC. A remote location name can be up to 8 characters and must begin with an alphabetic character (A through Z, @, #, $). The remaining characters can be any character except blank, comma (,), period (.), question mark (?), hyphen (-), slash (/), or apostrophe (').

4. Type the location password. Use command key 6 to have the system generate a random password for you or use the method described in Appendix E. The location password must be 1 through 16 hexadecimal characters. Valid hexadecimal characters are 0 through 9 and A through F.

   Write down the location password and give it to the person responsible for communications security at the remote location. Passwords for the local and remote systems must be identical.

5. *Require user password for starting procedure* specifies whether a valid user ID and user password does (Y) or does not (N) have to be sent before a procedure can be started on your system.

6. A comment of up to 60 characters can be entered here.

7. Press the Enter key. Another blank location profile is displayed. Continue entering location profiles for each remote location you want to communicate with. Press command key 7 to end the SECEDIT COMM procedure.

Changing Information in the User ID File

The SECEDIT USERID procedure also allows you to add, change, or remove user profiles in the user ID file. The SECEDIT COMM procedure allows you to add, change, or remove location profiles in the user ID file.

Changing User Profiles

If password security is active, the SECEDIT USERID procedure can be run:

- By a master security officer to display, add, change, or remove any user profile in the user ID file.
- By a security officer to display, add, change, or remove his or her own user profile or the user profiles of system console operators, subconsole operators, and display station operators.

  *Note: A security officer cannot display, add, change, or remove the user profile of a master security officer, another security officer, or the *NULL user profile.*

- By a system console operator, subconsole operator, or display station operator to change the following fields in his or her own user profile:

  Password
  Default library
  Default user menu
  Default sign-on procedure
  Beginning help menu
  Comment

  Note: If the default user menu or the default sign-on procedure of a system console operator, subconsole operator, or display station operator is mandatory, the user cannot change those fields or the default library field.

If password security is not active, anyone can run the SECEDIT USERID procedure to edit all information in the user ID file, but only from the system console. If not at a system console, the user can edit information only for that user ID. Also, certain password security information (passwords, badge numbers, mandatory menus and service aid authorization) cannot be displayed, added, changed, or removed.

If You Are a Master Security Officer or Security Officer

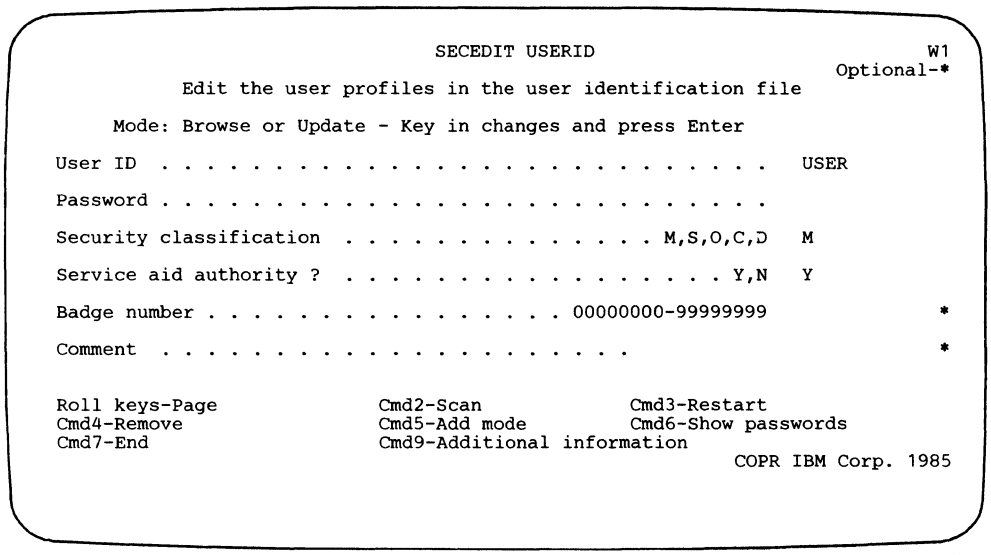
A master security officer can add, change, or remove any user profile in the user ID file. A security officer can change his or her own user profile and the profile of any other user with a security classification lower than his or her own. A security officer cannot add, change, or remove user profiles for master security officers, other security officers, or the *NULL user profile.

1. To display, add, change, or remove user profiles in the user ID file, type:

   ```
   SECEDIT USERID
   ```

   Press the Enter key.

   Two displays are required to show all the information in a user profile. The first display looks like this:



S9042605

The second display looks like this:

```
                                SECEDIT USERID                          W1
                                                                Optional-*
          Edit the user profiles in the user identification file

User ID:     USER

     Mode: Browse or Update - Key in changes and press Enter

Default user menu . . . . . . . . . . . . . . . . . . . . . .           *
  Menu mandatory? . . . . . . . . . . . . . . . . . . . . . . Y,N   N

Default sign-on procedure . . . . . . . . . . . . . . . . . .           *
  Procedure mandatory? . . . . . . . . . . . . . . . . . . . Y,N   N

Default library . . . . . . . . . . . . . . . . . . . . . . .           *
Beginning help menu . . . . . . . . . . . . . . . . . . . . .   MAIN    *

Comment . . . . . . . . . . . . . . . . . . . . .                       *


Roll keys-Page       Cmd2-Scan        Cmd3-Restart       Cmd4-Remove
Cmd5-Add mode        Cmd7-End         Cmd10-Previous information
                                                  COPR IBM Corp. 1985
```

S9042606

2. Use the displays shown in step 1 to do your work with user profiles. Refer to "Entering User Profiles" earlier in this chapter for a description of the prompts on these displays. You can use the following keys to help you edit the file:

Key	What It Does
Cmd2	Starts Scan mode. Scan mode allows you to display a specific user profile if your security classification allows you to display that user profile. After you press command key 2, a display appears on which you can enter the user ID for the user profile you want to display. When the user profile you requested is displayed, the SECEDIT USERID procedure is in Browse or Update mode so you can change information in that user profile. If the requested user ID cannot be found, or if you are not allowed to display that user profile, a message is displayed.
Cmd3	Starts Browse or Update mode and displays the first user profile you are allowed to see. Browse or Update mode allows you to display, change, or remove user profiles. The SECEDIT USERID procedure begins in this mode after the user ID file contains user profiles. You can display all the user profiles your security classification allows you to see. You can change all the fields in those user profiles, including the user ID field.
Cmd4	Removes a user profile from the user ID file. Command key 4 can be used only during Browse or Update mode. After you display a user profile and press command key 4, a message warns you that the user profile will be removed from the file. Press the Enter key to remove the user profile. If you decide not to remove the user profile, press a roll key or any of the other allowed command keys to continue editing.

Cmd5 Starts Add mode. Add mode allows you to add new user profiles.

When Add mode begins, a blank user profile is displayed. Type the information for the user profile prompts on the first display and then press command key 9 or the Enter key to see the second display of user profile information. Type the information for the user profile prompts on the second display and press the Enter key. The new user profile is added to the user ID file and another blank user profile is displayed. Press an allowed command key to end Add mode or press command key 7 to end the SECEDIT USERID procedure.

Cmd6 When you first enter the SECEDIT USERID procedure, passwords are not displayed. You can use command key 6 to display the passwords; then command key 6 again to not display them. This command key is only allowed on the first display of user profile information.

Cmd7 Ends the SECEDIT USERID procedure.

Cmd9 Displays the second display (additional information) of user profile information. The additional prompts are:

- Default user menu
- Mandatory menu
- Default sign-on procedure
- Mandatory procedure
- Default library
- Beginning help menu
- Comment

The comment field is displayed again. You can make changes to this field on either display. The user ID field is displayed again, too. You cannot, however, change the user ID field from this display; it is displayed for your convenience only.

Use command key 9 when you complete the first display of user profile information and you want to view (display) the second display of user profile information.

Cmd10 Displays the first display (previous information) of user profile information. This previous information includes:

- User ID
- Password
- Security classification
- Service aid authority
- Badge number
- Comment

The comment field is shown on both user profile displays. You can make changes to this field on either display.

Use command key 10 when you are viewing the second display of user profile information and you want to view (display) the first display of user profile information.

Roll keys The roll keys start Browse or Update mode. The roll keys page forward and backward through the user profiles that you are allowed to display or change. For example, if you are a security officer, you can only page through your own user profile and the user profiles for system console operators, subconsole operators, and display station operators; you cannot page through the user profiles of other security officers and master security officers, or the *NULL user profile.

Enter Enters information into the file from the display.

Help Can be used at any time to show information about the display you are viewing.

If You Are a System Console Operator, Subconsole Operator, or Display Station Operator

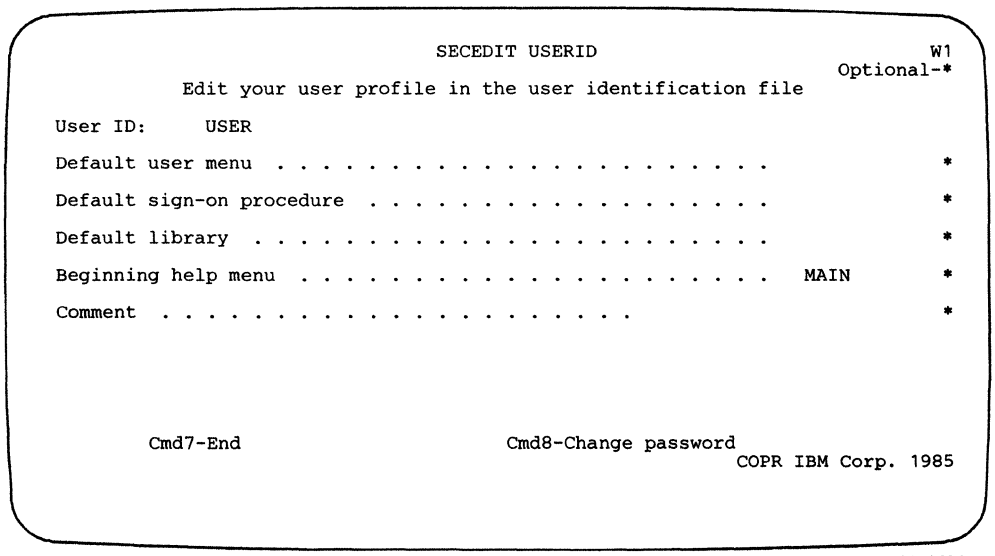
Any user with a security classification lower than security officer (system console operator, subconsole operator, or display station operator) can change only his or her own user profile.

1. To display or change your user profile, type:

   ```
   SECEDIT USERID
   ```

   Press the Enter key.

   The following display appears:



S9042607

   Note that your user ID is shown on this display. However, you cannot use this display to change your user ID. If you want your user ID changed, contact your master security officer or security officer.

2. Type the name of the user menu you want to be your default user menu. If you already have a default user menu that is not mandatory, just type over the default user menu name displayed. If you already have a default user menu that is mandatory, you cannot change it using this display. If you want your mandatory default user menu changed, contact your master security officer or security officer.

3. Type the name of the procedure you want to be your default sign-on procedure. If you already have a default sign-on procedure that is not mandatory, just type over the default sign-on procedure name displayed. If you already have a default sign-on procedure that is mandatory, you cannot change it using this display. If you want your mandatory default sign-on procedure changed, contact your master security officer or security officer.

4. Type the name of the library you want to be your default library. If neither your default user menu nor your default sign-on procedure is mandatory, you can change your default library by typing over the default library name already displayed. If either your default user menu or your default sign-on procedure is mandatory, you cannot change your default library using this display. In this case, if you want your default library changed, contact your master security officer.

5. Type the name of the help menu you want to be your beginning help menu.

6. Type a comment of up to 60 characters.

7. When you finish making changes to your user profile, press the Enter key. A message is displayed that the user profile changes were made.

You can use the following command keys when you are changing your user profile:

Key	**What It Does**
Cmd7	Ends the SECEDIT USERID procedure.
Cmd8	Allows you to change your password. A display is shown on which you can enter your current password and a new password. If password security is not active, command key 8 is not valid and will not be shown on the screen.

Changing Passwords

If password security is active, any user can use the PASSWORD procedure to change his or her password. The SECEDIT USERID procedure can also be used to change a password. See "Changing User Profiles" earlier in this chapter.

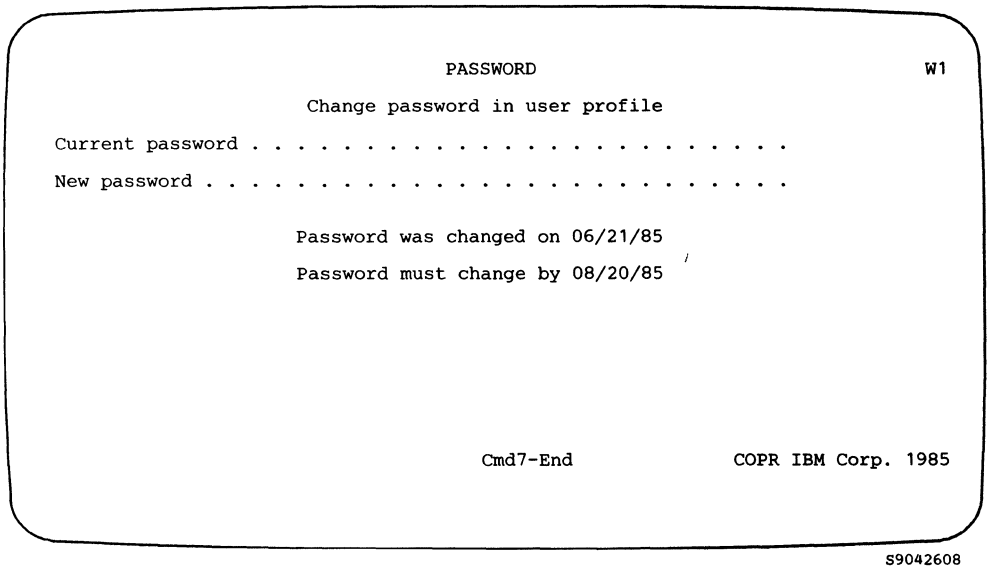
If password security is active and the password date checking function is started, users must change their password within a certain number of days. Your master security officer determined the number of days users may use a particular password and also the number of days users will receive a warning message before their password expires.

1. To change your password, type:

   ```
   PASSWORD
   ```

   Press the Enter key.

   The following display appears:



S9042608

   Note: If password date checking is not active, the additional line of text on the screen showing the date when the password must change is not displayed.

2. Type your current password. Your password will not appear on the display when you type it.

3. Type your new password. Your new password will not appear on the display when you type it.

4. Press the Enter key.

   If you entered your correct current password and a valid new password, the display is shown again with the message `Reenter new password to confirm change`. Type your new password again. If the password you enter this time matches the password you entered in step 3, your password is changed in your user profile. The PASSWORD procedure ends.

   Note: If you type your current password incorrectly, you receive an error message. Also, command key 7 and the attention key are not allowed. You must enter your correct current password on this display or you are signed off the system. The number of times you can enter an incorrect password was determined by your master security officer when he or she activated password security.

Changing Location Profiles

Password security must be active to run the SECEDIT COMM procedure. The SECEDIT COMM procedure can be run from any display station but only by a master security officer. A master security officer can display, add, change, or remove location profiles in the user ID file.

1. To display, add, change, or remove location profiles in the user ID file, type:

   ```
   SECEDIT COMM
   ```

   Press the Enter key.

   The first location profile in the user ID file is displayed. A display similar to the following appears:

```
                              SECEDIT COMM                              W1

          Edit location profiles in the user identification file

   Mode: Browse or Update - Key in changes and press Enter

                                                              Optional-*
Remote location name . . . . . . . . . . . . . . . . . . . . CHICAGO

Location password  . . . . . . . . . . . . . . . . . . . . 9B234A759E965B67

Require user password to start each procedure? . . . . . . . . . . Y,N  Y

Comment  . . . . . . . . . . . . . . . . . . . . . . . . . . WAREHOUSE    *
                                                            123 FOURTH STREET NW
                                                            CHICAGO, ILLINOIS



Roll keys-Page          Cmd2-Scan        Cmd3-Restart          Cmd4-Remove
Cmd5-Add mode           Cmd6-Create password                   Cmd7-End
                                                            COPR IBM Corp. 1985
```

S9042521

2. Use the display shown in step 1 to do your work with location profiles. Refer to "Entering Location Profiles" earlier in this chapter for a description of the prompts on this display. You can use the following keys to help you edit the file and to select a mode of operation:

Key	What It Does
Cmd2	Starts Scan mode. Scan mode allows you to display a specific location profile. After you press command key 2, a display appears on which you can enter the remote location name for the location profile you want to display. When the location profile you requested is displayed, the SECEDIT COMM procedure is in Browse or Update mode so you can change information in that location profile. If the requested remote location name cannot be found, a message is displayed.

Cmd3 Starts Browse or Update mode and displays the first location profile. Browse or Update mode allows you to display, change, or remove location profiles. The SECEDIT COMM procedure begins in this mode after the user ID file contains location profiles.

You can display all the location profiles in the user ID file. You can change all the fields in the location profiles, including the remote location name field.

Cmd4 Removes a location profile from the user ID file. Command key 4 can be used only during Browse or Update mode.

After you display a location profile and press command key 4, a message warns you that the location profile will be removed from the file. Press the Enter key to remove the location profile. If you decide not to remove the location profile, press a roll key or any of the other allowed command keys to continue editing.

Cmd5 Starts Add mode. Add mode allows you to add new location profiles.

Because you are a master security officer, you can add location profiles to the user ID file.

When Add mode begins, a blank location profile (if one is available) is displayed. Type the location profile information and press the Enter key. The new location profile is added to the user ID file and another blank location profile is displayed (if one is available). Press an allowed command key to end Add mode or press command key 7 to end the SECEDIT COMM procedure.

As you add new location profiles, you might run out of blank location profiles. When that happens, you must increase the size of the user ID file, see "Changing the Size of the User ID File" later in this chapter.

Cmd6 Creates a random hexadecimal location password for you. If you press this key, then press the Enter key, a random hexadecimal location password is created for the location profile.

Cmd7 Ends the SECEDIT COMM procedure.

Roll keys The roll keys start Browse or Update mode. The roll keys page forward and backward through the location profiles.

Enter Can be used to enter information and page forward through the location profiles.

Help Can be used at any time to show information about the display you are viewing.

Listing the User ID File

You can use the SECLIST procedure to print or display information contained in the user ID file.

Listing User Profiles

How much user profile information you can print or display depends on:

- Whether password security is active
- Your security classification

If password security is active, you must be a security officer or a master security officer to use the SECLIST USERID procedure to list user profile information. A master security officer can list all user profile information in the user ID file; a security officer can list all user profile information in the file except the passwords and badge numbers of master security officers and security officers. If password security is active, user profile information in the user ID file can be requested from any display station.

If password security is not active, anyone can use the SECLIST USERID procedure to list user profile information, but the procedure can be run only from the system console. If you are listing user profile information and password security is not active, the password, badge number, service aid authorization, menu mandatory, procedure mandatory, and password last changed date information is not listed.

To list user profile information in the user identification file, do the following:

1. On the command display, type:

   SECLIST

   Press the Help key.

   The following display appears:

```
                              SECLIST PROCEDURE

          Lists the user identification or resource security file

Security information
  to be listed  . . . . . . . . . . USERID,RESOURCE,COMM,OFFICE  USERID

Print or display output . . . . . . . . . . . . . . PRINTER,CRT  PRINTER









Cmd3-Previous menu                                    COPR IBM Corp. 1986
```

S9042522

   You do not have to enter the security file type. USERID (the default value) indicates that user profiles in the user ID file are to be listed.

2. Type the device for the listing:

   PRINTER specifies that the output from the SECLIST USERID procedure is to be printed on the printer assigned to your display station. PRINTER is the default, and is already displayed.

   CRT specifies that the output is to be displayed on your display screen.

   Press the Enter key.

   The following display appears:

```
                              SECLIST PROCEDURE

          Lists the user identification or resource security file

Security information
  to be listed  . . . . . . . . . . USERID,RESOURCE,COMM,OFFICE  USERID

Print or display output . . . . . . . . . . . . . . PRINTER,CRT  PRINTER

Display passwords . . . . . . . . . . . . . . . . . . NOPW,PW  NOPW

List user profiles by . . . . . . . . . . . . . . USERID,CLASS  USERID









Cmd2-Page back      Cmd4-Put on job queue                  COPR IBM Corp. 1986
```

S9042523

3. Type one of the following to indicate whether you want to list passwords and badge numbers:

   NOPW specifies that passwords and badge numbers are not to be listed. NOPW is the default, and is already displayed.

   PW specifies that passwords and badge numbers can be listed if password security is active. If you are a master security officer, all passwords and badge numbers are listed. If you are a security officer, the printout includes the passwords and badge numbers of users that have a security classification of system console operator, subconsole operator, or display station operator.

4. Type one of the following to indicate the order you want the user profiles listed in:

   USERID specifies that the output is to be listed in alphabetic order by user ID. USERID is the default, and is already displayed.

   CLASS specifies that the output is to be listed in security classification order starting with master security officers. User IDs within each security classification are listed in alphabetic order.

   Press the Enter key.

The user profile information in the user ID file is printed or displayed on the device that you specified in step 2.

Sample Printout of User Profiles with Passwords Listed

This example shows the printout that is produced by the SECLIST USERID procedure if the master security officer chooses to list passwords. If the master security officer enters:

```
SECLIST USERID,PRINTER,PW,CLASS
```

When password security is active, the printout shown in Figure 2-1 is printed on the printer assigned to the display station where the master security officer is running the procedure. The user IDs within each security class are listed in alphabetic order. The printout on the following page is only a partial listing which shows the user profile information for two user IDs.

```
List of User Profiles
User ID         LAG535

User ID                                                          Comment
-------                                                          -------
LKS         Security Class . . .  Display Station Operator
            Password . . . . . . . . . . . . . . DE28            LISA K. SORENSON
               Password Last Changed . . . . . . 01/28/85        SALES REPRESENTATIVE
            Badge . . . . . . . . . . . . . . .                  EXT. 5551
            Service Aid Authority . . . . . . . No
            Sign-on Defaults:
               Library . . . . . . . . . . . . . SALESLIB
               User Menu . . . . . . . . . . . . SALESM
                  Mandatory . . . . . . . . . . No
               Procedure . . . . . . . . . . . . SALESP
                  Mandatory . . . . . . . . . . No
               Beginning Help Menu . . . . . . . MAIN


PHDEPT51    Security Class . . .  Display Station Operator
            Password . . . . . . . . . . . . . . 145L            PAUL HANSON
               Password Last Changed . . . . . . 01/06/85        DEPT. SUPERVISOR
            Badge . . . . . . . . . . . . . . .                  MANUFACTURING DEPT51
            Service Aid Authority . . . . . . . No
            Sign-on Defaults:
               Library . . . . . . . . . . . . . PLANTLIB
               User Menu . . . . . . . . . . . . PLANTM
                  Mandatory . . . . . . . . . . No
               Procedure . . . . . . . . . . . . PLANTP
                  Mandatory . . . . . . . . . . No
               Beginning Help Menu . . . . . . . MAIN


Master Security Officers                    2
Security Officers                           1
System Operators                            1
Subconsole Operators                        1
Display Station Operators                   3
                                          -----
Total User Profiles                         8

Other Profiles                              0
                                          -----
Total Profiles Used                         8

Available Profiles                         10
                                          -----
Total Profiles Defined                     18

File Size in Blocks                         1
```

Figure 2-1. Sample Printout of User Profiles with Passwords Listed

Sample Printout of User Profiles when Password Security Is Not Active

This example shows the printout that is produced by the SECLIST USERID procedure if the procedure is entered from the system console when password security is not active. If the user enters:

```
SECLIST USERID,PRINTER,NOPW
```

The printout shown in Figure 2-2 is printed on the printer assigned to the system console.

```
List of User Profiles
User ID          LAG535

User ID                                                        Comment
-------------
PETER       Sign-on Defaults:
               Library  . . . . . . . . . . . . . . . PAY.LIB1      PETER SMITH
               User Menu  . . . . . . . . . . . . .                 MANAGER, DEPT. 436
               Procedure  . . . . . . . . . . . . . PAYSETUP        EXT. 2206
               Beginning Help Menu  . . . . . . . . MAIN

PHDEPT51    Sign-on Defaults:
               Library  . . . . . . . . . . . . . . . PLANTLIB      PAUL HANSON
               User Menu  . . . . . . . . . . . . . . PLANTM        DEPT. SUPERVISOR
               Procedure  . . . . . . . . . . . . . . PLANTP        MANUFACTURING DEPT51
               Beginning Help Menu  . . . . . . . . MAIN

Total User Profiles                                    8
Other Profiles                                         0
-------------------------------------------------------
Total Profiles Used                                    8
Available Profiles                                    10
-------------------------------------------------------
Total Profiles Defined                                18
File Size in Blocks                                    1
```

Figure 2-2. Sample Printout of User Profiles when Password Security Is Not Active

Description of User Profile Entries on the User ID File Printouts

Figure 2-1 and Figure 2-2 show sample printouts of user profiles in the user ID file. The following entries are found on those printouts:

User ID indicates the user ID of each user.

Security Class indicates the security classification of each user. Security classifications are:

Master security officer

Security officer

System console operator

Subconsole operator

Display station operator

Password indicates the password of each user.

Password Last Changed indicates the date the user last changed his or her password. If the user ID is *NULL, the date the user last changed his or her password does not apply and is not listed.

Badge indicates the badge number of each user if badge security is active.

Service Aid Authority indicates whether the user can run service aid procedures.

Sign-On Defaults indicates the sign-on defaults for this user:

Library indicates the name of the library that is automatically used as the session library when the user signs on.

User Menu indicates the name of the menu that is automatically displayed when the user signs on.

Mandatory indicates whether this user menu is a mandatory menu for this user.

Procedure indicates the name of the procedure that is automatically run when the user signs on.

Mandatory indicates whether this procedure is a mandatory procedure for this user.

Beginning Help Menu indicates the name of the beginning help menu of each user.

Comment indicates any additional information entered in the user's profile.

Master Security Officers indicates the number of master security officers.

Security Officers indicates the number of security officers.

System Operators indicates the number of system console operators.

Subconsole Operators indicates the number of subconsole operators.

Display Station Operators indicates the number of display station operators.

Total User Profiles indicates the total number of user profiles in the user ID file.

Other Profiles indicates the number of location profiles in the user ID file.

Total Profiles Used indicates the total number of profiles in the user ID file that contain information.

Available Profiles indicates the number of profiles that are available in the user ID file.

Total Profiles Defined indicates the number of profiles in the file. This number includes used and available user and location profiles.

File Size in Blocks indicates the number of disk blocks the user ID file is using.

Listing Location Profiles

Password security must be active to run the SECLIST COMM procedure. The SECLIST COMM procedure can be run from any display station but only by a master security officer. A master security officer can list all location profiles in the user ID file.

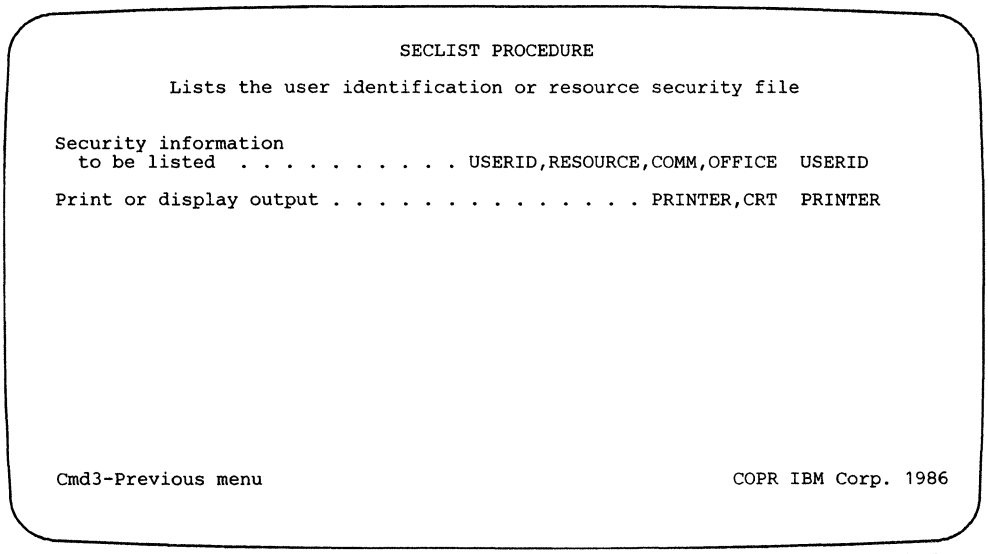
To list location profile information in the user identification file, do the following:

1. On the command display, type:

   ```
   SECLIST
   ```

   Press the Help key.

   The following display appears:



S9042524

   Because you want to list location profiles, replace USERID with COMM.

2. Type the device for the listing:

   PRINTER specifies that the output from the SECLIST COMM procedure is to be printed on the printer assigned to your display station. PRINTER is the default, and is already displayed.

   CRT specifies that the output is to be displayed on your display screen.

   Press the Enter key.

The location profile information in the user ID file is printed or displayed on the device that you specified in step 2.

Sample Printout of Location Profiles

This example shows the printout that is produced by the SECLIST COMM procedure. If a master security officer enters:

```
SECLIST COMM,PRINTER
```

The printout shown in Figure 2-3 is printed on the printer assigned to the display station where the master security officer is running the procedure.

```
Communications Security
User ID       LAG535

Location        Location          Require User Password
  Name          Password          for Starting a Proc        Comment
--------  ----------------------  -------------------  ----------------------
AUSTIN    3B963C562FA7CAC7                Y            PROGRAMMING CENTER
                                                       HILTON BLDG.
                                                       AUSTIN, TEXAS

CHICAGO   9B234A759E965B67                Y            WAREHOUSE
                                                       123 FOURTH STREET NW
                                                       CHICAGO, ILLINOIS

LONDON    726C0BBD098DA2AE                N            DISTRIBUTION
                                                       #2 WESTMINSTER ST.
                                                       LONDON, ENGLAND

NEWYORK   C9C3621460E4FA04                N            PAYROLL
                                                       325 FIFTH AVE.
                                                       NEW YORK, NY


                          Total location profiles listed     4

                          Records Defined                   38

                          File Size in Blocks                2
```

Figure 2-3. Sample Printout of Location Profiles

Description of Location Profile Entries on User ID File Printout

Figure 2-3 shows a sample printout of location profiles in the user ID file. The following entries are found on those printouts:

Location Name indicates the name of the remote location.

Location Password indicates the password that must be exchanged with the remote location.

Require User Password for Starting a Proc indicates whether a valid user password is required for another system to start a procedure on your system.

Comment indicates any additional information entered in the location profile.

Total Location Profiles Listed indicates the total number of location profiles listed. This is the number of location profiles in the user ID file.

Records Defined indicates the maximum number of records in the file. This number indicates the maximum number of user profiles and location profiles that the file can contain.

File Size in Blocks indicates the number of disk blocks the user ID file is using.

Saving the User ID File

The SECSAVE procedure allows you to copy the user ID file onto diskette or tape, or onto another area on disk. You should consider making a copy of the user ID file in case the original user ID file is somehow damaged or destroyed. The extra copies allow you to easily recover from intentional or unintentional destruction of your security information.

If password security is active, only a master security officer can run the SECSAVE procedure (the procedure can be run from any display station).

If password security is not active, anyone can run the SECSAVE procedure, but only from the system console.

Saving Copies on Diskette

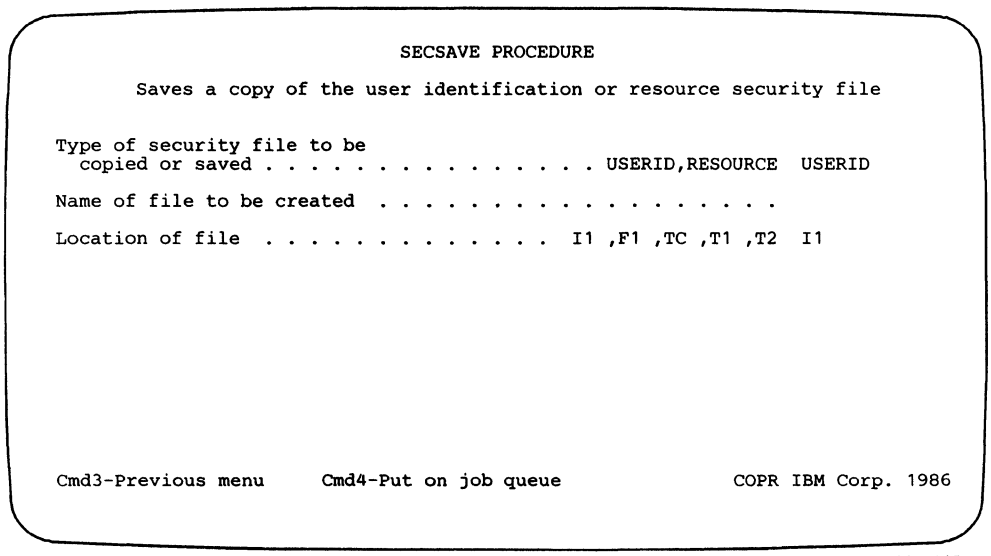
To copy the user ID file onto diskette, do the following:

1. On the command display, type:

   ```
   SECSAVE
   ```

   Press the Help key.

   The following display appears:



S9042525

2. You do not have to enter the type of security file you want to copy. USERID (the default value) indicates that the user ID file is to be copied.

3. Type a name for the file to be created. For example, you could call the copy USERFILE (user ID file).

4. You do not have to type the location of the file. I1 (the default value) indicates that the file is to be copied onto diskette.

   Press the Enter key.

   The following display appears:

```
                              SECSAVE PROCEDURE

        Saves a copy of the user identification or resource security file

Type of security file to be
  copied or saved . . . . . . . . . . . . . . . USERID,RESOURCE  USERID

Name of file to be created  . . . . . . . . . . . . . . . . . . USERFILE

Location of file  . . . . . . . . . . . . . . I1 ,F1 ,TC ,T1 ,T2  I1

Volume ID of diskette . . . . . . . . . . . . . . . . . . . . .

Retention days  . . . . . . . . . . . . . . . . . . . . . . . . 1-999  999

Location of diskette  . . . . . . . . . . . . S1,S2,S3,M1.nn,M2.nn  S1

Automatic advance to next slot or magazine  . . . . NOAUTO,AUTO  NOAUTO



Cmd2-Page back      Cmd4-Put on job queue                  COPR IBM Corp. 1986
```

S9042526

5. Type the following information:

   a. The volume ID of the diskette that is to receive the copy. A volume ID must be specified.
   b. The number of days the diskette file is to be retained, any decimal number from 1 through 999. If you do not specify the number of retention days, 999 days are assumed. If 999 days are entered or assumed, the file is a permanent diskette file.
   c. The diskette slot or diskette magazine location containing the first diskette to be used. Any of the following can be specified:

      S1, S2, or S3 specifies the diskette slot containing the first diskette to be used.

      M1.nn or M2.nn specifies the magazine location containing the first diskette to be used. M1 indicates the first magazine location, and M2 indicates the second magazine location. **nn** is a decimal number from 01 through 10 that identifies the location of the diskette in the magazine. Specifying M1 is the same as specifying M1.01; specifying M2 is the same as specifying M2.01.

d. Whether the system is to automatically advance to the next diskette slot or magazine location. You can specify either AUTO or NOAUTO:

NOAUTO specifies the following:

1) If S1, S2, or S3 is specified, only the specified slot (S1, S2, or S3) is used. If more diskettes need to be processed, a message is displayed and you must insert the next diskette into the slot being used.
2) If M1.nn or M2.nn is specified, only the specified magazine location (M1 or M2) is used. Processing begins with the diskette at the specified location within the magazine and continues through the last diskette in the magazine. If more diskettes need to be processed, a message is displayed and you must then insert the next magazine in the magazine location being used. Processing resumes at the first diskette location in the magazine.

AUTO specifies the following:

1) If S1, S2, or S3 is specified, all three slots (S1, S2, and S3) are used. Processing begins with the diskette in the specified slot and continues through the diskette in slot S3. If more diskettes need to be processed, a message is displayed and you must then insert the next diskettes. Processing resumes with the diskette in slot S1.
2) If M1.nn or M2.nn is specified, both magazine locations (M1 and M2) are used. Processing begins with the diskette at the specified location and continues through the diskette in location M2.10. If more diskettes need to be processed, a message is displayed and you must then insert the next magazines. Processing resumes at location M1.01 and continues through M2.10.

Press the Enter key.

The SECSAVE procedure copies the user ID file onto diskette, and the procedure ends.

Example of Copying the User ID File on Diskette

This example shows the procedure and parameters a master security officer can use to copy the user ID file onto diskette. The volume ID of the diskette is VOL001, and the diskette is located in diskette slot S1. The name of the diskette file is USERFILE; the diskette file will be retained for 60 days.

```
SECSAVE USERID,USERFILE,I1,VOL001,60,S1,NOAUTO
```

Saving Copies on Tape or Tape Cartridge

To copy the user ID file onto tape or tape cartridge, do the following:

1. On the command display, type:

   SECSAVE

   Press the Help key.

   The following display appears:

```
                              SECSAVE PROCEDURE

       Saves a copy of the user identification or resource security file

Type of security file to be
  copied or saved . . . . . . . . . . . . . . . USERID,RESOURCE  USERID

Name of file to be created  . . . . . . . . . . . . . . . . . . .

Location of file  . . . . . . . . . . . . . .  I1, F1 ,TC ,T1 ,T2  I1




Cmd3-Previous menu     Cmd4-Put on job queue                COPR IBM Corp. 1986
```

S9042527

2. You do not have to enter the type of security file you want to copy. USERID (the default value) indicates that the user ID file is to be copied.

3. Type a name for the file to be created. For example, you could call the copy USERFILE (user ID file).

4. Type T1 to specify that the file is to be copied onto a tape on the first tape drive, T2 to specify that the file is to be copied onto a tape on the second tape drive, or TC to specify that the file is to be copied onto a tape cartridge. You must type over the system default shown.

   Press the Enter key.

   The following display appears:

```
                              SECSAVE PROCEDURE

        Saves a copy of the user identification or resource security file

Type of security file to be
  copied or saved . . . . . . . . . . . . . . . USERID,RESOURCE  USERID

Name of file to be created  . . . . . . . . . . . . . . . . . . USERFILE

Location of file  . . . . . . . . . . . . .  I1 ,F1 ,TC ,T1 ,T2  T1

Volume ID of tape . . . . . . . . . . . . . . . . . . . . . . .

Retention days  . . . . . . . . . . . . . . . . . . . . . . . . 1-999  999

Automatic advance to next tape drive  . . . . . . . NOAUTO,AUTO  NOAUTO

End position of tape drive  . . . . . . . . . REWIND,LEAVE,UNLOAD  REWIND


Cmd2-Page back      Cmd4-Put on job queue                    COPR IBM Corp. 1986
```

S9042528

5. Type the following information:

   a. The volume ID of the tape or tape cartridge that is to receive the copy. A volume ID must be specified.
   b. The number of days the tape or tape cartridge file is to be retained, any decimal number from 1 through 999. If you do not specify the number of retention days, 999 days are assumed. If 999 days are entered or assumed, the file is a permanent tape file.
   c. Whether the system is to automatically advance to the next tape drive if the end of the first tape is reached:

      NOAUTO specifies that if the end of the tape is reached on the selected tape drive, processing continues with the same tape drive. If more tapes need to be processed, a message is displayed and you must then mount the next tape on the selected tape drive.

      AUTO specifies that both tape drives can be used. If the end of the tape is reached on the selected tape drive, processing continues with the tape on the other tape drive. If the other drive is not available, the first drive is used again. If more tapes need to be processed, a message is displayed and you must then mount the next tape on the appropriate tape drive.

      Note: NOAUTO, the system default value, must be used if you are saving the user ID file on a tape cartridge.

   d. The end position of the tape drive after the user ID file is copied. Any of the following can be specified:

      REWIND rewinds the tape to the beginning of the tape.

      LEAVE leaves the tape positioned at the end of the copied security file.

      UNLOAD rewinds the tape to the beginning and unloads the tape.

      Note: UNLOAD is not valid if you are saving the user ID file on a tape cartridge.

   Press the Enter key.

   The SECSAVE procedure copies the user ID file onto tape or tape cartridge, and the procedure ends.

Example of Copying the User ID File on Tape

This example shows the procedure and parameters a master security officer can use to copy the user ID file onto tape. The name of the tape file is USERFILE, the file will be copied to the tape on the first tape drive, both tape drives can be used if necessary, and the system will leave the tape positioned after the copied file.

```
SECSAVE USERID,USERFILE,T1,VOL001,999,,AUTO,LEAVE
```

Saving Copies on Disk

To copy the user ID file onto another area on disk, do the following:

1. On the command display, type:

   ```
   SECSAVE
   ```

   Press the Help key.

   The following display appears:

```
                              SECSAVE PROCEDURE

        Saves a copy of the user identification or resource security file

Type of security file to be
  copied or saved . . . . . . . . . . . . . . . USERID,RESOURCE  USERID

Name of file to be created  . . . . . . . . . . . . . . . . . . .

Location of file  . . . . . . . . . . . . . .  I1 ,F1 ,TC ,T1 ,T2  I1









Cmd3-Previous menu      Cmd4-Put on job queue                 COPR IBM Corp. 1986
```

S9042529

2. You do not have to enter the type of security file you want to copy. USERID (the default value) indicates that the user ID file is to be copied.

3. Type a name for the file to be created. For example, you could call the copy USERFILE (user ID file).

4. Type F1 to specify that the file is to be copied to another area on disk. You must type over the system default shown.

Press the Enter key.

The SECSAVE procedure copies the user ID file onto another area on disk, and the procedure ends.

Example of Copying the User ID File to Another Area on Disk

This example shows the procedure and parameters the master security officer can use to copy the user ID file into a disk file. The name of the disk file is USERFILE.

```
SECSAVE USERID,USERFILE,F1
```

Restoring the User ID File

The SECREST procedure restores the user ID file with the copy that was created by the SECSAVE procedure. When restoring the user ID file, it is not necessary to deactivate password security, activate password security, or perform an IPL. The user ID file that is currently on disk is replaced with the version created by the SECSAVE procedure.

If password security is active, only a master security officer can run the SECREST procedure from any display station.

If password security is not active, anyone can run the SECREST procedure, but only from the system console.

Restoring Copies from Diskette

To restore the user ID file from diskette, do the following:

1. On the command display, type:

   SECREST

   Press the Help key.

   The following display appears:

```
                          SECREST PROCEDURE                    Optional-*
          Restores the user identification or resource security file

Security file to restore  . . . . . . . . . . . USERID,RESOURCE  USERID
Name of file to be restored . . . . . . . . . . . . . . . . . .
Size of file in records . . . . . . . . . . . . . . . . . . . .          *
Creation date of file to be restored  . . . . . . . . . . . . .          *
Location of file  . . . . . . . . . . . . . I1 ,F1 ,TC ,T1 ,T2  I1




Cmd3-Previous menu                                   COPR IBM Corp. 1986
```

   S9042530

2. You do not have to enter the type of security file you want to restore. USERID (the default value) indicates that the user ID file is to be restored.

3. Type the following information:

   a. The name of the diskette file that contains the copy of the user ID file that was created by the SECSAVE procedure. If the specified file does not contain a copy of a user ID file, an error message is displayed.
   b. The number of records to allow in the newly restored user ID file. This number can be any decimal number from 18 through 3998. If no number is specified, the number of records that were copied is used. If the number entered is too large for the system, or too small to contain all the copied records, an error message is displayed.

      Note: The number of records in the newly restored user ID file might differ slightly from the number you specify. That is because the system rounds the number of records to the next greatest multiple of 20, and then subtracts 2. For example, if you specify 165 records, the actual number of records in the file will be 178 (that is, 180 - 2).

   c. The creation date of the diskette file that contains the copied user ID file. If no creation date is specified, and if more than one diskette file exists with the specified file name, the first (oldest) file is used.

      *Note: The creation date entered must be in the current session date format, either month-day-year (**mmddyy**), day-month-year (**ddmmyy**), or year-month-day (**yymmdd**). You can use the STATUS SESSION command to determine the session date format.*

   d. You do not have to type the location of the file. I1 (default value) indicates that the file is to be copied from diskette.

   Press the Enter key.

   The following display appears:

```
                          SECREST PROCEDURE                    Optional-*
          Restores the user identification or resource security file

Security file to restore  . . . . . . . . . . . USERID,RESOURCE  USERID
Name of file to be restored . . . . . . . . . . . . . . . . . .  USERFILE
Size of file in records . . . . . . . . . . . . . . . . . . . .  100        *
Creation date of file to be restored  . . . . . . . . . . . . .            *
Location of file  . . . . . . . . . . . . . I1 ,F1 ,TC ,T1 ,T2  I1
Volume ID of diskette . . . . . . . . . . . . . . . . . . . . .            *
Location of diskette  . . . . . . . . . . . S1,S2,S3,M1.nn,M2.nn  S1
Automatic advance to next slot or magazine  . . . . AUTO,NOAUTO  NOAUTO
Update password last changed date . . . . . . . NOUPDATE,UPDATE  NOUPDATE

Cmd2-Page back     Cmd4-Put on job queue                COPR IBM Corp. 1986
```

S9042531

4. Type the following information:

   a. The volume ID of the diskette that contains the copied user ID file. If no volume ID is specified, the file is copied from the diskette in the specified location.
   b. The diskette slot or diskette magazine location containing the first diskette to be used. Any of the following can be specified:

      S1, S2, or S3 specifies the diskette slot containing the first diskette to be used.

      M1.nn or M2.nn specifies the magazine location containing the first diskette to be used. M1 indicates the first magazine location, and M2 indicates the second magazine location. **nn** is a decimal number from 01 through 10 that identifies the location of the diskette in the magazine. Specifying M1 is the same as specifying M1.01; specifying M2 is the same as specifying M2.01.

   c. Whether the system is to automatically advance to the next diskette slot or magazine location. You can specify either AUTO or NOAUTO:

      NOAUTO specifies the following:
      1) If S1, S2, or S3 is specified, only the specified slot (S1, S2, or S3) is used. If more diskettes need to be processed, a message is displayed and you must then insert the next diskette into the slot being used.
      2) If M1.nn or M2.nn is specified, only the specified magazine location (M1 or M2) is used. Processing begins with the diskette at the specified location within the magazine and continues through the last diskette in the magazine. If more diskettes need to be processed, a message is displayed and you must insert the next magazine in the magazine location being used. Processing resumes at the first location in the magazine.

      AUTO specifies the following:
      1) If S1, S2, or S3 is specified, all three slots (S1, S2, and S3) are used. Processing begins with the diskette in the specified slot and continues through the diskette in slot S3. If more diskettes need to be processed, a message is displayed and you must then insert the next diskettes. Processing resumes with the diskette in slot S1.
      2) If M1.nn or M2.nn is specified, both magazine locations (M1 and M2) are used. Processing begins with the diskette at the specified location and continues through the diskette in location M2.10. If more diskettes need to be processed, a message is displayed and you must then insert the next magazines. Processing resumes at location M1.01 and continues through M2.10.

d. Whether the system is to update the *Date the password last changed* field.

UPDATE specifies that the *Update password last changed date* field in every user profile is to be set to the current system date.

NOUPDATE specifies that the *Update password last changed date* field will not be changed. Only dates that are zeroes are updated to contain the current system date. Other profiles are not changed. NOUPDATE is the default, and is already specified.

Press the Enter key.

The user ID file is restored by the SECREST procedure, the procedure ends, and a message is sent to the system console indicating that the user ID file was restored.

Example of Restoring the User ID File from Diskette

This example shows the procedure and parameters a master security officer can use to restore the user ID file from a copy on diskette. The name of the diskette file is USERFILE, the size of the user ID file is 200 records, the volume ID of the diskette is VOL001, and the diskette is located in diskette slot S1. The user profile will be updated with the current system date.

```
SECREST USERID,USERFILE,200,,I1,VOL001,S1,NOAUTO,UPDATE
```

Restoring Copies from Tape or Tape Cartridge

To restore the user ID file from tape or tape cartridge, do the following:

1. On the command display, type:

   SECREST

   Press the Help key.

   The following display appears:

```
                          SECREST PROCEDURE                    Optional-*
          Restores the user identification or resource security file

Security file to restore  . . . . . . . . . . . USERID,RESOURCE  USERID
Name of file to be restored . . . . . . . . . . . . . . . . . .
Size of file in records . . . . . . . . . . . . . . . . . . . .           *
Creation date of file to be restored  . . . . . . . . . . . . .           *
Location of file  . . . . . . . . . . . . . .  I1 ,F1 ,TC ,T1 ,T2  I1




Cmd3-Previous menu                                    COPR IBM Corp. 1986
```

S9042532

2. You do not have to enter the type of security file you want to restore. USERID (the default value) indicates that the user ID file is to be restored.

3. Type the following information:

   a. The name of the file that contains the copy of the user ID file that was created by the SECSAVE procedure. If the specified file does not contain a copy of a user ID file, an error message is displayed.
   b. The number of records to allow in the newly restored user ID file. This number can be any decimal number from 18 through 3998. If no number is specified, the number of records that were copied is used. If the number entered is too large for the system, or too small to contain all the records, an error message is displayed.

      Note: The number of records in the newly restored user ID file might differ slightly from the number you specify. That is because the system rounds the number of records to the next greatest multiple of 20, and then subtracts 2. For example, if you specify 165 records, the actual number of records in the file will be 178 (that is, 180 - 2).

c. The creation date of the tape or tape cartridge file that contains the copied user ID file. If no creation date is specified, and if more than one tape or tape cartridge file exists with the specified file name, the first (oldest) file is used.

   *Note: The creation date entered must be in the current session date format, either month-day-year (**mmddyy**), day-month-year (**ddmmyy**), or year-month-day (**yymmdd**). You can use the STATUS SESSION command to determine the session date format.*

d. T1 to specify that the file is to be copied from a tape on the first tape drive, T2 to specify that the file is to be copied from a tape on the second tape drive, or TC to specify that the file is to be copied from a tape cartridge. You must type over the system default shown.

Press the Enter key.

The following display appears:

```
                          SECREST PROCEDURE                    Optional-*
          Restores the user identification or resource security file

Security file to restore  . . . . . . . . . . . USERID,RESOURCE  USERID
Name of file to be restored . . . . . . . . . . . . . . . . . .  USERFILE
Size of file in records . . . . . . . . . . . . . . . . . . . .  100        *
Creation date of file to be restored  . . . . . . . . . . . . .            *
Location of file  . . . . . . . . . . . . . . I1 ,F1 ,TC ,T1 ,T2  T1
Volume ID of tape . . . . . . . . . . . . . . . . . . . . . . .            *
Automatic advance to next tape drive  . . . . . . . AUTO,NOAUTO  NOAUTO
End position of tape drive  . . . . . . . . REWIND,LEAVE,UNLOAD  REWIND
Update password last changed date . . . . . . . NOUPDATE,UPDATE  NOUPDATE
Cmd2-Page back     Cmd4-Put on job queue                 COPR IBM Corp. 1986
```

S9042533

Note: If your system has a tape cartridge, the default for the location of the file is TC instead of T1.

4. Type the following information:

   a. The volume ID of the tape or tape cartridge that contains the copied user ID file. If no volume ID is specified, the file is copied from the tape in the specified location.
   b. Whether the system is to automatically advance to the next tape drive if the end of the first tape is reached:

      NOAUTO specifies that if the end of the tape is reached on the selected tape drive, processing continues on the same tape drive. If more tapes need to be processed, a message is displayed and you must then mount the next tape on the selected tape drive.

      Note: NOAUTO, the system default value, must be used if you are restoring the user ID file from a tape cartridge.

      AUTO specifies that both tape drives can be used. If the end of the tape is reached on the selected tape drive, processing continues with the tape on the other tape drive. If the other drive is not available, the first drive is used again. If more tapes need to be processed, a message is displayed and you must then mount the next tape on the tape drive.

   c. The end position of the tape drive after the user ID file is restored. Any of the following can be specified:

      REWIND rewinds the tape to the beginning of the tape.

      LEAVE leaves the tape positioned at the end of the restored user ID file.

      UNLOAD rewinds the tape to the beginning and unloads the tape.

      Note: UNLOAD is not valid if you are restoring the user ID file from a tape cartridge.

   d. Whether the system is to update the *Date the password last changed* field.

      UPDATE specifies that the *Update password last changed date* field in every user profile is to be set to the current system date.

      NOUPDATE specifies that the *Update password last changed date* field will not be changed. Only dates that are zeroes are updated to contain the current system date. Other profiles are not changed.

   Press the Enter key.

   The user ID file is restored by the SECREST procedure, the procedure ends, and a message is sent to the system console indicating that the user ID file was restored.

Example of Restoring the User ID File from Tape

This example shows the procedure and parameters a master security officer can use to restore the user ID file from tape. The name of the tape file is USERFILE, the size of the restored user ID file is to be 200 records, its creation date is December 4, 1983, the file is to be restored from the tape on the first tape drive, both tape drives can be used if necessary, and the system will leave the tape positioned after the restored file. The user profile will be updated with the current system date.

```
SECREST USERID,USERFILE,200,120483,T1,,,AUTO,LEAVE,UPDATE
```

Restoring Copies from Disk

To restore the user ID file from disk, do the following:

1. On the command display, type:

   SECREST

   Press the Help key.

   The following display appears:

```
                              SECREST PROCEDURE                    Optional-*
          Restores the user identification or resource security file

Security file to restore . . . . . . . . . . . USERID,RESOURCE  USERID
Name of file to be restored . . . . . . . . . . . . . . . . . .
Size of file in records . . . . . . . . . . . . . . . . . . . .          *
Creation date of file to be restored . . . . . . . . . . . . .           *
Location of file . . . . . . . . . . . . . . I1 ,F1 ,TC ,T1 ,T2  I1




Cmd3-Previous menu                                    COPR IBM Corp. 1986
```

S9042534

2. You do not have to enter the type of security file you want to restore. USERID (the default value) indicates that the user ID file is to be restored.

3. Type the following information:

   a. The name of the disk file that contains the copy of the user ID file that was created by the SECSAVE procedure. If the specified file does not contain a copy of a user ID file, an error message is displayed.
   b. The number of records to allow in the newly restored user ID file. This number can be any decimal number from 18 through 3998. If no number is specified, the number of records that were copied is used. If the number entered is too large for the system, or too small to contain all the records, an error message is displayed.

      Note: The number of records in the newly restored user ID file might differ slightly from the number you specify. That is because the system rounds the number of records to the next greatest multiple of 20, and then subtracts 2. For example, if you specify 165 records, the actual number of records in the file will be 178 (that is, 180 - 2).

   c. The creation date of the disk file that contains the copied user ID file. If no creation date is specified, and if more than one disk file exists with the specified file name, the first (oldest) file is used.

      *Note: The creation date entered must be in the current session date format, either month-day-year (**mmddyy**), day-month-year (**ddmmyy**), or year-month-day (**yymmdd**). You can use the STATUS SESSION command to determine the session date format.*

   d. F1 to specify that the file is to be copied from a disk file.

   Press the Enter key.

   The SECREST procedure restores the user ID file, the procedure ends, and a message is sent to the system console indicating that the user ID file was restored.

4. Whether the system is to update the *Date the password last changed* field.

   UPDATE specifies that the *Update password last changed date* field in every user profile is to be set to the current system date.

   NOUPDATE specifies that the *Update password last changed date* field will not be changed. Only dates that are zeroes are updated to contain the current system date. Other profiles are not changed.

Example of Restoring the User ID File from a Disk File

This example shows the procedure and parameters a master security officer can use to restore the user ID file from a disk file. The name of the disk file is USERFILE, the size of the restored user ID file is to be 200 records, and its creation date is December 4, 1984. Because neither UPDATE nor NOUPDATE is specified, the default (NOUPDATE) is used.

```
SECREST USERID,USERFILE,200,120484,F1
```

Changing the Size of the User ID File

You can increase the size of the user ID file if you want to. However, the system will increase the size of the user ID file when all the blank records are used, providing there is enough disk space available and the user ID file has not reached its maximum allowable size (3998 records).

At some point, you might need to make available a certain amount of disk space. You can do so by decreasing the size of the user ID file. You can decrease the size of the user ID file by removing profiles you no longer need, then following these steps:

1. Run the SECDEF procedure to determine the current size of the user ID file. Enter the following:

   ```
   SECDEF USERID,CREATE
   ```

   The size of the user ID file is displayed. Press command key 3 to end the SECDEF procedure.

2. Run the SECSAVE procedure to copy the user ID file onto a temporary disk file. For example:

   ```
   SECSAVE USERID,TEMPUSER,F1
   ```

   See "Saving the User ID File" earlier in this chapter for more information about the SECSAVE procedure.

3. Run the SECREST procedure to restore the temporary file back to the user ID file. When you run the SECREST procedure, you can specify a new size for the user ID file. To increase the size of the file, specify a number of records greater than the number of records contained in the original user ID file. To decrease the size of the file, specify a number of records fewer than the number of records contained in the original user ID file. If the specified size is too small to hold all the records in the file, a message is displayed with an option to make the file just large enough to contain the records.

   For example, if the current size is 100, you can increase that size to 165 by entering the following:

   ```
   SECREST USERID,TEMPUSER,165,,F1
   ```

   Note: The number of records in the newly restored user ID file might differ slightly from the number you specified in the SECREST procedure. That is because the system rounds the number of records to the next greatest multiple of 20, and then subtracts 2. For example, if you specify 165 records, the actual number of records in the file will be 178 (that is, 180 - 2).

   For more information about the SECREST procedure, see "Restoring the User ID File" earlier in this chapter.

4. Use the DELETE procedure to remove the temporary file from the system. For example:

```
DELETE TEMPUSER,F1
```

The DELETE procedure removes files from the system. For more information about the DELETE procedure, see the manual, *System Reference*.

Deactivating Password Security

If you deactivate password security, the user ID file remains on disk and information in the file is unchanged.

When password security is deactivated, anyone can sign on to your system; therefore, you should carefully evaluate whether unauthorized access to your system might cause you problems.

When password security is not active:

- You no longer have badge security, communications security, and menu security.
- The SECEDIT USERID and SECEDIT COMM procedures cannot be used to add, change, or display certain information in the user ID file.
- The SECLIST USERID and SECLIST COMM procedures cannot be used to list certain information in the user ID file.

These restrictions ensure that vital security information cannot be changed or viewed when password security is not active.

Password security can be deactivated by running the SECDEF procedure. Only a master security officer can run the SECDEF procedure from any display station to deactivate password security.

To deactivate password security, do the following:

1. On the command display, type:

   SECDEF

   Press the Help key.

   The following display appears:

```
                              SECDEF PROCEDURE

            Creates or removes the user identification file; creates
            or removes the resource security file; or activates
            or deactivates password, resource, or badge security.

Security type . . . . . . . . . . . . . . . . . USERID,RESOURCE  USERID




Cmd3-Previous menu                                        COPR IBM Corp. 1985
```

S9042535

2. On the display shown in step 1, the system asks you for the type of security file that you want to work with. The system has already filled in USERID for the security file type. Because password security uses the user ID file, press the Enter key.

   The following display appears:

```
                              SECDEF PROCEDURE

            Creates or removes the user identification file; creates
            or removes the resource security file; or activates
            or deactivates password, resource, or badge security.


Security type . . . . . . . . . . . . . . . . . . USERID,RESOURCE  USERID

Option  . . . . . . . . . . . . . . . . . . . . . ACTBDG,ACTPW,CREATE
                    DEACTBDG,DEACTPW,DELETE,STRTDATE,STOPDATE              *









Cmd2-Page back                                          COPR IBM Corp. 1985
```

S9042536

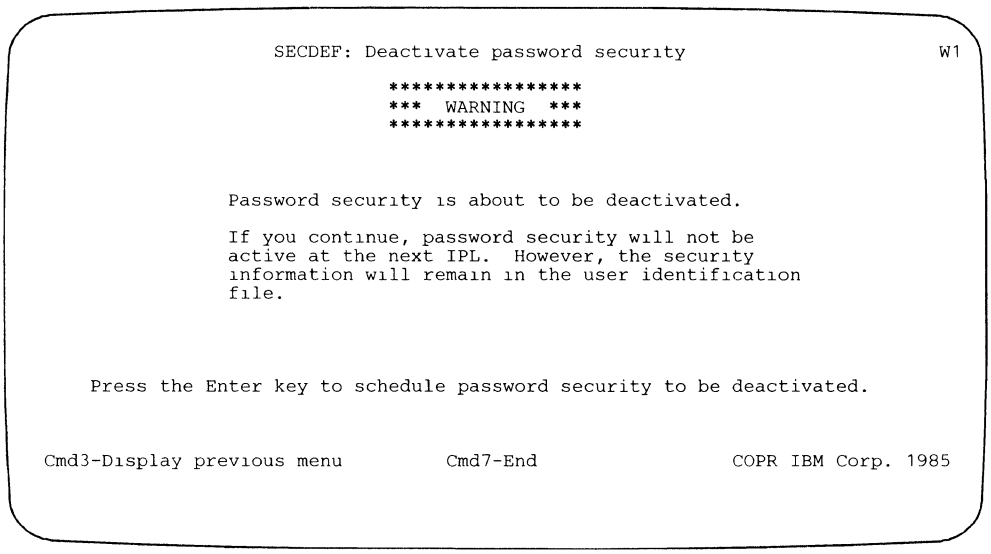
3. Using the display shown in step 2, you can choose one of several tasks:

   Activate badge security
   Activate password security
   Create the user ID file
   Deactivate badge security
   Deactivate password security
   Delete the user ID file
   Start the date checking function
   Stop the date checking function

   Because you want to deactivate password security, type DEACTPW, and press the Enter key.

   Note: Remember that badge security requires that password security be active. Therefore, if you attempt to deactivate password security but you have not yet deactivated badge security, a message is displayed that lets you deactivate badge security or cancel the request.

   The following display appears:



S9042537

4. If you decide not to deactivate password security, press command key 7. The SECDEF procedure does not deactivate password security, and the procedure ends.

   To deactivate password security, press the Enter key. The system displays a message indicating that password security will be deactivated at the next IPL. To complete the SECDEF procedure, press command key 3 or the Enter key.

Password security (and if required, badge security) will be deactivated after an IPL of the system is performed. For information on how to perform an IPL, see the manuals, *Operating Your System* and *Using Your Display Station.*

Stopping the Password Date Checking Function

When the password date checking function is stopped, users are no longer required to change their passwords. You must be a master security officer to stop the password date checking function.

To stop the password date checking function, do the following:

1. On the command display, type:

   SECDEF

   Press the Help key.

   The following display appears:

```
                              SECDEF PROCEDURE

            Creates or removes the user identification file; creates
            or removes the resource security file; or activates
            or deactivates password, resource, or badge security.

Security type . . . . . . . . . . . . . . . . . USERID,RESOURCE  USERID




Cmd3-Previous menu                                        COPR IBM Corp. 1985
```

S9042609

2. On the display shown in step 1, the system asks you for the type of security file that you want to work with. The system has already filled in USERID for the security file type. Because the password date checking function uses the user ID file, press the Enter key.

   The following display appears:

```
                              SECDEF PROCEDURE

            Creates or removes the user identification file; creates
            or removes the resource security file; or activates
            or deactivates password, resource, or badge security.


Security type . . . . . . . . . . . . . . . . . . USERID,RESOURCE  USERID

Option  . . . . . . . . . . . . . . . . . . . . . ACTBDG,ACTPW,CREATE
                      DEACTBDG,DEACTPW,DELETE,STRTDATE,STOPDATE              *









Cmd2-Page back                                          COPR IBM Corp. 1985
```

S9042610

3. Using the display shown in step 2, you can choose one of several tasks:

   Activate badge security
   Activate password security
   Create the user ID file
   Deactivate badge security
   Deactivate password security
   Delete the user ID file
   Start the date checking function
   Stop the date checking function

   Because you want to stop the password date checking function, type STOPDATE, and press the Enter key.

   The following display appears:

```
                    SECDEF : Stop password date checking                W1

                Password date checking is about to be stopped.

                If you continue, password date checking will
                be stopped.  However, the password change date
                information will remain in the user profiles
                in the user identification file.  No IPL is
                necessary to stop password date checking.


              Press the Enter key to stop password date checking.




Cmd3-Display previous menu          Cmd7-End          COPR IBM Corp. 1985
```

S9042611

4. If you decide not to stop the password date checking function, press command key 7. The SECDEF procedure does not stop the password date checking, and the procedure ends.

   If you decide to stop the password date checking function, press the Enter key. The system displays a message indicating that the password date checking function was stopped. To complete the SECDEF procedure, press command key 3 or the Enter key.

Deactivating Badge Security

Care should be taken when you deactivate badge security. Remember that when badge security is deactivated, users no longer have to pass a badge through a magnetic stripe reader to sign on to a display station that has a magnetic stripe reader configured.

If you deactivate badge security, the user ID file remains on disk and badge numbers that are identified in the user profiles remain unchanged. Password security, communications security, and menu security are not affected.

Badge security can be deactivated by running the SECDEF procedure when password security is active or is scheduled to be active. Deactivating badge security has no effect on password security; however, if password security is deactivated, badge security is automatically deactivated.

Only the master security officer can run the SECDEF procedure from any display station to deactivate badge security.

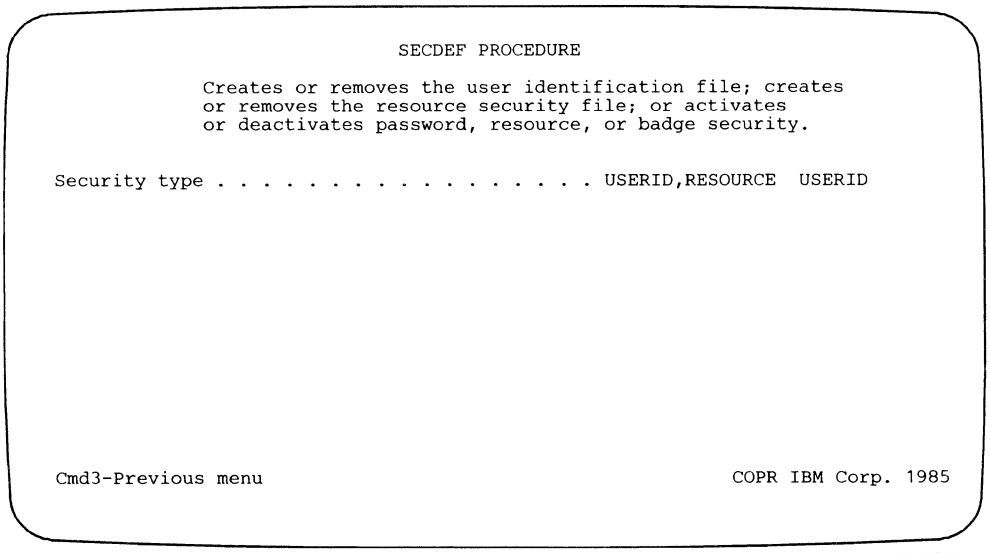
To deactivate badge security, do the following:

1. On the command display, type:

   SECDEF

   Press the Help key.

   The following display appears:



S9042538

2. On the display shown in step 1, the system asks you for the type of security file that you want to work with. The system has already filled in USERID for the security file type. Because badge security uses the user ID file, press the Enter key.

   The following display appears:

```
                              SECDEF PROCEDURE

            Creates or removes the user identification file; creates
            or removes the resource security file; or activates
            or deactivates password, resource, or badge security.

Security type . . . . . . . . . . . . . . . . . . USERID,RESOURCE  USERID

Option  . . . . . . . . . . . . . . . . . . . . . ACTBDG,ACTPW,CREATE
                    DEACTBDG,DEACTPW,DELETE,STRTDATE,STOPDATE              *









Cmd2-Page back                                          COPR IBM Corp. 1985
```

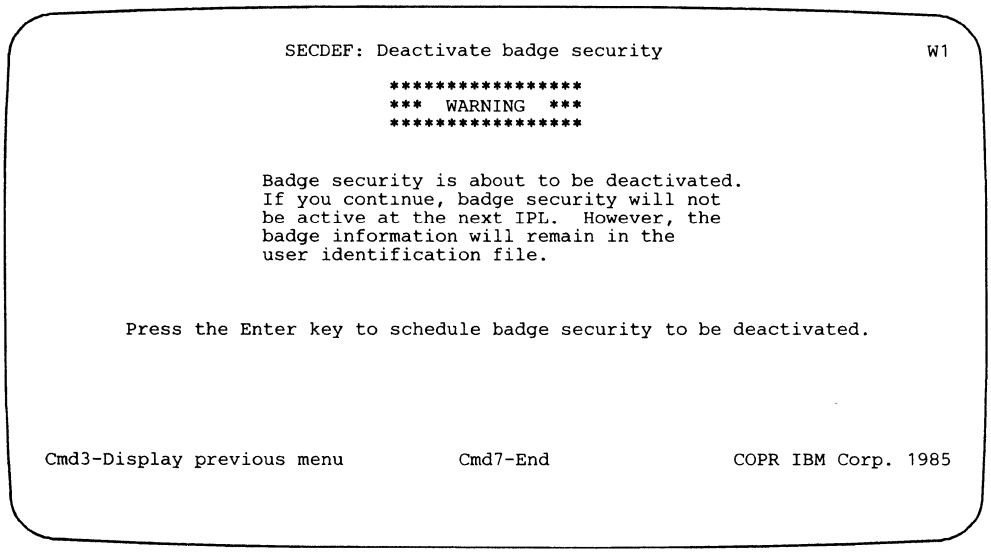
S9042539

3. Using the display shown in step 2, you can choose one of several tasks:

   Activate badge security
   Activate password security
   Create the user ID file
   Deactivate badge security
   Deactivate password security
   Delete the user ID file
   Start the date checking function
   Stop the date checking function

   Because you want to deactivate badge security, type DEACTBDG and press the Enter key.

   The following display appears:



S9042540

4. If you decide not to deactivate badge security, press command key 7. The SECDEF procedure does not deactivate badge security, and the procedure ends.

   To deactivate badge security, press the Enter key. The system displays a message indicating that badge security will be deactivated at the next IPL. To complete the SECDEF procedure, press command key 3 or the Enter key.

Badge security is deactivated after an IPL of the system is performed.

Removing the User ID File from Disk

The user ID file can be removed from the system by using the SECDEF procedure. Password security cannot be active when you run the SECDEF procedure to remove the user ID file. Anyone can run the SECDEF procedure to remove the user ID file but only from the system console.

Note: Before you remove the user ID file, we recommend that you create a copy on diskette, tape, or tape cartridge (see "Saving the User ID File" earlier in this chapter), or create a listing of the file (see "Listing the User ID File" earlier in this chapter). This will help you to restore or create again the user ID file should you ever decide to use password security or the user ID file in the future.

You must deactivate password security and perform an IPL before you remove the user ID file. See "Deactivating Password Security" earlier in this chapter for information about deactivating password security.

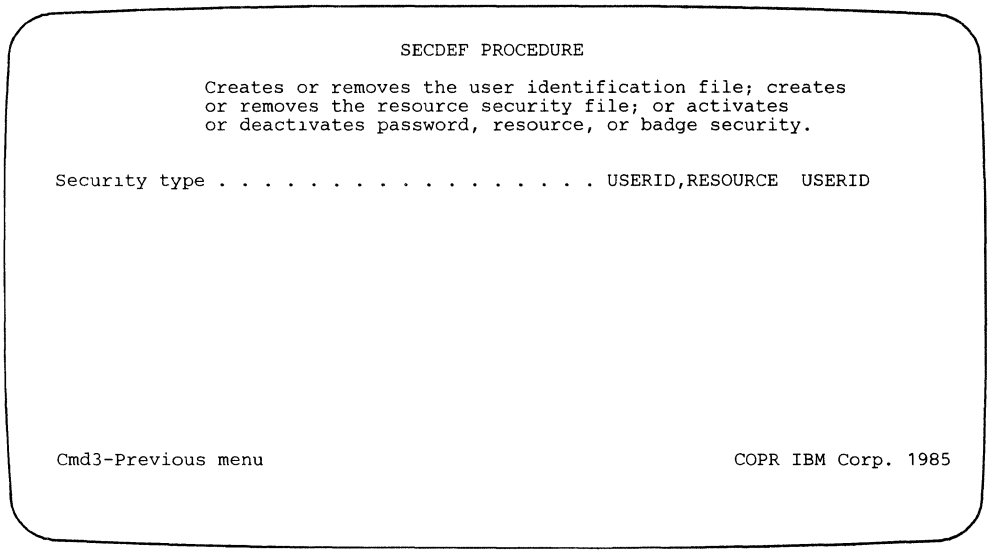
To remove the user ID file, do the following at the system console:

1. On the command display, type:

   ```
   SECDEF
   ```

   Press the Help key.

   The following display appears:



S9042541

2. You do not have to enter the type of security file you want to remove. USERID (the default value) indicates that the user ID file is to be removed.

   Press the Enter key.

   The following display appears:

```
                              SECDEF PROCEDURE

            Creates or removes the user identification file; creates
            or removes the resource security file; or activates
            or deactivates password, resource, or badge security.


Security type . . . . . . . . . . . . . . . . . USERID,RESOURCE  USERID

Option  . . . . . . . . . . . . . . . . . . . . ACTBDG,ACTPW,CREATE
                    DEACTBDG,DEACTPW,DELETE,STRTDATE,STOPDATE              *









Cmd2-Page back                                          COPR IBM Corp. 1985
```

S9042542

3. Using the display shown in step 2, you can choose one of several tasks:

   Activate badge security
   Activate password security
   Create the user ID file
   Deactivate badge security
   Deactivate password security
   Delete the user ID file
   Start the date checking function
   Stop the date checking function

   Because you want to remove the user ID file, type DELETE and press the Enter key.

   The following display appears:

```
                SECDEF: Remove the user identification file                W1

                              ****************
                              **  WARNING  ***
                              ****************

          The user identification file currently exists.

          If you remove the user identification file, all records
          in the file will be erased.  If you want to save a copy
          of the user identification file before removing it, use
          the SECSAVE procedure.


        Press the Enter key to remove the user identification file.




Cmd3-Display previous menu          Cmd7-End              COPR IBM Corp. 1985
```

S9042543

4. If you decide not to remove the user ID file, press command key 7. The SECDEF procedure does not remove the user ID file, and the SECDEF procedure ends.

   To remove the user ID file, press the Enter key. The system displays a message indicating that the user ID file was removed. To complete the SECDEF procedure, press command key 3 or the Enter key.

Chapter 3. Resource Security File

Introduction

Resource security is the type of data security that protects your information by restricting access to files, libraries, folders, subdirectories, folder members, and special resource types, such as alternative index files, the system library, and groups of files, libraries, and folders.

Note: System files are secured by the system, and are not affected by resource security.

Password security need not be active to have resource security active.

This chapter describes how to create and maintain the resource security file on your system. The methods for securing files and libraries are different from the methods for securing folders, subdirectories, and folder members. Also described are methods of combining resource records to save time and system storage.

Securing Files, Libraries, and Groups

To secure a file, library, or group, you must first identify it to the system. You do this by using the SECEDIT RESOURCE procedure to create a resource record in the resource security file.

After you create the resource record for the file, library, or group, you need to create a user record for each user who is allowed to use the file, library, or group. A user record contains a user ID and an access level.

Note: System files cannot be secured with resource security. Access to system files is controlled by the system.

Access Levels

You can assign an access level to each user of the file, library, or group. You can also assign a default access level for the file, library, or group; the default access level is used if the user is not specifically listed as a user of the file, library, or group. When resource security is active, the system checks the access level to determine if the attempted operation is allowed.

The following are the different access levels that you can assign to a user:

- Owner
- Change
- Update
- Read
- Run
- None (no access)

The following table shows the access levels and the operations that can be performed for each level:

	Library or File			Library Members			File Records	
Access Level	**Update List of Users**	**Rename**	**Create, Remove**	**Add, Change, Remove**	**List, Read**	**Run**	**Add, Change, Remove**	**List, Read**
Owner	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Change	No	No	Yes	Yes	Yes	Yes	Yes	Yes
Update	No	No	No	Yes	Yes	Yes	Yes	Yes
Read	No	No	No	No	Yes	Yes	No	Yes
Run	No	No	No	No	No	Yes	No	No
None	No	No	No	No	No	No	No	No

If resource security is active, and a person wants to access a secured file or library, the following occurs:

1. The system checks the resource security file to determine if the file or library is secured. If the file or library is not secured, the user is allowed to use it; if the file or library is secured, the next steps are performed.

2. The system then checks the list of users for the secured file or library. If the file or library does not have a resource record, the system checks to see if the file or library is secured as part of a group. If the system finds the user ID of the person attempting to use the file or library and his or her access level is high enough for the operation requested, the person is allowed to access the file or library.

3. If the person's user ID is not found in the list of users for the file or library, the system checks to see if the list of users for another file or library should also be checked. If the system finds the user ID of the person in the list of users for the second file or library, the person is given the access specified in the second list of users. See the explanation of parent and child files later in this chapter.

4. If the person's user ID is not found in either list of users, the person is allowed to use the file or library only at the default access level specified for the file or library.

If the remote system does not send a user ID, the user ID of *NULL must be specified in the list of users for each file, library, or group on your system that you will allow the remote system to access. The user ID of *NULL is not given the default access level of a file, library, or group.

If the person attempts to access a file or library at a level higher than he or she is authorized, an error message is displayed and recorded in the history file.

Parent and Child Concept

Some of your programs may require several different files and libraries. In some cases, the users of these files and libraries may be the same. Normally, you would be required to create a resource record for each file and library and a user record for each user of that file or library. If your program required 3 different files and each file had the same 5 users, you would have to create 3 resource records and 15 user records. The same 5 users would have a user record for each of the 3 files.

By using the parent and child concept you can reduce the number of records in the resource security file and the amount of security information you must enter. This concept lets you specify one file or library as the parent of another file or library. If a user doesn't have a user record for a particular file or library, the system checks to see if that file or library has a parent. If it does, and if the user has a user record for the parent, the user can access the child. You can put into effect the parent and child concept like this:

- First, secure a file or library by creating a resource record.
- Then, create a user record for each user of that file or library.
- Now, when you secure a second file or library, you can specify the first file as the parent of the second file. This means you do not have to create another user record for each user of the second file or library.
- Then all the users of the first file (the parent) can use the second file (the child).

  Note: A folder cannot have a parent resource or be a parent resource.

Figure 3-1 shows an example of the parent and child concept.

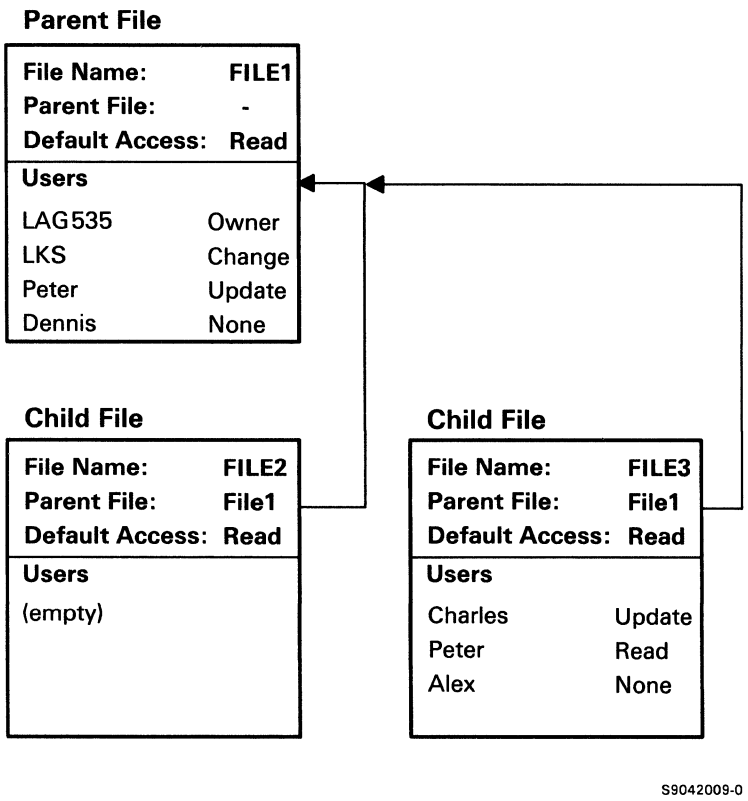


Figure 3-1. Example of Parent and Child Concept

Following is an explanation of this example:

- FILE1 is the parent file; FILE2 and FILE3 are child files.

- FILE2 does not have any users listed (empty). Because there are no users specifically listed for FILE2, the system checks the user records for FILE1 when a user attempts to use FILE2. For example, if user LKS attempts to use FILE2, she is given the access level in her user record for FILE1 (change). Also, anyone attempting to use FILE2 who does not have a user record for FILE2 (the child) or FILE1 (the parent) is given the default access level for FILE2 (read). Only a master security officer or a security officer can change security information (for example, add users) for FILE2.

- FILE3 has three user records and also has FILE1 listed as its parent file. In this case, the system checks the user records for FILE3 looking for a particular user. If the user has a user record for FILE3, the access level specified in the user record for FILE3 is used. For example, if user, Peter, attempts to use FILE3, he is given the access level in his user record for FILE3 (read) even though he has an access level of update in his user record for FILE1.

  If a user who does not have a user record for FILE3 but does have a user record for FILE1 attempts to use FILE3, the access level in the user record for FILE1 is given to the user. For example, if user LKS attempts to use FILE3, she is given the access level in her user record for FILE1 (parent file) because she does not have a user record for FILE3.

  A user who does not have a user record for FILE1 or FILE3 who attempts to use FILE3 is given the default access level for FILE3 (read).

Note: If FILE1 had a parent file of FILE0, FILE2 and FILE3 could not be child files of FILE0.

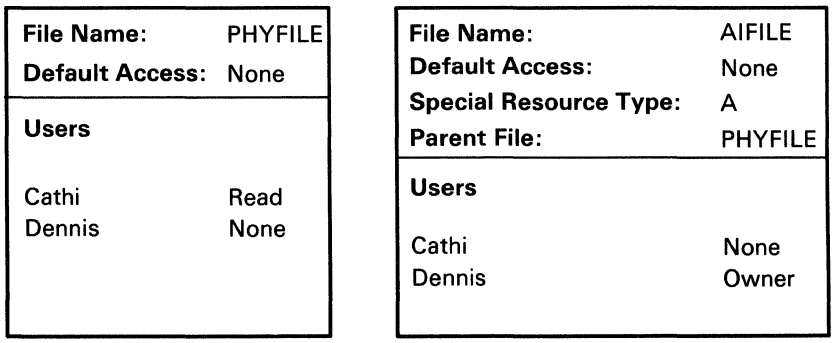
Special Resource Types

The special resource types are:

- Alternative index files
- Groups
- System library

Alternative Index Files: An alternative index file is an index that is built after a physical file is created and provides a different order for reading and writing records in the file. A physical file is an indexed file containing data for which one or more alternative indexes were created.

To create or secure an alternative index file over a secured physical file, the alternative index file name must be secured as an alternative index file, the user must have read access to the physical file, and the alternative index file security record must have the physical file as the parent resource.



Cathi can create an alternative index file called AIFILE because she has read access to the physical file PHYFILE, the alternative index file called AIFILE is secured as a special resource type A, and the parent file is PHYFILE.

To secure another alternative index file called AIFILE1, Cathi must specify that AIFILE1 is an alternative index file, the parent file must be PHYFILE, and Cathi must have read access to PHYFILE.

To create an alternative index file over an unsecured physical file, the user must have change access to the alternative index file if it is secured.

File Name:	AIFILE2
Default Access:	None
Users	
Cathi	Change
Dennis	None

S9042020-0

Cathi can create a secured alternative index file named AIFILE2 because she has change access to the file. Because the physical file is not secured, security is only checked on the alternative index file AIFILE2.

If a physical file is part of a secured group resource, the alternative index file must also be part of that group resource. The alternative index file can be secured by its own record after it is created.

Group Name:	GRP
Default Access:	None
Users	
Cathi	Read
Dennis	Change
Rick	Owner

S9042021-0

To create an alternative index file over a physical file called GRP.PHY, which is secured by the group resource security record GRP, the alternative index file must also be part of the group of resources. The alternative index file name must begin with GRP. Dennis can create an alternative index file named GRP.AI over GRP.PHY because he has change access to the group and the alternative index file name is part of the group.

If at a later time you want the alternative index file GRP.AI to have security different from the group's security, you can secure it on its own. For a description of group resources, refer to "Groups" later in this chapter.

If a physical file is secured and an alternative index file exists, the alternative index file must also be secured. The user can secure the alternative index file if the user has owner access to the physical file.

File Name:	PHYFILE2
Default Access:	None
Users	
Cathi	Owner
Dennis	Read

S9042022-0

AIFILE3 is an alternative index file for a physical file called PHYFILE2 and is not secured. Before AIFILE3 can be used, it must be secured because the physical file it is associated with is secured. Cathi can secure AIFILE3 because she is an owner of the physical file PHYFILE2.

Note: Avoid assigning users a higher level of access to the alternative index file than you assign for the physical file. If you add or change a user's access level to the alternative index file, you are in effect adding or changing a user's access to the physical file.

Groups: Normally, to secure several files and libraries, you would create a resource record for each file and library and user records for each user who could access each of the files and libraries. And to secure several folders, you would create a resource record for each folder and an authorization list of users who could access each folder.

However, you can group files, libraries, and folders to reduce the number of records in the resource security file. For example, a group of four files, two libraries, and one folder could be secured with one resource record in the resource security file.

Each of the four files, two libraries, and one folder does not need its own resource record and user records. One group resource record secures them all.

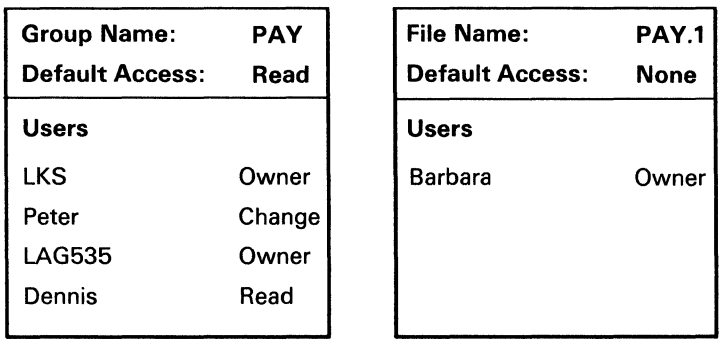
There are some rules regarding the naming of groups and the naming of files, libraries, and folders within groups.

- The group must have a group identifier (for example, PAY).
- The names of any individual files, libraries, and folders in the group must begin with the group identifier followed by a period.
- The names of any individual files, libraries, and folders in the group must be identified by unique characters (for example, PAY.1).
- The total name cannot be more than 8 characters (for example, PAY.LIBR).

For example, you could create a single resource record for a group of payroll files, libraries, and folders and name this the PAY group. Within this PAY group are four files (call them PAY.1, PAY.2, PAY.3, and PAY.4), two libraries (call them PAY.LIB1 and PAY.LIB2), and one folder (call it PAY.FOLD). Each of the file, library, and folder names in the PAY group must start with the group identifier PAY. All the files, libraries, and folders in the PAY group are secured even though they do not have individual resource records in the resource security file.

If you want all the files, libraries, and folders in this group to have the same users with the same access levels, one resource record in the resource security file is all you need to create to secure this group. This resource record contains the group identifier as the resource name. A user record with this resource name should be created for each user who can access the resources in the group.

However, if you want one of the PAY files (let's choose PAY.1) to have some users that do not have user records for the PAY group, that file must have its own resource record and its own user records. Only a user with owner access to the PAY group can create a separate resource record to secure file PAY.1.



When someone attempts to use one of the files, libraries, or folders in the PAY group, the system first searches for a resource record for that file, library, or folder. If the file, library, or folder has its own resource record, as in the case of PAY.1, the user is given that access level. For the file PAY.1, Barbara has owner access. Anyone else attempting to use file PAY.1 is given the default access. Since the default access for PAY.1 is none, no one else can use this file.

If the file, library, or folder does not have its own resource record, the system checks whether the file, library, or folder is part of a group resource. If the file, library, or folder is part of a group (as in the case of PAY.2), a user attempting to use file PAY.2 is given the access level in his or her user record for the PAY group or the default access for the PAY group. For example, if Peter attempts to use file PAY.2, he is given the access level assigned to him for the PAY group (change).

When you secure group resources, you should keep the following in mind:

- If a physical file is part of a secured group resource, the alternative index file must also be part of that group resource when the alternative index file is created. For example, if you have secured the group resource named PAY, and have a physical file named PAY.1, the name of the alternative index file you are creating must begin with the characters PAY and a period (PAY.).

- If you secure a group resource, you secure all files, libraries, and folders within that group, and the specified access levels apply in exactly the same way to all those files, libraries, and folders. The only exception is if a file, library, or folder within the group has its own unique entry in the resource security file: the unique access levels for that file, library, or folder are used instead of those for the group resource, and are used only for that file, library, or folder.

- A group resource, like any other file or library, can have a parent resource or be a parent resource. The user records for the parent resource are used in place of, or in addition to, the user records specified for the group resource.

  Note: Although the use of parent resources and group resources can save you time and disk space, be careful not to make your resource security file too complicated.

System Library: You should consider securing the system library (#LIBRARY) and specifying a default access level of read or run. This will prevent anyone from modifying the system procedures contained in #LIBRARY. Only master security officers and security officers can secure #LIBRARY.

Securing Folders, Subdirectories, and Folder Members

To secure a folder you must first identify it to the system. You do this by using the SECEDIT RESFLDR procedure. Anyone can secure folders, or folder members they have created.

You use the SECEDIT RESFLDR procedure to secure a subdirectory within a folder by specifying the series of subdirectory names. The last subdirectory in the series is the one you are securing. The *Concepts and Programmer's Guide*, SC21-9019, has more information about subdirectories.

You also use the SECEDIT RESFLDR procedure to secure folder members or PC files.

A folder can also be part of a secured group resource. For more information on group resources, refer to "Groups" earlier in this chapter.

Authorization Lists

An authorization list is a list of user IDs and access levels assigned to those users. You assign a name to each authorization list. Then when you secure a folder, subdirectory, or folder member, you must specify the authorization list name. This way the same authorization list can be used for many folders, subdirectories, and folder members.

SECEDIT RESFLDR is also the procedure you should use to create and work with authorization lists. Anyone can create an authorization list. Authorization lists can have the same name as the folders, subdirectories, or folder members they secure, if you wish.

Authorization lists can be used in two ways—as a primary authorization list or as an override authorization list. When securing a folder, subdirectory, or folder member, a primary authorization list is required; an override authorization list is optional.

A primary authorization list should contain the user IDs of the users you want to access a folder, subdirectory, or folder member.

An override authorization list is used to override the access level of a user on the primary authorization list. If a user has owner access on the primary authorization list for a folder or subdirectory and read access on the override authorization list for that folder or subdirectory, that user is given read access to that folder or subdirectory.

Users not listed on either authorization list are allowed default access to the folder.

The following illustration shows an example of primary and override authorization lists for folders:

Authorization List Name: AUTH1	
Bev	Owner
Dave	Update
Joe	Read
Nancy	None

Folder Name: FOLDER1
Default Access: Read

Primary Authorization List Name: AUTH1

Override Authorization List Name: AUTH2

Authorization List Name: AUTH2	
Bev	None
Nancy	Owner
Mary	Change

Folder Name: FOLDER2
Default Access: Read

Primary Authorization List Name: AUTH2

Override Authorization List Name: AUTH1

S9042011-0

Following is an explanation of this example:

- FOLDER1 has a default access level of read. The primary authorization list is AUTH1; the override authorization list is AUTH2.

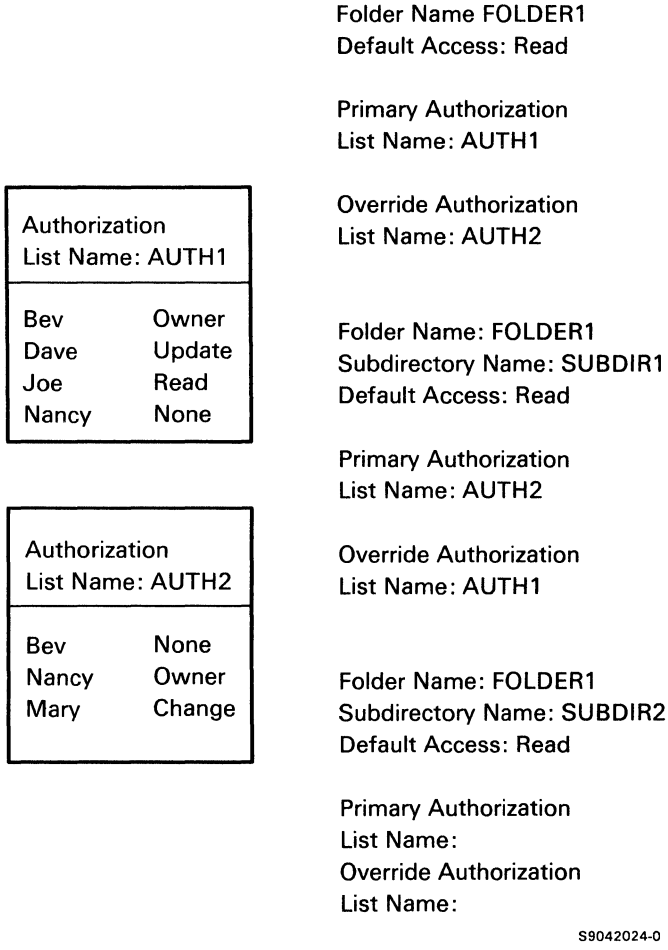
  - When Dave accesses this folder, he is given update access because he has update access on the primary authorization list (AUTH1) and he is not listed on the override authorization list (AUTH2).
  - Nancy has no access on the primary authorization list (AUTH1). Because Nancy has owner access on the override authorization list (AUTH2), she is given owner access to FOLDER1.
  - Bev is not allowed to access FOLDER1 even though she has owner access on AUTH1. Bev's access level on AUTH2 (none) overrides her owner access level on AUTH1.
  - Mary can access FOLDER1 even though she is not listed on the primary authorization list (AUTH1) for FOLDER1. She is given an access level of change because she has change access on the override authorization list (AUTH2).
  - Joe is given read access because that is his access level on the primary authorization list (AUTH1), and he is not specifically listed on the override authorization list (AUTH2).

- FOLDER2 has a default access level of read. The primary authorization list is AUTH2; the override authorization list is AUTH1.

  - Dave can access FOLDER2 even though he is not listed on the primary authorization list (AUTH2) for FOLDER2. He is given an access level of update because he has update access on the override authorization list (AUTH1).
  - Nancy is not allowed to access FOLDER2 even though she has owner access on AUTH2. Nancy's access level on AUTH1 (none) overrides her owner access level on AUTH2.
  - Bev has no access on the primary authorization list (AUTH2). Because Bev has owner access on the override authorization list (AUTH1), she is given owner access.
  - Mary is given change access because that is her access level on the primary authorization list (AUTH2) and she is not specifically listed on the override authorization list (AUTH1).
  - Joe can access FOLDER2 even though he is not listed on the primary authorization list (AUTH2) for FOLDER2. He is given an access level of read because he has read access on the override authorization list (AUTH1).

Note: Any user not listed on either the primary authorization list or the override authorization list is given the folder's default access level.

The following illustration shows an example of the primary authorization list and override authorization list for FOLDER1 with two subdirectories: SUBDIR1 and SUBDIR2.



Following is an explanation of this example:

- FOLDER1 has a default access level of read. The primary authorization list is AUTH1; the override authorization list is AUTH2.

- SUBDIR1 has a default access level of read. The primary authorization list is AUTH2; the override authorization list is AUTH1.

  - Dave has update access to FOLDER1 because he has update access on the primary authorization list (AUTH1) and he is not listed on the override authorization list (AUTH2). He has no access on the primary authorization list (AUTH2) for SUBDIR1. Because he has update access on the override authorization list (AUTH1), he can update SUBDIR1.
  - Nancy has no access on the primary authorization list (AUTH1) for FOLDER1 but because Nancy has owner access on the override authorization list (AUTH2), she is given owner access to FOLDER1. Nancy is not allowed to access SUBDIR1 even though she has owner access on AUTH2. Nancy's access level on AUTH1 (none) overrides her owner access level on AUTH2.
  - Bev is not allowed to access FOLDER1 even though she has owner access on AUTH1. Bev's access level on AUTH2 (none) overrides her owner access level on AUTH1. Bev can access SUBDIR1 even though she has no access level on AUTH2 (none). Bev's access level on AUTH1 (owner) overrides the access level of AUTH2.
  - Mary can access FOLDER1 even though she is not listed on the primary authorization list (AUTH1) for FOLDER1. She is given an access level of change because she has change access on the override authorization list (AUTH2). Mary is given change access (AUTH2) even though she is not listed on the override authorization list (AUTH1) for SUBDIR1. She is given an access level of change because she has change access on the primary authorization list (AUTH2).
  - Joe is given read access to FOLDER1 because he is on the primary authorization list (AUTH1), and he is not specifically listed on the override authorization list (AUTH2). Joe is given read access to SUBDIR1 even though he is not specifically listed on the primary authorization list (AUTH2) because his access level of read on the override authorization list (AUTH1) overrides the primary authorization list.

- Because SUBDIR2 has no security information listed, the system defaults to security of the parent (SUBDIR1) of SUBDIR2.

  - Dave has update access to SUBDIR2 because he has update access to SUBDIR1.
  - Nancy cannot access SUBDIR2 because she has no access level to SUBDIR1.
  - Bev has owner access to SUBDIR2 because she has owner access to SUBDIR1 even though she cannot access FOLDER1.
  - Mary has change access to SUBDIR2 because she has change access to SUBDIR1.
  - Joe has read access to SUBDIR2 because he has read access to SUBDIR1.

Note: Any user not listed on either the primary authorization list or the override authorization list is given the folder's default access level.

Access Levels

You assign an access level to each user on an authorization list. You also assign a default access level for the folder, subdirectory, or folder member; that access level is used if the user is not specifically listed on the primary or override authorization list for the folder, subdirectory, or folder member. When resource security is active, the system checks the access level to determine if the attempted operation is allowed.

The following are the different access levels that you can assign to a user:

- Owner
- Change
- Update
- Read
- Run
- None (no access)

Owner: Owner access to a folder or subdirectory allows a user to:

- Revise or delete security information for a folder or subdirectory
- Rename the folder
- Add, revise, or delete security information for any member in the folder or subdirectory (whether or not the user has access to the member)
- Create or delete the folder or subdirectory, and members of that folder or subdirectory
- Read, revise, or copy any information in any member of the folder or subdirectory

Owner access to a folder member allows a user to:

- Revise or delete security information for the folder member if the user also has at least update access to the folder or subdirectory
- Read, revise, or delete the folder member if the user also has at least update access to the folder or subdirectory

Note: A user listed as an owner on an authorization list can make the following changes to the authorization list itself:

- *Add or delete user IDs*
- *Change access levels*
- *Delete the authorization list*

Change: Change access to a folder or subdirectory allows a user to:

- Revise or delete security information for folder members that he or she owns
- Secure any folder members that are not secured
- Create or delete the folder or subdirectory
- Create folder members
- Delete folder members for which he or she has at least update access
- Read, revise, or copy information in folder members for which he or she has at least update access

Notes:

1. *Change access on an authorization list does not allow a user to change or remove the authorization list.*
2. *Change is not a valid access level for folder members. If a user is listed on an authorization list with an access level of change and that authorization list is used for a folder member, the user with an access level of change is given an access level of update.*

Update: Update access to a folder allows a user to:

- Revise or delete security information for folder members that he or she owns
- Secure a folder member that is not secured
- Create folder members
- Delete folder members for which he or she has at least update access
- Read, revise, copy information in folder members for which he or she has at least update access

Update access to a folder member allows a user to revise or delete the folder member if the user also has at least update access to the folder or subdirectory.

Note: Update access on an authorization list does not allow a user to revise or delete the authorization list.

Read: Read access to a folder or subdirectory allows a user to read or copy information in folder members for which he or she has at least read access.

Read access to a folder member allows a user to read or copy information in the folder member if the user also has at least read access to the folder or subdirectory.

Note: Read access on an authorization list does not allow a user to revise or delete the authorization list.

Run: Run access to a folder member allows the user to run a PC file if he or she has at least read access to the folder or subdirectory.

Note: Run access on an authorization list does not allow a user to revise or delete the authorization list.

None: An access level of none prevents a user from accessing a folder, subdirectory, or folder member.

Note: An access level of none on an authorization list prevents a user from changing or removing the authorization list.

Creating the Resource Security File

The following steps and system displays help you create the resource security file.

If password security is active, only a master security officer can create the resource security file from any display station. If password security is not active, anyone can perform the following steps, but only from the system console.

Note: Only one security procedure that uses the resource security file can be run at a time. For example, one user cannot be editing the resource security file (SECEDIT RESOURCE procedure) while another is listing the file (SECLIST RESFLDR procedure).

1. On the command display, type:

   SECDEF

   Press the Help key.

   The following display appears:

```
                          SECDEF PROCEDURE

            Creates or removes the user identification file; creates
            or removes the resource security file; or activates
            or deactivates password, resource, or badge security.

Security type . . . . . . . . . . . . . . . . . USERID,RESOURCE  USERID




Cmd3-Previous menu                                      COPR IBM Corp. 1985
```

S9042544

2. Because you want to work with the resource security file, replace USERID with RESOURCE. Press the Enter key.

   The following display appears:

```
                              SECDEF PROCEDURE

                 Creates or removes the user identification file; creates
                 or removes the resource security file; or activates
                 or deactivates password, resource, or badge security.

Security type . . . . . . . . . . . . . . . . . USERID,RESOURCE  RESOURCE

Option  . . . . . . . . . . . . . ACTRES,CREATE,DEACTRES,DELETE            *









Cmd2-Page back                                          COPR IBM Corp. 1985
```

S9042545

3. Using the display in step 2, you can choose one of several tasks:

   Activate resource security
   Create the resource security file
   Deactivate resource security
   Delete the resource security file

   Because you want to create the resource security file, type CREATE, and press the Enter key.

   The following display appears:

```
                SECDEF: Create the resource security file                  W1

          The resource security file does not currently exist.
          To create the file enter the following value:

Number of records (size of file). . . . . .  72 - 63992     72



          Press the Enter key to create the resource security file.



   Cmd3-Return to previous menu              Cmd7-Cancel this request
                                                   COPR IBM Corp. 1985
```

S9042546

4. Using the display shown in step 3, specify the size of the resource security file. The number 72 (already displayed) is the minimum number of records allowed for the resource security file; 63,992 is the maximum number allowed.

   Each file, library, or group counts as one record and each user that is specifically listed as having access to that file or library also counts as one record. Each folder or authorization list counts as one record and each user on an authorization list also counts as one record.

   For example, if you want to secure:

   10 files
   20 users for each file
   3 folders
   5 subdirectories
   5 authorization lists
   5 users on each authorization list

   Then, specify a size of 263 records:

   10 files x 1 record = 10 resource records
   20 users x 10 files = 200 user records
   3 folders x 1 record = 3 resource records
   5 subdirectories x 4 records = 20 resource records
   5 authorization lists x 1 record = 5 resource records
   5 users x 5 authorization lists = 25 user records
   263 records in all

   Type the number of records.

   Note: The actual number of records in the resource security file might be slightly larger than the number you specify. That is because the system rounds the number of records to the next greatest multiple of 80, then subtracts 8. For example, if you specify 263 records, the actual number of records will be 312 (that is, 320 - 8).

5. If you decide not to create the resource security file, press command key 7. The SECDEF procedure does not create the resource security file, and the procedure ends

   If you decide to create the resource security file, press the Enter key. The resource security file is created on disk. To complete the SECDEF procedure, press command key 3 or the Enter key.

You can now use the SECEDIT procedure to enter security information about your files, libraries, groups, folders, subdirectories, and folder members and then activate resource security using the SECDEF procedure. Or, you can activate resource security now with the SECDEF procedure, and enter the security information for your files, libraries, groups, folders, subdirectories, and folder members later. In this manual, we will explain how to activate resource security and then enter security information using the SECEDIT procedure.

Note: Your resources are not secured until you activate resource security.

Activating Resource Security

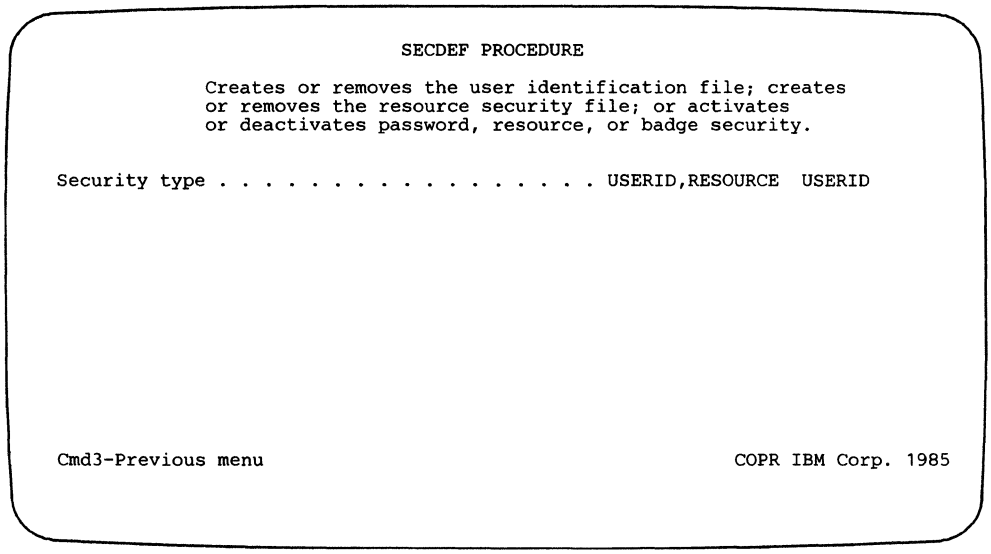
If password security is active, only a master security officer can activate resource security, but from any display station. If password security is not active, anyone can activate resource security, but only from the system console.

To activate resource security, do the following:

1. On the command display, type:

   SECDEF

   Press the Help key. The following display appears:



S9042547

2. Because resource security uses the resource security file, replace USERID with RESOURCE. Press the Enter key.

   The following display appears:

```
                              SECDEF PROCEDURE

            Creates or removes the user identification file; creates
            or removes the resource security file; or activates
            or deactivates password, resource, or badge security.

Security type . . . . . . . . . . . . . . . . . . USERID,RESOURCE  RESOURCE

Option  . . . . . . . . . . . . . . ACTRES,CREATE,DEACTRES,DELETE            *









Cmd2-Page back                                                 COPR IBM Corp. 1985
```

S9042548

3. Using the display in step 2, you can choose one of several tasks:

   Activate resource security
   Create the resource security file
   Deactivate resource security
   Delete the resource security file

   Because you want to activate resource security, type ACTRES and press the Enter key.

   The following display appears:

```
                SECDEF: Activate resource security                    W1

        Resource security is not currently active.  Type choice,
        press the Enter key to schedule resource security to be
        activated at next IPL.


List folders to display during OFFICE/36 . . . . . 1,2 |1|
  1-All folders  2-Only folders user is authorized to









Cmd3-Return to previous menu          Cmd7-Cancel this request
                                                 COPR IBM Corp. 1986
```

S9042549

   The default value for the list of secured folders is 1. If you want users to see only the folders they have access to, change the default to 2.

4. If you decide not to activate resource security, press command key 7. The SECDEF procedure does not activate resource security, and the SECDEF procedure ends.

5. Perform an IPL of the system. To activate resource security, you *must* perform an IPL.

Use the SECEDIT procedure to enter security information about your resources.

If resource security is already active, the following display appears:

```
                    SECDEF: Activate resource security                    W1

            Resource security is currently active with the following

Type choice and press Enter.

  List of folders to display during OFFICE/36. . . . . 1,2 |1|
   1- All folders  2-Only folders user is authorized to.









  Cmd3-Return to previous menu          Cmd7-Cancel this request
                                                  COPR IBM Corp. 1986
```

S9042749

Note: Resource security is already activated with the value (all folders) shown. You can change this value, and press the Enter key to change the resource security. You must perform an IPL of the system to change the value for resource security.

Entering Information into the Resource Security File

Now that you have created the resource security file, you can enter information into that file. However, you must activate resource security and IPL the system before your files, libraries, folders, and folder members are actually secured.

Entering Information for Files and Libraries

If you filled out a planning form (Resource Security Form P) for each file, library, and group resource on your system, you can use the completed forms when you enter the security information into the resource security file. If you did not fill out a planning form for each file, library, or group resource, you can still enter security information about files, libraries, and group resources into the resource security file. However, you might want to jot down some notes about each file, library, or group resource before you begin to do the actual entry work.

The following illustration shows a completed Form P and those entries being entered into the resource security file using the SECEDIT RESOURCE procedure.

P **Resource Security Form**

Customer Name _____
Customer Number _____

File ✓ Library _____ Resource Group _____

Application Personnel
Purpose personnel department

Optional = *

Resource name PERSFILE

*Special resource type (A,G,S) —

A = The file is an alternative index.
G = The files and libraries are secured as a group.
S = The library is #LIBRARY.

Default access N

(O, C, U, R, E, N)

O = Owner
C = Change
U = Update
R = Read
E = Run
N = No access

*Parent resource name —

Is the parent resource a group resource record? — (Y,N)

Log successful accesses? Y (Y,N)

User ID	Access allowed (O,C,U,R,E,N)	User ID	Access allowed (O,C,U,R,E,N)
JMS	O		
LAG	U		
PMP	U		
SLK	E		

S9042003-0

```
                        SECEDIT RESOURCE                                W7

                    Edit the resource security file

          Mode: Add - Key in requested information and press Enter or Cmd6


                                                              Optional-*
Resource name. . . . . . . . . . . . . . . . . . . . . . .    PERSFILE

Special resource type. . . . . . . . . . . . . . . . . . A,G,S          *

Default access . . . . . . . . . . . . . . . . . . O,C,U,R,E,N  N

Parent resource name . . . . . . . . . . . . . . . . . .               *

   Is the parent resource a group resource record? . . . . Y,N  N
Log successful accesses? . . . . . . . . . . . . . . . . Y,N  Y

Roll keys-Page          Cmd2-Scan          Cmd3-Restart        Cmd4-Remove
Cmd5-Add mode           Cmd6-Display user records              Cmd7-End
                                                          COPR IBM Corp. 1985
```

S9042550

```
                        SECEDIT RESOURCE                                W1

                    Edit the resource security file

          Mode: Add - Key in requested information and press Enter or Cmd6


Resource name. . . . . . . . . . . . . . . . . . . . . . . PERSFILE

User ID  . . . . . . . . . . . . . . . . . . . . . . . . . JMS

Access allowed . . . . . . . . . . . . . . . . . . O,C,U,R,E,N  O




Roll keys-Page          Cmd2-Scan          Cmd3-Restart        Cmd4-Remove
Cmd5-Add mode           Cmd6-Display resource records          Cmd7-End
                                                          COPR IBM Corp. 1985
```

S9042551

1. To enter security information about files, libraries, and group resources into the resource security file, type:

   SECEDIT RESOURCE

   Press the Help key. The following display appears:

```
                          SECEDIT PROCEDURE

                  Updates the user identification file
                  or the resource security file


Type of security
  information . . . . . .  USERID,RESOURCE,COMM,RESFLDR  RESOURCE









Cmd3-Previous menu                                  COPR IBM Corp. 1985
```

S9042552

2. Press the Enter key. The following display appears, which shows the first blank record in the resource security file.

```
                          SECEDIT RESOURCE                          W7

                  Edit the resource security file

      Mode: Add - Key in requested information and press Enter or Cmd6


                                                          Optional-*
Resource name. . . . . .

Special resource type. . . . . A,G,S                          *

Default access . . . . . O,C,U,R,E,N  N

Parent resource name . . . . . .                              *

   Is the parent resource a group resource record? . . . . Y,N  N
Log successful accesses? . . . . . Y,N  N

Roll keys-Page        Cmd2-Scan        Cmd3-Restart       Cmd4-Remove
Cmd5-Add mode         Cmd6-Display user records           Cmd7-End
                                                       COPR IBM Corp. 1985
```

S9042553

3. Type the resource name of the file, library, or group resource. A file, library, or group resource name must begin with an alphabetic character (A through Z, #, $, or @). The remaining characters can be any combination of characters (numeric, alphabetic, and special). File and library names can be up to 8 characters with a 3 character extension. If you are securing a group resource, the group identifier you enter in the resource name field should be less than 8 characters. That is because you will need to uniquely identify each file, library, or folder that is part of the group resource. For more information about naming group resources, see the section, "Groups," earlier in this chapter.

4. Type the special resource type if this resource is a special resource. Special resource types are:

   A Alternative index file
   G Group
   S System Library

   Special resource types are described in detail in the section, "Special Resource Types," earlier in this chapter.

5. Type the default access level for this resource. Access levels are:

   O Owner
   C Change
   U Update
   R Read
   E Run
   N None

   Access levels are described in detail in the section, "Access Levels," earlier in this chapter.

6. Type the parent resource name if this resource is a child file or child library.

   Parent resources are described in detail in the section, "Parent and Child Concept," earlier in this chapter.

7. Type Y (yes) or N (no) to indicate whether the parent resource is a group resource.

8. Type Y (yes) or N (no) to indicate whether or not successful accesses to the file, library, or resource secured as part of a group are to be recorded in the history file. (Unsuccessful accesses to the file, library, or resource secured as part of a group are always recorded in the history file.)

When you press the Enter key, you create the first resource record in the resource security file. Next, you need to create a user record for each user you want to access this resource.

Press the Enter key. The following display appears:

```
                          SECEDIT RESOURCE                              W1
                    Edit the resource security file
      Mode: Add - Key in requested information and press Enter or Cmd6


Resource name. . . . . . . . . . . . . . . . . . . . . . . . . . PERSFILE
User ID  . . . . . . . . . . . . . . . . . . . . . . . . . . . . JMS
Access allowed . . . . . . . . . . . . . . . . . . O,C,U,R,E,N  O




Roll keys-Page        Cmd2-Scan        Cmd3-Restart       Cmd4-Remove
Cmd5-Add mode         Cmd6-Display resource records       Cmd7-End
                                                       COPR IBM Corp. 1985
```

S9042554

The first user record is filled in with your user ID because the system assumes you want to be an owner of the resource you just secured.

This display contains:

- The resource name of the file, library, or group you just secured
- Your user ID
- An O (owner) access level

If you want to be an owner of this resource, press the Enter key. You have just created the first user record (yours) for this resource.

If you want to be a user of this resource, but not an owner, you can change the access level.

If you do not want to be a user of this resource, change the user ID and access level to that of a user who does need access to this resource.

You cannot change the resource name from this display.

Press the Enter key. The following display appears:

```
                              SECEDIT RESOURCE                              W1

                        Edit the resource security file

          Mode: Add - Key in requested information and press Enter or Cmd6


     Resource name. . . . . . . . . . . . . . . . . . . . . . . . . PERSFILE

     User ID  . . . . . . . . . . . . . . . . . . . . . . . . . . .

     Access allowed . . . . . . . . . . . . . . . . . . O,C,U,R,E,N




     Roll keys-Page          Cmd2-Scan          Cmd3-Restart          Cmd4-Remove
     Cmd5-Add mode           Cmd6-Display resource records            Cmd7-End
                                                          COPR IBM Corp. 1985
```

S9042555

1. The system has again filled in the resource name with the name of the file, library, or group you secured in the previous steps.

2. Type the user ID of another user you want to access this resource.

3. Type the access level allowed this user.

4. Press the Enter key. The next blank user record is displayed. Continue entering user records for each user you want to access the resource you just secured.

The user ID of *NULL and an access level must be entered for each file, library, and group on your system that you will allow the null user ID (*NULL) to use. For a description of the null user ID (*NULL), see "Entering User Profiles" in Chapter 2.

An access level must be specified with the *NULL user ID. The *NULL user ID is not given the default access level of a file, library, or group.

When you finish entering user records, press command key 6 to display the resource records. Then press command key 5 to add another resource record.

You can then secure another resource by creating a resource record and user records for that resource.

Press command key 7 to end the SECEDIT RESOURCE procedure.

Entering Information for Authorization Lists, Folders, Subdirectories, and Folder Members

If you filled out a planning form (Folder Security Form T) for each authorization list, folder, and folder member on your system, you can use the completed forms when you enter the security information into the resource security file. If you did not fill out a planning form for each authorization list, folder, and folder member, you can still enter security information. However, you might want to jot down some notes about each authorization list, folder, subdirectory, and folder member before you begin to do the actual entry work.

Figure 3-2 shows a completed Form T for an authorization list and the information being entered on the Create an Authorization List display. Figure 3-3 shows a completed Form T for a folder and the information being entered on the Secure a Folder display. Figure 3-4 shows a completed Form T for a subdirectory and the information being entered on the Secure a Subdirectory display. Figure 3-5 shows a completed Form T for a folder member and the information being entered on the Revise Folder Member Security display.

T **Security For Folders (reverse side)**

Customer Name _____
Customer Number_____

Authorization List

Authorization list name AUTH1___

Purpose Dept 123

User ID	Access Allowed (O, C, U, R, N)
Bev_____	O
Dave____	U
Joe_____	R
Nancy___	N
_____	_
_____	_
_____	_
_____	_
_____	_
_____	_
_____	_
_____	_
_____	_
_____	_
_____	_
_____	_
_____	_

S9042005-0

```
                    CREATE AN AUTHORIZATION LIST
Type choices, press Enter.
 ITEM                              CHOICE      POSSIBLE CHOICES
Authorization list . . . . . . . AUTH1       Name of list

Position list to . . . . . .                  Starting character(s)

                                LIST OF USER IDS                          ALL

Type user ID and access level (O=Owner C=Change U=Update R=Read E=Run N=None)
USER ID   ACCESS    USER ID   ACCESS    USER ID    ACCESS    USER ID   ACCESS
BEV         O
DAVE        U
JOE         R
NANCY       N



Cmd3=Go back  Cmd7=End   Cmd8=Reset  Roll keys=Page       COPR IBM Corp.  1986
```

S9042701

Figure 3-2. Completed Planning Form for an Authorization List

T **Security For Folders**

Customer Name ________
Customer Number ________

Folder	Folder
Folder name *Folder1* Purpose *Text folder for Dept 436* Primary authorization list *AUTH1* Override authorization list *AUTH4* Default access level (O, C, U, R, N) *R* Log successful accesses Yes (1) or No (2) *1*	Folder name ________ Purpose ________ Primary authorization list ________ Override authorization list ________ Default access level (O, C, U, R, N) __ Log successful accesses Yes (1) or No (2) __
Members Within Folder	**Members Within Folder**
Subdirectory ________ ________ Folder member name ________ Default access level __ Primary authorization list ________ Override authorization list ________	Subdirectory ________ ________ Folder member name ________ Default access level __ Primary authorization list ________ Override authorization list ________
Members Within Folder	**Members Within Folder**
Subdirectory ________ ________ Folder member name ________ Default access level __ Primary authorization list ________ Override authorization list ________	Subdirectory ________ ________ Folder member name ________ Default access level __ Primary authorization list ________ Override authorization list ________
Members Within Folder	**Members Within Folder**
Subdirectory ________ ________ Folder member name ________ Default access level __ Primary authorization list ________ Override authorization list ________	Subdirectory ________ ________ Folder member name ________ Default access level __ Primary authorization list ________ Override authorization list ________

S9042006-1

```
                          SECURE A FOLDER
Type information, press Enter to secure a folder.

 ITEM                                CHOICE      POSSIBLE CHOICES
 Folder . . . . . . . . . . . . . . FOLDER1        Name

 Default access . . . . . . . . . . R               O=Owner    C=Change
                                                    U=Update   R=Read
                                                    N=None

 Primary authorization list . . . . AUTH1           Name
 Override authorization list  . . . AUTH4           Name
 Log successful accesses? . . . . . 1               1=Yes     2=No




 Cmd3=Go back                                       Cmd7=End
 Cmd9=Work with the Primary authorization list
 Cmd10=Work with the Override authorization list        COPR IBM Corp. 1986
```

S9042702

Figure 3-3. Completed Planning Form for a Folder

Security For Folders

Customer Name _____
Customer Number _____

Folder	Folder
Folder name Folder1 Purpose Text folder for Dept 436 Primary authorization list AUTH1 Override authorization list AUTH4 Default access level (O, C, U, R, N) — Log successful accesses Yes (1) or No (2) —	Folder name _____ Purpose _____ Primary authorization list _____ Override authorization list _____ Default access level (O, C, U, R, N) — Log successful accesses Yes (1) or No (2) —
Members Within Folder	**Members Within Folder**
Subdirectory /Folder1/SUBDIR1 Folder member name _____ Default access level R Primary authorization list AUTH1 Override authorization list AUTH2	Subdirectory _____ Folder member name _____ Default access level — Primary authorization list _____ Override authorization list _____
Members Within Folder	**Members Within Folder**
Subdirectory _____ Folder member name _____ Default access level — Primary authorization list _____ Override authorization list _____	Subdirectory _____ Folder member name _____ Default access level — Primary authorization list _____ Override authorization list _____
Members Within Folder	**Members Within Folder**
Subdirectory _____ Folder member name _____ Default access level — Primary authorization list _____ Override authorization list _____	Subdirectory _____ Folder member name _____ Default access level — Primary authorization list _____ Override authorization list _____

S9042023-0

```
                        SECURE A SUBDIRECTORY

Type choices, press Enter.
 ITEM                          CHOICE          POSSIBLE CHOICES
Subdirectory . . . . . . . . SUBDIR1

Folder name  . . . . . . . . FOLDER1            Blank for list

Default access . . . . . . . R                  O=Owner   C=Change
                                                U=Update  R=Read
                                                N=None

Primary authorization list. . AUTH1             Name of list
Override authorization list . AUTH2             Name of list
Log successful accesses?. . . 1                 1=Yes  2=No



 Cmd3=Go back                                   Cmd7=End
 Cmd9=Work with Primary authorization list
 Cmd10=Work with Override authorization list
 Cmd14=Subdirectory                                    COPR IBM Corp. 1986
```

S9042703

Figure 3-4. Completed Planning Form for a Subdirectory

Security For Folders

Customer Name _____
Customer Number _____

Folder	Folder
Folder name Folder2 Purpose project status reports Primary authorization list AUTH2 Override authorization list AUTH1 Default access level (O, C, U, R, N) R Log successful accesses Yes (1) or No (2) 2	Folder name Purpose Primary authorization list Override authorization list Default access level (O, C, U, R, N) Log successful accesses Yes (1) or No (2)
Members Within Folder	**Members Within Folder**
Subdirectory Folder member name REPORTS Default access level N Primary authorization list AUTH2 Override authorization list AUTH1	Subdirectory Folder member name Default access level Primary authorization list Override authorization list
Members Within Folder	**Members Within Folder**
Subdirectory Folder member name Default access level Primary authorization list Override authorization list	Subdirectory Folder member name Default access level Primary authorization list Override authorization list
Members Within Folder	**Members Within Folder**
Subdirectory Folder member name Default access level Primary authorization list Override authorization list	Subdirectory Folder member name Default access level Primary authorization list Override authorization list

S9042007-1

```
                    REVISE FOLDER MEMBER SECURITY

Folder member: REPORTS
Folder: FOLDER2

Type changes, press Enter.
 ITEM                                    CHOICE      POSSIBLE CHOICES

 Default access . . . . . . . . . . . . N            U=Update  R=Read
                                                     E=Run  N=None
 Primary authorization list . . . . . . AUTH2        Name of list

 Override authorization list . . . . . . AUTH1       Name of list



Cmd3=Go back       Cmd4=Remove security       Cmd7=End
Cmd9=Work with the Primary authorization list
Cmd10=Work with the Override authorization list          COPR IBM Corp. 1986
```

S9042704

Figure 3-5. Completed Planning Form for a Folder Member

Use the SECEDIT RESFLDR procedure to create authorization lists and secure folders, subdirectories, and folder members.

You should create your authorization lists first because you must enter the name of an existing authorization list when you secure your folders, subdirectories, and folder members. If the authorization list name you enter does not exist, an error message is displayed. You are prompted to press the Enter key, and the Create an Authorization List display appears.

You must create folder members before you can secure them. If the folder member does not exist when you try to secure it, an error message is displayed.

You must secure a folder before you can secure any of the subdirectories or members of that folder.

Creating an Authorization List

1. To access the folder security display, type:

   ```
   SECEDIT RESFLDR
   ```

   Press the Enter key.

   The following display appears:

```
                    WORK WITH FOLDER RESOURCE SECURITY
Type choices, press Enter.
ITEM                              CHOICE          POSSIBLE CHOICES
Option . . . . . .                                 1=Folder
                                                   2=Subdirectory
                                                   3=Member
                                                   4=Authorization List




Cmd3=Go back   Cmd7=End                                  COPR IBM  Corp. 1986
```

S9042706

Note: To bypass the Work with Folder Resource Security display and go directly to the Work with Authorization Lists display, type SECEDIT RESFLDR,AUTHLIST and press the Enter key.

2. To create an authorization list, type 4 (*Authorization list*) in the *Option* prompt.

   Press the Enter key.

   The following display appears:

```
                          WORK WITH AUTHORIZATION LISTS
Type choices, press Enter.
ITEM                              CHOICE          POSSIBLE CHOICES
Option . . . . . .                                1=Create   2=Revise
                                                  4=Delete

Authorization list name . . .                     Blank for list
Position list to . . . . . .                      Starting character(s)




Cmd3=Go back  Cmd7=End                                  COPR IBM  Corp. 1986
```

S9042707

   If you leave the *Authorization list name* prompt blank and press the Enter key, the following display appears with a list of authorization lists.

```
                          WORK WITH AUTHORIZATION LISTS
Type choices, press Enter.
ITEM                              CHOICE          POSSIBLE CHOICES
Option . . . . . .                                1=Create   2=Revise
                                                  4=Delete

Authorization list name . . .                     Blank for list
Position list to . . . . . .                      Starting character(s)
                          LIST OF AUTHORIZATION LISTS                   ALL
Or select authorization list using option 2=change or 4=remove.
OPTION   NAME     OPTION   NAME     OPTION   NAME     OPTION   NAME
         AUTH1
         AUTH2
         FOLD2
         DEPT535


Cmd3=Go back  Cmd7=End  Roll key=Page                   COPR IBM  Corp. 1986
```

S9042708

3. Type 1 (*Create*) in the *Option* prompt and the name for the authorization list that you want to create in the *Authorization list name* prompt.

   Press the Enter key.

   The following display appears:

```
                        CREATE AN AUTHORIZATION LIST
Type choices, press Enter.
 ITEM                                CHOICE      POSSIBLE CHOICES
Authorization list . . . . . . . DEPT535      Name of list

Position list to . . . . . . . .              Starting character(s)

                                  LIST OF USER IDS                              ALL

Type user ID and access level (O=Owner C=Change U=Update R=Read E=Run N=None)
USER ID   ACCESS    USER ID   ACCESS    USER ID    ACCESS    USER ID   ACCESS
KKG535      O


Cmd3=Go back  Cmd7=End   Cmd8=Reset Roll keys=Page       COPR IBM Corp.  1986
```

S9042709

4. Move the cursor to the first user ID field in column 1.

   Note: Your user ID and an access level of ***O*** *(owner) was entered by the system. If you do not want to be an owner on this authorization list, you can change your access level. If you do not want to be listed on this authorization list, type the user ID and access level of another user over your user ID and access level.*

5. Type the user ID of each user you want to put on this authorization list. User IDs can be up to 8 characters. A user ID must begin with an alphabetic character (A through Z), or #, $, @ or a numeric character (0 through 9). The remaining characters can be any character except a blank or a comma.

6. Type the access level you want to assign to each user specified in the user ID field. Allowed access levels are:

   O Owner
   C Change
   U Update
   R Read
   E Run
   N None

   Access levels are described in detail in the section, "Access Levels," earlier in this chapter.

7. Continue typing user IDs and access levels for all the users you want to put on this authorization list. You can use the Roll ↑ (Roll Up) key to display more blank user ID and access level fields. Pressing the Roll ↑ key automatically saves the information you already entered for this authorization list.

8. After you have entered all the information, press the Enter key to create the authorization list. A message is displayed telling you the authorization list was created.

   All fields are blank except the first *User ID* and *Access* fields. You can create another authorization list by repeating steps 4 through 8.

9. Press command key 3 to go back to the Work with Authorization Lists display. On this display you will see that the authorization list you just created was added to the list of authorization lists. The authorization list names are displayed in alphabetic order.

Securing Folders

1. To secure a folder, type:

   ```
   SECEDIT RESFLDR
   ```

   Press the Enter key.

   The following display appears:

```
                    WORK WITH FOLDER RESOURCE SECURITY

Type choices, press Enter.
ITEM                              CHOICE          POSSIBLE CHOICES
Option . . . . . .                                1=Folder
                                                  2=Subdirectory
                                                  3=Member
                                                  4=Authorization List




Cmd3=Go back   Cmd7=End                                  COPR IBM  Corp. 1986
```

S9042710

   Note: To bypass the Work with Folder Resource Security display and go directly to the Work with Resource Security for Folders display, type SECEDIT RESFLDR,FOLDER and press the Enter key.

2. Type 1 (*Folder*) in the *Option* prompt and press the Enter key.

The following display appears:

```
                WORK WITH RESOURCE SECURITY FOR FOLDERS

Type choices, press Enter.
 ITEM                          CHOICE              POSSIBLE CHOICES

Option . . . . . .                                1=Secure    2=Revise
                                                  4=Delete

Folder name. . . . . .                            Blank for list
Position list to . . . . . .                      Starting character(s)




 Cmd3=Go back  Cmd7=End                                  COPR IBM  Corp. 1986
```

S9042711

If you leave the *Folder name* prompt blank and press the Enter key, the following display appears with a list of secured folders:

```
                WORK WITH RESOURCE SECURITY FOR FOLDERS

Type choices, press Enter.
 ITEM                          CHOICE              POSSIBLE CHOICES

Option . . . . . .                                1=Secure    2=Revise
                                                  4=Delete

Folder name. . . . . .                            Blank for list
Position list to . . . . . .                      Starting character(s)

                          LIST OF SECURED FOLDERS                    ALL

 Or select secured folder using option 2=revise or 4=delete.
 OPTION   NAME     OPTION   NAME     OPTION   NAME     OPTION   NAME
          FOLD1
          FOLDER1
          FOLDER2


 Cmd3=Go back  Cmd7=End  Cmd8=Reset  Roll keys=Page       COPR IBM  Corp. 1986
```

S9042712

3. Type a 1 (*Secure*) in the *Option* prompt and the name of the folder in the *Folder name* prompt. Press the Enter key.

The following display appears:

```
                              SECURE A FOLDER
Type information, press Enter to secure a folder.

 ITEM                                CHOICE       POSSIBLE CHOICES
 Folder . . . . . . . . . . . . . . . FOLDER1     Name

 Default access . . . . . . . . . . . N           O=Owner   C=Change
                                                  U=Update  R=Read
                                                  N=None

 Primary authorization list . . . .  AUTH1        Name
 Override authorization list  . . .  AUTH2        Name
 Log successful accesses? . . . . .  2            1=Yes     2=No




 Cmd3=Go back                                          Cmd7=End
 Cmd9=Work with the Primary authorization list
 Cmd10=Work with the Override authorization list       COPR IBM Corp. 1986
```

S9042713

Note: If you create a folder using DisplayWrite/36 (DW/36) and request to secure it, a similar display appears with the folder name already entered. The folder name cannot be changed on that display.

A folder name can be up to 8 characters and must begin with an alphabetic character (A through Z), or #, $, or @. The remaining characters can be any combination of characters (numeric, alphabetic, and special).

4. Type the default access level of this folder. The default is None (N). The default access level is given to any user who is not listed in the authorization lists used by this folder. Allowed default access levels are:

   O Owner
   C Change
   U Update
   R Read
   N None

   Access levels are described in detail in the section, "Access Levels," earlier in this chapter.

5. Type the primary authorization list name for this folder. A primary authorization list name is required. A primary authorization list name can be up to 8 characters, and must begin with an alphabetic character (A through Z), or #, $, or @. The remaining characters can be any combination of characters (numeric, alphabetic, and special).

   Note: If the authorization list does not exist for this folder, you must create one before you can continue. A message is displayed prompting you to press the Enter key to create an authorization list on the Create an Authorization List display. On this display, the authorization list name is already entered and cannot be changed. Command key 9 (Create a primary authorization list) or command key 10 (Create an override authorization list) also takes you to the Create an Authorization List display.

   Authorization lists are described in detail in the section, "Authorization Lists," earlier in this chapter.

6. Type the name of the override authorization list if you wish to create or change it. An override authorization list name is optional. An override authorization list name can be up to 8 characters. An override authorization list name must begin with an alphabetic character (A through Z), or #, $, or @. The remaining characters can be any combination of characters (numeric, alphabetic, and special).

   Authorization lists are described in detail in the section, "Authorization Lists," earlier in this chapter.

7. Type 1 (*Yes*) or 2 (*No*) to indicate whether or not successful accesses to the folder are to be recorded in the history file. (Unsuccessful accesses to the folder are always recorded in the history file.) The default is 2 (*No*).

8. Press the Enter key. A message is displayed telling you the folder is secured.

   The cursor is positioned under the first character in the *Folder name* field.

   All fields are blank except the *Default access* field and and the *Log successful accesses* field. These fields are reset to their default values. You can secure another folder by repeating steps 3 through 8.

9. Press command key 3 to go back to the Work with Resource Security for Folders display. You will see that the folder was added to the list of secured folders. The folder names are displayed in alphabetic order.

Securing a Subdirectory

1. To secure a subdirectory, type:

   ```
   SECEDIT RESFLDR
   ```

   Press the Enter key.

   The following display appears:

```
                    WORK WITH FOLDER RESOURCE SECURITY
Type choices, press Enter.
ITEM                          CHOICE              POSSIBLE CHOICES
Option . . . . . .                                1=Folder
                                                  2=Subdirectory
                                                  3=Member
                                                  4=Authorization List

Cmd3=Go back   Cmd7=End                                  COPR IBM  Corp. 1986
```

S9042714

   Note: To bypass the Work with Folder Resource Security display and go directly to Work with Resource Security for a Subdirectory, type SECEDIT RESFLDR,SUBDIR and press the Enter key.

2. Type 2 (*Subdirectory*) in the *Option* prompt and press the Enter key.

The following display appears:

```
                WORK WITH RESOURCE SECURITY FOR A SUBDIRECTORY

Type choices, press Enter.
 ITEM                              CHOICE     POSSIBLE CHOICES
 Option . . . . . . . . . . . .               1=Secure  2=Revise
                                              4=Delete

 Subdirectory. . . . . . . . . .

                                               Blank for list
 Folder name . . . . . . . . . .              Blank for list
 Position list to  . . . . . . .              Starting character(s)




Cmd3=Go back  Cmd7=End                                  COPR IBM Corp. 1986
```

S9042715

If you specify a folder name but leave the *Subdirectory* prompt blank and press the Enter key, a list of subdirectories for that folder appears:

```
                WORK WITH RESOURCE SECURITY FOR A SUBDIRECTORY

Type choices, press Enter.
 ITEM                              CHOICE     POSSIBLE CHOICES
 Option . . . . . . . . . . . . . 1           1=Secure  2=Revise
                                              4=Delete
 Subdirectory. . . . . . . . . .

                                               Blank for list

 Folder name . . . . . . . . . . FOLDER1      Blank for list
 Position list to  . . . . . . .              Starting character(s)

                              LIST OF SUBDIRECTORIES                    ALL

Or select item using option 2=revise or 4=delete.
OPTION     SUBDIRECTORY
           /DIR1/DIR2/REPORT1
           /DIR1/DIR2/SALES
           /DIR1/DIR2/DIR3/REPORT2

Cmd3=Go back  Cmd7=End  Cmd8=Reset  Roll keys=Page        COPR IBM Corp. 1986
```

S9042716

Note: If a folder is restored from a system that has subdirectory support and you do not have subdirectory support on the system or it has been removed, you cannot secure subdirectories because the system cannot validate the subdirectory name. However, you do have the option to revise or delete security information.

3. Type 1 (*Secure*) in the *Option* prompt.

4. Type the names of all previous subdirectories, followed by the name of the subdirectory you want to secure in the *Subdirectory* prompt.

The sum of the characters in the folder name and the subdirectory names (including forward slashes) cannot exceed 63 characters. For example, if the folder name is 2 characters, the longest subdirectory could not be over 61 characters.

The last subdirectory name in the series is the subdirectory you are securing. For example:

```
/DIR1/DIR2/DIR3
```

Subdirectory names must begin with an alphabetic character (A through Z), or a numeric character (0 through 9). The remaining characters can be any combination of characters (numeric, alphabetic, and special).

The #, $, @, \, >, or ¦ are valid characters but should not be used.

The *Concepts and Programmer's Guide*, SC21-9019, has more information about the naming convention for subdirectories.

Press the Enter key.

The following display appears:

```
                        SECURE A SUBDIRECTORY

Type choices, press Enter.
 ITEM                          CHOICE              POSSIBLE CHOICES
Subdirectory . . . . . .

                                                  Blank for list
Folder name  . . . . . .                          Blank for list

Default access . . . . . . . N                    O=Owner  C=Change
                                                  U=Update  R=Read
                                                  N=None

Primary authorization list. .                     Name of list
Override authorization list .                     Name of list
Log successful accesses?. . . 2                   1=Yes  2=No



 Cmd3=Go back     Cmd7=End
 Cmd9=Work with Primary authorization list
 Cmd10=Work with Override authorization list              COPR IBM Corp. 1986
```

S9042717

Note: If Cmd14 is displayed, you can use it to select the name of a subdirectory you want to secure instead of typing the name.

5. Type the name of the folder that contains this subdirectory. If you do not specify a folder name, the Select Secured Folder display appears for you to select a folder name from the list of secured folders.

6. Type the default access level for the path to the subdirectory. The default value is None (N). The default access is given to any user who is not listed in authorization lists for the subdirectory.

   Default access levels allowed are:

   O Owner
   C Change
   U Update
   R Read
   N None

   Access levels are described in detail in the section, "Access Levels," earlier in this chapter.

7. Type the name of the primary authorization list. A primary authorization list name is required. A primary authorization list name can be up to 8 characters, and must begin with an alphabetic character (A through Z), or #, $, or @. The remaining characters can be any combination of characters (numeric, alphabetic, and special).

   Note: If an authorization list does not exist for this subdirectory, you must create one before you can continue. A message is displayed prompting you to press the Enter key to create an authorization list on the Create an Authorization List display. The authorization list name cannot be changed on that display. Command key 9 (Create a primary authorization list) or command key 10 (Create an override authorization list) also takes you to the Create an Authorization List display.

   Authorization lists are described in detail in the section, "Authorization Lists," earlier in this chapter.

8. Type the override authorization list name. An override authorization list name is optional. An override authorization list name can be up to 8 characters, and must begin with an alphabetic character (A through Z), or #, $, or @. The remaining characters can be any combination of characters (numeric, alphabetic, and special).

   Authorization lists are described in detail in the section, "Authorization Lists," earlier in this chapter.

9. Type 1 (*Yes*) or 2 (*No*) to indicate whether or not successful accesses are to be recorded in the history file. (Unsuccessful accesses are always recorded in the history file.) The default value is 2 (*No*).

10. Press the Enter key. A message is displayed telling you the the subdirectory is secured.

    The cursor is positioned under the first character in the *Subdirectory name* field.

    All fields are blank except the *Default access* field and and the *Log successful accesses* field. These fields are reset to their default values. You can secure another subdirectory by repeating steps 3 through 10. A message is displayed telling you the path to the subdirectory is secured.

11. Press command key 3 to go back to the Work with Resource Security for Folders display. On this display you will see that the subdirectory you just secured was added to the list of secured subdirectories. The subdirectory names are displayed in alphabetic order.

Securing Folder Members

1. To secure a folder member, type:

   ```
   SECEDIT RESFLDR
   ```

   Press the Enter key.

   The following display appears:

```
                    WORK WITH FOLDER RESOURCE SECURITY
Type choices, press Enter.
ITEM                              CHOICE          POSSIBLE CHOICES
Option . . . . . .                                1=Folder
                                                  2=Subdirectory
                                                  3=Member
                                                  4=Authorization List

Cmd3=Go back   Cmd7=End                          COPR IBM  Corp. 1986
```

S9042718

   Notes:

   a. *To bypass the Work with Folder Resource Security display and go directly to the Select Folder Member display, type SECEDIT RESFLDR,MEMBER and press the Enter key.*

   b. *If a folder is restored from a sytem that has subdirectory support and you do not have subdirectory support on the system or it has been removed, you can not secure subdirectories because the system cannot validate the subdirectory name. However, you do have the option to revise or delete security information.*

   c. *If folder management support is not on the system, you cannot work with folder member security. Option 3 (**Subdirectory**) will not be displayed.*

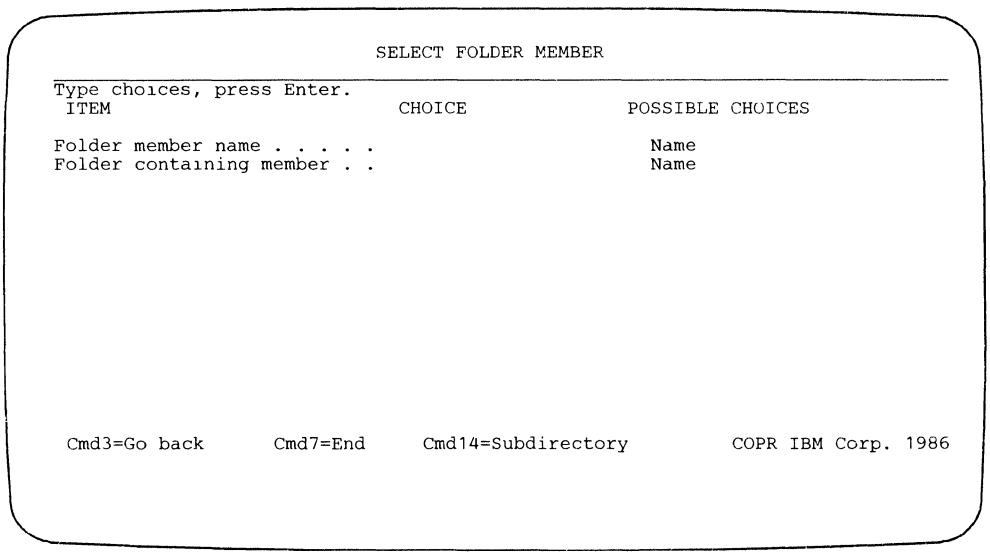
2. Type 3 (*Member*) in the *Option* prompt. Press the Enter key.

The following display appears:

```
                          SELECT FOLDER MEMBER
Type choices, press Enter.
 ITEM                          CHOICE              POSSIBLE CHOICES

Folder member name . . . . .                        Name
Folder containing member . .                        Name

 Cmd3=Go back      Cmd7=End     Cmd14=Subdirectory        COPR IBM Corp. 1986
```



S9042719

Note: Command key 14 is used to select a secured subdirectory you want to work with in the secured folder you specified.

3. Type the name of the folder member you are securing.
4. Move the cursor to the *Folder containing member* prompt.
5. Type the name of the folder that contains this member.
6. Press the Enter key.

The following display appears if:

a. The folder exists.
b. The folder member exists.
c. The folder is secured. (If the folder is not secured, and you are the owner of the folder, you can secure the folder and return to this point.)
d. You have an access level of update or higher to the folder, or you are a master security officer or security officer.
e. You have an access level of owner to the member, if the member has its own security.

```
                        REVISE FOLDER MEMBER SECURITY

Folder member: REPORT2

Folder: FOLDER2

Type changes, press Enter.
 ITEM                                    CHOICE      POSSIBLE CHOICES

 Default access . . . . . . . . . . . . . N          U=Update  R=Read
                                                     E=Run  N=None
 Primary authorization list . . . . . .              Name of list

 Override authorization list . . . . . .             Name of list




Cmd3=Go back       Cmd4=Remove security               Cmd7=End
Cmd9=Work with the Primary authorization list
Cmd10=Work with the Override authorization list          COPR IBM Corp. 1986
```

S9042720

7. Type the default access level of this folder member. The default access level is given to any user who is not listed in the authorization lists for this folder member. Default access levels allowed are:

   U Update
   R Read
   E Run
   N None

   Access levels are described in detail in the section, "Access Levels," earlier in this chapter.

8. Type the name of the primary authorization list. A primary authorization list is required. A primary authorization list name can be up to 8 characters, and must begin with an alphabetic character (A through Z), or #, $, or @. The remaining characters can be any combination of characters (numeric, alphabetic, and special).

   Note: If an authorization list does not exist for this member, you must create one before you can continue. A message is displayed prompting you to press the Enter key to create an authorization list on the Create an Authorization List display. The authorization list name cannot be changed on that display. Command key 9 (Create a primary authorization list) or command key 10 (Create an override authorization list) also takes you to the Create an Authorization list display.

9. Type the name of the override authorization list. An override authorization list is optional. An override authorization list name can be up to 8 characters, and must begin with an alphabetic character (A through Z), or #, $, or @. The remaining characters can be any combination of characters (numeric, alphabetic, and special).

10. Press the Enter key. A message is displayed telling you the folder member is secured. The Select Folder Member display is displayed again.

    To secure another folder member, you can repeat steps 3 through 10.

11. Press command key 3 to go back to the Work with Resource Security for Folders display.

Changing Information in the Resource Security File

The SECEDIT RESOURCE procedure allows you to add, revise, or delete security information for files, libraries, and groups. The SECEDIT RESFLDR procedure allows you to add, revise, or delete security information for authorization lists, folders, subdirectories, and folder members.

Changing Information for Files, Libraries, and Groups

Any user can run the SECEDIT RESOURCE procedure from any display station to display, add, change, or remove information about a file, library, or group for which the user has an access level of owner.

If password security is active, master security officers and security officers can run the SECEDIT RESOURCE procedure from any display station to display, add, change, or remove any file, library, or group information in the resource security file.

If password security is not active, *any* user can run the SECEDIT RESOURCE procedure to display, add, change, or remove *any* file library, or group information in the resource security file, but only from the system console.

1. To display, add, change, or remove security information for a file, library, or group, type:

   ```
   SECEDIT RESOURCE
   ```

   Press the Enter key.

   The first file or library resource record in the resource security file is displayed if you are a master security officer or a security officer. The first resource record for a file library that you own is displayed if your security classification is lower than security officer. A display similar to the following appears:

```
                          SECEDIT RESOURCE                              W1

                    Edit the resource security file

      Mode: Browse or Update - Key in change and press Enter or Cmd6


 Resource name. . . . . .

 Special resource type  . . . . . A,G,S          *

 Default access . . . . . O,C,U,R,E,N   N      *

 Parent resource name . . . . . .

   Is the parent resource a group resource record?. . . . Y,N   N
 Log successful accesses? . . . . . Y,N   N


 Roll keys=Page          Cmd2=Scan       Cmd3=Restart          Cmd4=Remove
 Cmd5=Add mode           Cmd6= display user records            Cmd7=End
                                                              COPR IBM CORP 1985
```

S9042567

2. Use the display shown in step 1 to do your work with file, libraries, and group resource records in the group resource security file. Refer to "Entering Information for Files and Libraries" earlier in this chapter for a description of the prompts and fields on this display.

You can use the following keys to help you change file, library, group resource records and user records.

Key	What It Does
Cmd2	Starts Scan mode. Scan mode allows you to display a specific file, library, or group resource record or a specific user record. After you press command key 2, a display appears on which you can enter a file, library, or group name and/or a user ID. If you want to display a specific file or library resource, type the name of that file or library and press the Enter key. If you want to display a specific group resource, type the name of the resource, specify the resource group, and press the Enter key. If you want to display a specific user record for a particular file, library, or group, type the name of the file, library, or group and the user ID. Press the Enter key. If you want to display all user records of a specific user, type the user ID and press the Enter key. The first user record of that user is displayed. To display the next user record of that user, press command key 2, then the Enter key.
Cmd3	Starts the Browse or Update mode and displays the first resource record in the resource security file. If you are browsing the user records for a resource record and press command key 3, the first user record for that resource is displayed. Browse or Update mode allows you to display, change, or remove resource records and user records. The SECEDIT RESOURCE procedure begins in this mode after the resource security file contains resource records. A master security officer or security officer can display and change the resource records and user records of all the files, libraries, and groups, including the name of the file, library or group and the special resource type. Any other user, with a lower security classification, can display and change only the resource records and user records of file, libraries, and groups that he or she owns. The fields that can be changed include the default access, the parent resource name, and the log information.

Cmd4 Removes the displayed resource record or user record of a file, library, or group. Command key 4 can be used only during Browse or Update mode. When you remove the resource record of a file, library, or group, that file, library, or group is no longer secured.

A master security officer or security officer can remove any resource records and user records for a file, library, or groups. Any other user, with a lower security classification, can remove only the resource records and user records for a file, library, or group that he or she owns.

After you display resource record or user record and press command key 4, a message warns you that the resource record or user record will be removed from the file. When you remove the resource record of a file, library, or group, the user records of that file, library, or group are also removed. If you decide not to remove the record, press a roll key or any other allowed command keys to continue editing.

Cmd5 Starts Add mode. Add mode allows you to add new resource records and user records for a file, library, or group.

Only a master security officer or security officer can secure #LIBRARY.

Any user can secure a file or library whether or not the file or library exists.

When Add mode begins, a blank record (if one is available) is displayed. Type in the resource or user information and press the Enter key. The new record is added to the resource security file and another blank record is displayed (if one is available). Press an allowed command key to end Add mode or press command key 7 to end the SECEDIT RESOURCE procedure.

To add a resource record when you are displaying a resource record, press command key 5 to start the Add mode.

To add a user record:

- Display the resource record of the file, library, or group
- Press command key 6 to display the user records that already exist
- Press command key 5 to start Add mode

Notes:

a. *If you add user records for a parent file or library, the child file or library user accesses are affected.*

b. *If you add user records for an alternative index file, you are, in effect, allowing the user access to the physical file.*

Cmd6	Switches the display information between resource records for files, libraries, and groups, and the user records for the files, libraries, and groups.
Cmd7	Ends the SECEDIT RESOURCE procedure.
Roll keys	The roll keys start Browse or Update mode. The roll keys page forward and backward through the resource records for files, libraries, and groups you are allowed to display, and through the user records for the file, library, or group.
Enter	Enters information and pages forward through the file.
Help	Shows additional information at any time about the display you are viewing.

Changing Information for Authorization Lists, Folders, Subdirectories, and Folder Members

Any user can run the SECEDIT RESFLDR procedure from any display station to display, add, change, or remove information about a folder, subdirectory, folder member, or authorization list for which the user has an access level of owner.

If password security is active, master security officers and security officers can run the SECEDIT RESFLDR procedure from any display station to display, add, change, or remove an authorization list or security information for any folder, subdirectory, or folder member.

If password security is not active, *any* user can run the SECEDIT RESFLDR procedure to display, add, change, or remove an authorization list or security information for *any* folder, subdirectory, or folder member, but only from the system console.

Changing an Authorization List

1. To change an authorization list, type:

   ```
   SECEDIT RESFLDR
   ```

   Press the Enter key.

   The following display appears:

```
                    WORK WITH FOLDER RESOURCE SECURITY
Type choices, press Enter.
ITEM                          CHOICE              POSSIBLE CHOICES
Option . . . . . .                                1=Folder
                                                  2=Subdirectory
                                                  3=Member
                                                  4=Authorization List

Cmd3=Go back   Cmd7=End                                COPR IBM  Corp. 1986
```

S9042721

   Note: To bypass the Work with Folder Resource Security display and go directly to the Work with Authorization Lists display, type SECEDIT RESFLDR,AUTHLIST and press the Enter key.

2. Type 4 (*Authorization list*) in the *Option* prompt. Press the Enter key.

The following display appears:

```
                        WORK WITH AUTHORIZATION LISTS
Type choices, press Enter.
ITEM                              CHOICE          POSSIBLE CHOICES
Option . . . . . .                                1=Create   2=Revise
                                                  4=Delete

Authorization list name . . .                     Blank for list
Position list to . . . . . .                      Starting character(s)




Cmd3=Go back  Cmd7=End                                  COPR IBM  Corp. 1986
```

S9042722

If you leave the *Authorization list name* prompt blank and press the Enter key, the following display appears with a list of authorization lists.

```
                        WORK WITH AUTHORIZATION LISTS
Type choices, press Enter.
ITEM                              CHOICE          POSSIBLE CHOICES
Option . . . . . .                                1=Create   2=Revise
                                                  4=Delete

Authorization list name . . .                     Blank for list
Position list to . . . . . .                      Starting character(s)
                              LIST OF AUTHORIZATION LISTS                 ALL
Or select authorization list using option 2=change or 4=remove.
OPTION   NAME     OPTION   NAME     OPTION   NAME     OPTION   NAME
         AUTH1
         AUTH2
         FOLD2
         DEPT535


Cmd3=Go back  Cmd7=End  Cmd8=Reset  Roll key=Page       COPR IBM  Corp. 1986
```

S9042723

There are two ways to specify the authorization list you want to work with.

One way is to:

1. Type 2 (*Revise*) in the *Option* prompt.
2. Type the name of the authorization list that you want to revise in the *Authorization list name* prompt.
3. Press the Enter key.

The other way is to:

1. Type 2 (*Revise*) in the Option column beside the authorization list name in the list.

   If the name you want is not shown on the list, use the roll keys to page forward or backward through the list.

   Note: A word to the right of the list title tells you the following information about the list:

All	*All the authorization list names are displayed.*
More	*There are more names than can be shown on one display; use the roll keys to display more.*
Top	*This is the top (or beginning) of the list.*
Bottom	*This is the bottom (or end) of the list.*

   Another way to position a name to the top of the list is with the *Position list to* prompt. Type the starting characters of the authorization list name you want, and the list starts with the first name beginning with those characters.

   If no authorization list name begins with the characters you specify, the list starts with the name that alphabetically comes before the characters you specified. For example, you have four authorization lists named CATHY, DAN, JOHN, and LOIS. If you type JIM in the *Position list to* prompt, the list starts with DAN because you have no name that starts with JIM.

2. Press the Enter key.

Whichever way you choose, the following display appears:

```
                        REVISE AN AUTHORIZATION LIST
Authorization list . . . . . . . DEPT535      Name of list
Type choices, press Enter.
 ITEM                              CHOICE     POSSIBLE CHOICES

Position list to . . . . . . . .             Starting character(s)

                                LIST OF USER IDS

Type user ID and access level (O=Owner C=Change U=Update R=Read E=Run N=None)
USER ID   ACCESS    USER ID   ACCESS    USER ID    ACCESS    USER ID   ACCESS
KKG535      O


Cmd3=Go back  Cmd7=End   Cmd8=Reset Roll keys=Page       COPR IBM Corp.  1986
```

S9042724

Use this display to make changes to the authorization list you specified. You cannot change the name of the authorization list from this display.

1. To add a user to this authorization list, type the user's user ID and access level in any blank *User ID* and *Access* field and press the Enter key. If there are no blank *User ID* and *Access* fields on the display, you can use the Roll key or type *END in the *Position list to* prompt to display the end of the authorization list. You can then add users after the last user ID and access level displayed.

2. To change a user on this authorization list, type over the displayed values and press the Enter key.

3. To remove a user from this authorization list, blank out the user's user ID and access level and press the Enter key.

   Refer to "Creating an Authorization List" earlier in this chapter for a description of the prompts and fields on this display.

4. To delete a list of authorization lists, type 4 (*Delete*) in the Option column beside the authorization list names in the list on the Work with Authorization Lists display.

   Press the Enter key.

   The following display appears:

```
                          DELETE AUTHORIZATION LIST
To delete security for the authorization lists shown, press Enter.
To cancel the delete press Cmd8.

NAME

  Cmd3=Go back  Cmd7=End  Cmd8=Reset delete          COPR IBM Corp. 1986
```

S9042725

5. Press the Enter key to delete the list or lists. To cancel the delete function, press command key 8.

Refer to "Entering Information for Authorization Lists, Folders, Subdirectories, and Folder Members" earlier in this chapter for a description of the prompts and fields on this display.

The following keys can be used with these displays:

Key	What It Does
Cmd3	Returns to the previous display.
Cmd7	Ends the SECEDIT RESFLDR procedure.
Cmd8	Cancels the delete function.

Changing Folder Security Information

1. To change folder security information, type:

   ```
   SECEDIT RESFLDR
   ```

   Press the Enter key.

   The following display appears:

```
                    WORK WITH FOLDER RESOURCE SECURITY
Type choices, press Enter.
ITEM                              CHOICE          POSSIBLE CHOICES
Option . . . . . .                                1=Folder
                                                  2=Subdirectory
                                                  3=Member
                                                  4=Authorization List

Cmd3=Go back   Cmd7=End                                COPR IBM  Corp. 1986
```

S9042726

   Note: To bypass the Work with Folder Resource Security display and go directly to the Work with Resource Security for Folders display, type SECEDIT RESFLDR,FOLDER and press the Enter key.

2. Type 1 (*Folder*) in the *Option* prompt. Press the Enter key.

The following display appears:

```
                    WORK WITH RESOURCE SECURITY FOR FOLDERS

Type choices, press Enter.
 ITEM                              CHOICE              POSSIBLE CHOICES

Option . . . . . .                                    1=Secure    2=Revise
                                                      4=Delete

Folder name. . . . . .                                Blank for list
Position list to . . . . . .                          Starting character(s)









 Cmd3=Go back  Cmd7=End                                    COPR IBM  Corp. 1986
```

S9042727

If you leave the *Folder name* prompt blank and press the Enter key, the following display appears:

```
                    WORK WITH RESOURCE SECURITY FOR FOLDERS

Type choices, press Enter.
 ITEM                              CHOICE              POSSIBLE CHOICES

Option . . . . . .                                    1=Secure    2=Revise
                                                      4=Delete

Folder name. . . . . .                                Blank for list
Position list to . . . . . .                          Starting character(s)

                              LIST OF SECURED FOLDERS                    ALL

Or select secured folder using option 2=revise or 4=delete.
OPTION   NAME     OPTION   NAME     OPTION   NAME     OPTION   NAME
         FOLD1
         FOLDER1
         FOLDER2


 Cmd3=Go back  Cmd7=End  Cmd8=Reset  Roll keys=Page       COPR IBM  Corp. 1986
```

S9042728

There are two ways to specify the folder you want to work with.

One way is to:

1. Type 2 (*Revise*) in the *Option* prompt.
2. Type the name of the folder in the *Folder name* prompt.
3. Press the Enter key.

The other way is to:

1. Type 2 (*Revise*) in the *Option* column, beside the folder name in the list.

   If the folder name you want is not shown on the list, use the roll keys to page forward or backward through the list.

   Note: A word to the right of the list title tells you the following information about the list:

All	*All the names are displayed.*
More	*There are more names than can be shown on one display; use the roll keys to display more.*
Top	*This is the top (or beginning) of the list.*
Bottom	*This is the bottom (or end) of the list.*

   Another way to position a name to the top of the list is with the *Position list to* prompt. Type the starting characters of the folder name you want, and the list starts with the first name beginning with those characters.

   If no folder name begins with the characters you specify, the list starts with the name that alphabetically comes before the characters you specified. For example, you have four folders named CATHY, DAN, JOHN, and LOIS. If you type JIM in the *Position list to* prompt, the list will start with DAN because you have no name that starts with JIM.

2. Press the Enter key.

Whichever way you choose, the following display appears:

```
                        REVISE FOLDER SECURITY
 ------------------------------------------------------------------------
 Folder:

 Type choices, press Enter.
  ITEM                                  CHOICE          POSSIBLE CHOICES
 Default access. . . . . . . . . . . .                  O=Owner  C=Change
                                                        U=Update  R=Read
                                                        N=None

 Primary authorization list  . . . . .                  Name of list
 Override authorization list . . . . .                  Name of list
 Log successful accesses . . . . . . .                  1=Yes  2=No




  Cmd3=Go back    Cmd4=Delete security                   Cmd7=End
  Cmd9=Work with Primary Authorization list
  Cmd10=Work with Override authorization list                 COPR IBM  Corp. 1986
```

S9042729

Use this display to make changes to the default access, primary authorization list, or override authorization list for the folder you specified. You cannot change the name of the folder from this display.

1. To revise security information for the folder, type over the displayed values and press the Enter key.

2. To delete security information for a folder, press command key 4.

   The following keys are valid for this display:

Key	What It Does
Cmd3	Returns to the Work with Resource Security for Folders display.
Cmd4	Removes security information for the specified folder. A message tells you to press the Enter key to remove security for the folder. After you press the Enter key, the system displays the Work with Resource Security for Folders display.
Cmd7	Ends the SECEDIT RESFLDR procedure.
Cmd9	Displays the primary authorization list, if you are allowed to see it. If the authorization list does not exist, command key 9 lets you create it.
Cmd10	Displays the override authorization list, if you are allowed to see it. If the authorization list does not exist, command key 10 lets you create it.

3. To delete security for a list of folders, type 4 (*Delete*) in the Option column beside the folder names in the list on the Work with Resource Security for Folders display.

   Press the Enter key.

   The following display appears:

```
                          DELETE FOLDER SECURITY

To delete security for the folders listed, press Enter.  To cancel
the delete press Cmd8.

NAME

 Cmd3=Go back  Cmd7=End  Cmd8=Reset delete              COPR IBM Corp. 1986
```

S9042730

4. To delete security for the folders in the list, press the Enter key. To cancel the delete function, press command key 8.

The following keys are valid on this display:

Key	What It Does
Cmd3	Returns to the previous display.
Cmd7	Ends the SECEDIT RESFLDR procedure.
Cmd8	Cancels the delete function.

Changing Subdirectory Security Information

1. To revise or delete security information for a subdirectory, type:

   ```
   SECEDIT RESFLDR
   ```

   Press the Enter key.

   The following display appears:

```
                    WORK WITH FOLDER RESOURCE SECURITY
Type choices, press Enter.
ITEM                              CHOICE          POSSIBLE CHOICES
Option . . . . . .                                1=Folder
                                                  2=Subdirectory
                                                  3=Member
                                                  4=Authorization List

Cmd3=Go back   Cmd7=End                                COPR IBM  Corp. 1986
```

S9042731

   Note: To bypass the Work with Folder Resource Security display and go directly to the Work with Resource Security for a Subdirectory, type SECEDIT RESFLDR,SUBDIR and press the Enter key.

2. Type 2 (*Subdirectory*) in the *Option* prompt. Press the Enter key.

The following display appears:

```
                WORK WITH RESOURCE SECURITY FOR A SUBDIRECTORY

Type choices, press Enter.
 ITEM                              CHOICE     POSSIBLE CHOICES
 Option . . . . . . . . . . . .               1=Create  2=Revise
                                              4=Delete
 Subdirectory. . . . . . . . . .


 Folder name . . . . . . . . . .              Blank for list
 Position list to  . . . . . . .              Starting character(s)









Cmd3=Go back  Cmd7=End                                  COPR IBM Corp. 1986
```

S9042732

If you type in the folder name, but leave the *Subdirectory* prompt blank and press the Enter key, you will see a list of all the subdirectories in that folder, if you are a master security officer or you have owner access to the folder.

```
                WORK WITH RESOURCE SECURITY FOR A SUBDIRECTORY

Type choices, press Enter.
 ITEM                              CHOICE     POSSIBLE CHOICES
 Option . . . . . . . . . . . .               1=Create  2=Revise
                                              4=Delete


 Folder name . . . . . . . . . .              Blank for list
 Position list to  . . . . . . .              Starting character(s)

                      LIST OF SUBDIRECTORIES                          ALL

Or select item using option 2=revise or 4=delete.

OPTION          SUBDIRECTORY
                /DIR1/DIR2/PAY
                /DIR1/DIR2/DIR3/REPORT2


Cmd3=Go back  Cmd7=End  Cmd8=Reset  Roll keys=Page      COPR IBM Corp. 1986
```

S9042733

3. Type 2 (*Revise*) in the *Option* prompt, and press the Enter key.

The following display appears:

```
                    REVISE SUBDIRECTORY SECURITY

 Folder name: FOLDER1

Type information, press Enter.

 ITEM                                    CHOICE      POSSIBLE CHOICES

 Default access . . . . . .                          O=Owner  C=Change
                                                     U=Update R=Read
                                                     N=None

 Primary authorization list . . . . . .              Name of list
 Override authorization list . . . . . .             Name of list
 Log successful accesses . . . . . .                 1=Yes     2=No


Cmd3=Go back  Cmd4=Delete security                       Cmd7=End
Cmd9=Work with the Primary authorization list
Cmd10=Work with the Override authorization list          COPR IBM Corp. 1986
```

S9042734

4. Use this display to make changes to the default access or authorization lists.

5. To change security information, type over the displayed values and press the Enter key.

   A message is displayed telling you the changes were made.

6. To delete security information for the subdirectory, press command key 4. You will be prompted to press the Enter key to delete security for that subdirectory.

   A message is displayed telling you the security was deleted.

The following keys are valid with this display:

Key	What It Does
Cmd3	Returns to the previous display.
Cmd4	Deletes security information for the specified subdirectory. A message tells you to press the Enter key to delete security for the subdirectory. *Note: Command key 4 is displayed only when using the SECEDIT through another program such as DW/36.*
Cmd7	Ends the SECEDIT RESFLDR procedure.
Cmd9	Displays the primary authorization list, if you are allowed to see it. If the authorization list does not exist, command key 9 lets you create it.
Cmd10	Displays the override authorization list, if you are allowed to see it. If the authorization list does not exist, command key 10 lets you create it.

7. To delete security information for a list of subdirectories, type 4 (*Delete*) in the Option column beside the subdirectories in the list on the Work with Resource Security for a Subdirectory display.

   Press the Enter key.

   The following display appears:

```
                    DELETE SUBDIRECTORY SECURITY
To delete security information for the subdirectories listed,
press Enter.  To cancel the delete press Cmd8.
SUBDIRECTORY




Cmd3=Go back  Cmd7=End  Cmd8=Reset delete              COPR IBM Corp. 1986
```

S9042735

8. To delete security information for the subdirectories listed, press the Enter key. To cancel the delete function, press command key 8.

The following keys are valid on this display:

Key	What It Does
Cmd3	Returns to the previous display.
Cmd7	Ends the SECEDIT RESFLDR procedure.
Cmd8	Cancels the delete function.

Changing Folder Member Security Information

1. To change or delete security information for folder members, type:

   ```
   SECEDIT RESFLDR
   ```

   Press the Enter key.

   The following display appears:

```
                    WORK WITH FOLDER RESOURCE SECURITY
Type choices, press Enter.
ITEM                              CHOICE          POSSIBLE CHOICES
Option . . . . . .                                1=Folder
                                                  2=Subdirectory
                                                  3=Member
                                                  4=Authorization List

Cmd3=Go back   Cmd7=End                          COPR IBM  Corp. 1986
```

S9042736

   Note: To bypass the Work with Folder Resource Security display and go directly to the Select Folder Member display, type SECEDIT RESFLDR,MEMBER and press the Enter key.

2. To change or delete security information for folder members, type 3 *(Member)* in the *Option* prompt. Press the Enter key.

The following display appears:

```
                        SELECT FOLDER MEMBER
Type information, press Enter.
 ITEM                                    CHOICE      POSSIBLE CHOICES
 Folder member name  . . . . . .                     Name
 Folder containing member  . . . . . .               Name

 Cmd3= Go back  Cmd7=End  Cmd14=Subdirectory          COPR IBM Corp. 1986
```

S9042737

The following keys are valid with this display:

Key	What It Does
Cmd3	Returns to the Work with Folder Resource Security display.
Cmd7	Ends the SECEDIT RESFLDR procedure.
Cmd14	Displays a list of subdirectories in that folder. This command key is displayed only if subdirectory support is on the system.

3. Enter the folder member name and the folder name. Press the Enter key.

The following display appears:

```
                    REVISE FOLDER MEMBER SECURITY
 Folder member name: PAY
 Folder: FOLDER2

Type changes, press Enter.
 ITEM                                  CHOICE      POSSIBLE CHOICES
 Default access . . . . . . . . . . . . N          U=Update R=Read
                                                   E=Run   N=None


 Primary authorization list . . . . . .            Name of list

 Override authorization list . . . . . .           Name of list




Cmd3=Go back        Cmd4=Delete security            Cmd7=End
Cmd9=Work with the Primary authorization list
Cmd10=Work with the Override authorization list     COPR IBM Corp. 1986
```

S9042738

Use this display to make changes to the security information for the folder member you specified. You cannot change the name of the folder or folder member from this display.

4. To revise security information for the folder member, type over the displayed values and press the Enter key.

5. To delete security information for the folder member, blank out the displayed values and press the Enter key, or press command key 4. Command key 4 displays a message telling you to press the Enter key to delete security for the folder member.

The following keys are valid with this display:

Key	What It Does
Cmd3	Returns to the Work with Folder Resource Security display.
Cmd4	Deletes security information for the specified folder member. A message tells you to press the Enter key to remove security for the folder member. After you press the Enter key, the system displays the Select Folder Member display. *Note: Command key 4 is displayed only when you are using SECEDIT through another program such as DW/36.*
Cmd7	Ends the function and returns you to the Select a Folder Member display again with the prompts blank, to let you select another folder member.
Cmd9	Displays the primary authorization list if you are allowed to see it. If the authorization list does not exist, command key 9 lets you create it.
Cmd10	Displays the override authorization list if you are allowed to see it. If the authorization list does not exist, command key 10 lets you create it.

Listing the Resource Security File

You can use the SECLIST procedure to print or display information contained in the resource security file.

Note: Security information about folder members cannot be listed because it is not stored in the resource security file.

Listing File, Library, and Group Security Information

How much file and library security information you can print or display depends on two things:

- Whether password security is active
- Your security classification

If password security is active, a master security officer or a security officer can use the SECLIST RESOURCE procedure to list all file, library, and group resource records and user records. Any other user can use the SECLIST RESOURCE procedure to list only the information about the files, libraries, and groups he or she owns or is authorized to access.

If password security is active, information in the resource security file can be requested from any display station. If password security is not active, anyone can use the SECLIST RESOURCE procedure to list all file, library, and group resource records and user records, but the procedure can be run only from the system console. If password security is not active, and the SECLIST RESOURCE procedure is run from a display station other than the system console, only the information about the files, libraries, and groups that the user owns or is authorized access to can be listed.

To list file, library, and group information contained in the resource security file, do the following:

1. On the command display, type:

   ```
   SECLIST RESOURCE
   ```

   Press the Help key.

   The following display appears:

```
                              SECLIST PROCEDURE

          Lists the user identification or resource security file

Security information
  to be listed  . . . . . . . . . . USERID,RESOURCE,COMM,RESFLDR  RESOURCE

Print or display output . . . . . . . . . . . . . . PRINTER,CRT   PRINTER









Cmd3-Previous menu                                   COPR IBM Corp. 1986
```

S9042574

2. Type the device for the listing:

   PRINTER specifies that the output from the SECLIST RESOURCE procedure is to be printed on the printer assigned to your display station. PRINTER is the default, and is already displayed.

   CRT specifies that the output is to be displayed on your display screen.

   Press the Enter key.

   The following display appears:

```
                              SECLIST PROCEDURE

          Lists the user identification or resource security file

Security information
  to be listed  . . . . . . . . . . USERID,RESOURCE,COMM,RESFLDR  RESOURCE

Print or display output . . . . . . . . . . . . . . PRINTER,CRT   PRINTER

Order of security file  . . . . . . . . . .  OWNERID,RNAME,USERID   OWNERID

Type of information to be listed  . . . . . . . . . .  USER,ALL   USER




Cmd2-Page back      Cmd4-Put on job queue                  COPR IBM Corp. 1986
```

S9042575

3. To indicate the order of the list, type one of the following:

   OWNERID specifies that secured files, libraries, and groups are to be listed alphabetically by the owner's user ID. OWNERID is the default, and is already displayed.

   You can list security information about the files, libraries, and groups for which you are listed as an owner. If you are a master security officer or a security officer, you can list all of the user IDs that have owner access to files, libraries, and groups.

   RNAME specifies that secured files, libraries, and groups are to be listed by resource name; that is, alphabetically by file, library, or group name. If RNAME is specified, USER cannot also be specified for the *Type of information to be listed* prompt.

   Only a master security officer or a security officer can list security information about secured files, libraries, and groups.

   USERID specifies that secured files, libraries, and groups are to be listed alphabetically by user ID.

   You can list security information about the files, libraries, and groups for which you are listed as a user. If you are a master security officer or a security officer, you can list all of the user IDs and security information about the files, libraries, and groups that users with those user IDs have access to.

4. To indicate the type of information to be listed, type one of the following:

   USER specifies that only the file, library, and group resource records for the user running the procedure are to be listed. This parameter is allowed only when OWNERID or USERID is specified. USER cannot be specified if RNAME is specified. USER is the default, and is already displayed.

   ALL specifies that all file, library, and group resource records are to be listed. You must be a master security officer or a security officer to specify ALL when password security is active.

   Press the Enter key.

The file, library, and group security information in the resource security file is printed or displayed on the device that you specified in step 2.

Sample Printout of Files, Libraries, and Groups by Resource Name

This example shows how a master security officer or security officer lists the file, library, and group entries in the resource security file in alphabetic order by file, library, or group name. If the master security officer enters:

```
SECLIST RESOURCE,PRINTER,RNAME,ALL
```

The printout shown in Figure 3-6 is printed on the printer assigned to the display station where the master security officer is running the procedure.

Resource Security by Resource Name
User ID LAG535

Resource	Type	Log	Default Access	Number	Users ID	Access	Parent	Children Number	Children Names
WARELIB	Library	N	None	2	LAG535	Owner		0	
					ALEX	Update			
FILE1	File	Y	Read	4	LAG535	Owner		2	FILE2
					LKS	Change			FILE3
					PETER	Update			
					DENNIS	None			
FILE2	File	N	Read	0			FILE1	0	
FILE3	File	N	Read	3	CHARLES	Update	FILE1	0	
					PETER	Read			
					ALEX	None			
PAY	Group	Y	Read	4	LAG535	Owner		0	
.LIB1	Library				LKS	Owner			
.1	File				PETER	Change			
.FOLD	Folder				DENNIS	Read			
FILE4	Remote	N	Run	2	PETER	Owner		0	
					DENNIS	Read			
LAGLIB	Unused	Y	Read	1	LAG535	Owner		0	

Records In Resource Security File

Secured Libraries	1
Secured Alternative Index (AI) Files	0
Secured Files	3
Secured Groups of resources	1
Secured Remote Files	1
Unused Secured Names	1
Total	7
User Records	16
Other Records	27
Total Records Used	50
Total Records Available	22
Total Records Defined	72
File Size in Blocks	1

Figure 3-6. Sample Printout of Files, Libraries, and Groups by Resource Name

Description of Entries on Sample Printout of Files, Libraries, and Groups by Resource Name

Ⓐ **User ID** indicates the user ID of the user who ran the SECLIST RESOURCE procedure.

Ⓑ **Resource** indicates the name of the secured file, library, or group.

If the secured resource is a group resource, the group identifier is listed. If a file, library, or folder is part of a group resource, the file, library, or folder is identified by the characters following the period within its name. For example, the payroll files could all be part of the group resource called PAY. If files PAY.LIB1, PAY.1, and PAY.FOLD are secured by the group resource record, they are identified within the list as .LIB1, .1, and .FOLD and appear immediately following the PAY entry.

Ⓒ **Type** indicates the type of the resource:

AI FILE	Indicates that the resource is an alternative index file.
FILE	Indicates that the resource is a file.
FOLDER	Indicates that the resource is a folder.
GROUP	Indicates that the resource is a group resource.
LIBRARY	Indicates that the resource is a library.
REMOTE	Indicates that the resource is on a remote system.
UNUSED	Indicates that the resource is not on disk. That is, the file or library is specified in the resource security file, but the file or library does not actually exist on disk.

Ⓓ **Log** indicates whether successful accesses to the file, library, or group are to be recorded in the history file. Y is yes; N is no.

Ⓔ **Default Access** indicates the default access for the file or library.

Ⓕ **Users Number** indicates how many users are defined for the file or library.

Ⓖ **Users ID** indicates the user IDs.

Ⓗ **Users Access** indicates the access level for each user ID.

Ⓘ **Parent** indicates the name of the file or library whose user records are to be included with the indicated resource's user records.

Ⓙ **Children Number** indicates the number of files or libraries that use this parent resource's user records.

Ⓚ **Children Names** indicates the names of the files and libraries that use this parent resource's user records.

Ⓛ **Secured Libraries** indicates the number of secured libraries in the resource security file.

(M) **Secured Alternative Index (AI) Files** indicates the number of secured alternative index files in the resource security file.

(N) **Secured Files** indicates the number of secured files in the resource security file.

(O) **Secured Groups of resources** indicates the number of secured groups of resources in the resource security file.

(P) **Secured Remote Files** indicates the number of files that have a file resource record in the resource security file but actually exist on a remote system.

(Q) **Unused Secured Names** indicates the total number of files and libraries specified in the resource security file, but not defined on the system.

(R) **Total** indicates the total of all file, library, and group resource records in the resource security file.

(S) **User Records** indicates the total number of user records for files, libraries, and groups in the resource security file.

(T) **Other Records** indicates the number of folders, authorization lists, and user records for authorization lists in the resource security file.

(U) **Total Records Used** indicates the total number of records in the resource security file that contain security information.

(V) **Total Records Available** indicates the number of unused records in the resource security file.

(W) **Total Records Defined** indicates the size of the file in records. This number includes used and unused records.

(X) **File Size in Blocks** indicates the number of disk blocks the resource security file is using.

Sample Printout of Files, Libraries, and Groups by User ID

This example shows how a master security officer or a security officer lists in alphabetic order all of the user IDs and the files, libraries, and groups that users with those user IDs have access to. If a master security officer enters:

```
SECLIST RESOURCE,PRINTER,USERID,ALL
```

The printout shown in Figure 3-7 is printed on the printer assigned to the display station where the master security officer is running the procedure.

```
Resource Security by  User ID
User ID        LAG535

                                                    --- Children ---
User ID    Resource    Type        Log   Access     Number   Names
--------   --------    ----------  ---   ----------  ------  --------

********   FILE2       File        N     Read          0
ALEX       WARELIB     Library     N     Update        0
           FILE3       File        N     None          0
CHARLES    FILE3       File        N     Update        0
DENNIS     FILE1       File        Y     None          2     FILE2
                                                           FILE3
           PAY         Group       Y     Read          0
              .LIB1    Library
              .1       File
              .FOLD    Folder
           FILE4       Remote      N     Read          0
LAG535     WARELIB     Library     N     Owner         0
           FILE1       File        Y     Owner         2     FILE2
                                                           FILE3
           PAY         Group       Y     Owner         0
              .LIB1    Library
              .1       File
              .FOLD    Folder
           LAGLIB      Unused      Y     Owner         0
LKS        FILE1       File        Y     Change        2     FILE2
                                                           FILE3
Records In Resource Security File

Secured Libraries                                          1
Secured Alternative Index (AI) Files                       0
Secured Files                                              3
Secured Groups of resources                                1
Secured Remote Files                                       1
Unused Secured Names                                       1
                                                         -----
Total                                                      7

User Records                                              16
Other Records                                             27
                                                         -----
Total Records Used                                        50

Total Records Available                                   22
                                                         -----
Total Records Defined                                     72

File Size in Blocks                                        1
```

Figure 3-7. Sample Printout of Files, Libraries, and Groups by User ID

Description of Entries on the Sample Printout of Files, Libraries, and Groups by User ID

A **User ID** indicates the user ID of the user who ran the SECLIST RESOURCE procedure.

B **User ID** indicates the user ID of a user who has access to one or more secured files, libraries, or groups. The files, libraries, and groups this user has access to are listed in the resource column.

C **Resource** indicates the name of the secured file, library, or group this user can access.

If the secured resource is a group resource, the group identifier is listed. If a file, library, or folder is part of a group resource, the file, library, or folder is identified by the characters following the period within its name. For example, the payroll files could all be part of the group resource called PAY. If files PAY.LIB1, PAY.1, and PAY.FOLD are secured by the group resource record, they are identified within the list as .LIB1, .1, and .FOLD and appear immediately following the PAY entry.

D **Type** indicates the type of the resource:

AI FILE	Indicates that the resource is an alternative index file.
FILE	Indicates that the resource is a file.
FOLDER	Indicates that the resource is a folder.
GROUP	Indicates that the resource is a group resource.
LIBRARY	Indicates that the resource is a library.
REMOTE	Indicates that the resource is on a remote system.
UNUSED	Indicates that the resource is not on disk. That is, the file or library is specified in the resource security file, but the file or library does not actually exist on disk.

E **Log** indicates whether successful accesses to the file, library, or group are to be recorded in the history file. Y is yes; N is no.

F **Access** indicates the access level for each user ID.

G **Children Number** indicates the number of files or libraries that use this parent resource's user records.

H **Children Names** indicates the names of the files and libraries that use this parent resource's user records.

I **Secured Libraries** indicates the number of secured libraries in the resource security file.

J **Secured Alternative Index (AI) Files** indicates the number of secured alternative index files in the resource security file.

K **Secured Files** indicates the number of secured files in the resource security file.

(L) **Secured Groups of resources** indicates the number of secured groups of resources in the resource security file.

(M) **Secured Remote Files** indicates the number of files that have a file resource record in the resource security file but actually exist on a remote system.

(N) **Unused Secured Names** indicates the total number of files and libraries specified in the resource security file, but not defined on the system.

(O) **Total** indicates the total of all file, library, and group resource records in the resource security file.

(P) **User Records** indicates the total number of user records for files, libraries, and groups in the resource security file.

(Q) **Other Records** indicates the number of folders, authorization lists, and user records for authorization lists in the resource security file.

(R) **Total Records Used** indicates the total number of records in the resource security file that contain security information.

(S) **Total Records Available** indicates the number of unused records in the resource security file.

(T) **Total Records Defined** indicates the size of the file in records. This number includes used and unused records.

(U) **File Size in Blocks** indicates the number of disk blocks the resource security file is using.

Sample Printout of Files, Libraries, and Groups by Owner ID

This example shows how any user can list in alphabetic order the files, libraries, and groups that he or she owns. If the user enters:

```
SECLIST RESOURCE,PRINTER,OWNERID,USER
```

The printout shown in Figure 3-8 is printed on the printer assigned to the display station where the user is running the procedure.

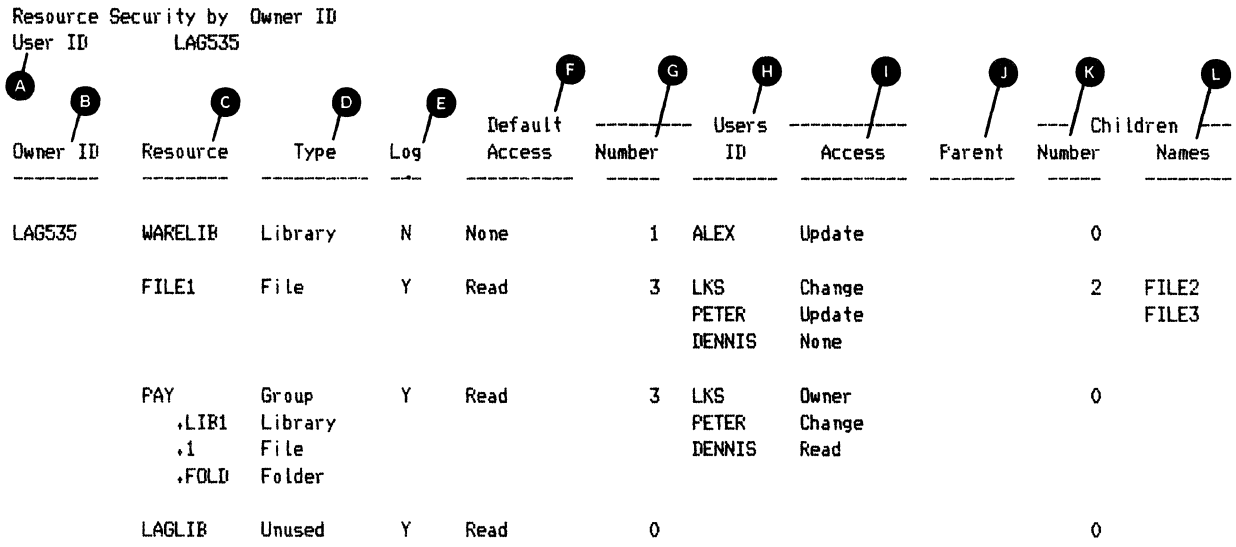


Figure 3-8. Sample Printout of Files, Libraries, and Groups by Owner ID

Description of Entries on Sample Printout of Files, Libraries, and Groups by Owner ID

Ⓐ **User ID** indicates the user ID of the user who ran the SECLIST RESOURCE procedure.

Ⓑ **Owner ID** indicates the owner of the resources listed in the resource column.

Ⓒ **Resource** indicates the name of the secured file, library, or group.

If the secured resource is a group resource, the group identifier is listed. If a file, library, or folder is part of a group resource, the file, library, or folder is identified by the characters following the period within its name. For example, the payroll files could all be part of the group resource called PAY. If files PAY.LIB1, PAY.1, and PAY.FOLD are secured by the group resource record, they are identified within the list as .LIB1, .1, and .FOLD and appear immediately following the PAY entry.

Ⓓ **Type** indicates the type of the resource:

AI FILE	Indicates that the resource is an alternative index file.
FILE	Indicates that the resource is a file.
FOLDER	Indicates that the resource is a folder.
GROUP	Indicates that the resource is a group resource.
LIBRARY	Indicates that the resource is a library.
REMOTE	Indicates that the resource is on a remote system.
UNUSED	Indicates that the resource is not on disk. That is, the file or library is specified in the resource security file, but the file or library does not actually exist on disk.

Ⓔ **Log** indicates whether successful accesses to the file, library, or group are to be recorded in the history file. Y is yes; N is no.

Ⓕ **Default Access** indicates the default access for the file or library.

Ⓖ **Users Number** indicates how many users are defined for the file or library.

Ⓗ **Users ID** indicates the user IDs.

Ⓘ **Users Access** indicates the access level for each user ID.

Ⓙ **Parent** indicates the name of the file or library whose user records are to be included with the indicated resource's user records.

Ⓚ **Children Number** indicates the number of files or libraries that use this parent resource's user records.

Ⓛ **Children Names** indicates the names of the files and libraries that use this parent resource's user records.

Listing Folder Security Information

How much folder or subdirectory security information you can print or display depends on:

- Whether password security is active
- Your security classification

If password security is active, a master security officer or a security officer can use the SECLIST RESFLDR procedure to list all folder or subdirectory security information. Any other user can use the SECLIST RESFLDR procedure to list only the information about the folders or subdirectories he or she owns or is authorized to access.

If password security is active, folder or subdirectory information in the resource security file can be requested from any display station. If password security is not active, anyone can use the SECLIST RESFLDR procedure to list all folder or subdirectory security information, but the procedure can be run only from the system console. If password security is not active, and the SECLIST RESFLDR procedure is run from a display station other than the system console, only the information about the folders or subdirectories that the user owns, or is authorized to access, can be listed.

Note: Security information about folder members cannot be listed because it is not stored in the resource security file.

To list folder or subdirectory information contained in the resource security file, do the following:

1. On the command display, type:

   ```
   SECLIST RESFLDR
   ```

   Press the Help key. The following display appears:

```
                              SECLIST PROCEDURE

          Lists the user identification or resource security file

Security information
  to be listed  . . . . . . . . . . USERID,RESOURCE,COMM,RESFLDR  RESFLDR

Print or display output . . . . . . . . . . . . . . PRINTER,CRT   PRINTER









Cmd3-Previous menu                                   COPR IBM Corp. 1986
```

S9042576

2. Type the device for the listing:

   PRINTER specifies that the output from the SECLIST RESFLDR procedure is to be printed on the printer assigned to your display station. PRINTER is the default, and is already displayed.

   CRT specifies that the output is to be displayed on your display screen.

   Press the Enter key.

   The following display appears:

```
                              SECLIST PROCEDURE

          Lists the user identification or resource security file

Security information
  to be listed  . . . . . . . . . . USERID,RESOURCE,COMM,RESFLDR  RESFLDR

Print or display output . . . . . . . . . . . . . . PRINTER,CRT   PRINTER

Order of security file  . . . . . . . . . .  OWNERID,RNAME,USERID   OWNERID

Type of information to be listed  . . . . . . . . . . .  USER,ALL   USER




Cmd2-Page back      Cmd4-Put on job queue                  COPR IBM Corp. 1986
```

S9042577

3. To indicate how you want the listing to be arranged, type one of the following:

   OWNERID specifies that authorization lists, secured folders, and subdirectories are to be listed alphabetically by the owner's user ID. OWNERID is the default, and is already displayed.

   You can list security information about the authorization lists, folders, and subdirectories for which you are listed as an owner. If you are a master security officer or a security officer, you can list all of the user IDs that have owner access to authorization lists, folders, and subdirectories.

   RNAME specifies that authorization lists, secured folders, and subdirectories are to be listed by resource name; that is, alphabetically by authorization list or folder name. If RNAME is specified, USER cannot be specified for the *Type of information to be listed* prompt.

   If you are a master security officer or a security officer, you can list security information about all of the authorization lists, secured folders, and subdirectories.

   USERID specifies that authorization lists, secured folders, and subdirectories are to be listed alphabetically by user ID.

   You can list security information about the folders or subdirectories for which you are listed as a user. If you are a master security officer or a security officer, you can list all of the user IDs and security information about the folders or subdirectories that users with those user IDs are authorized to access.

4. To indicate the type of information to be listed, type one of the following:

   USER specifies that only the entries for the user running the procedure are to be listed. This parameter is allowed only when OWNERID or USERID is specified. USER cannot be specified if RNAME is specified. USER is the default, and is already displayed.

   ALL specifies that all authorization lists, folder, and subdirectory security information in the resource security file is to be listed. You must be a master security officer or a security officer to specify ALL when password security is active.

   Press the Enter key.

The listing of authorization lists, secured folders, and subdirectories in the resource security file is printed or displayed on the device that you specified in step 2.

Sample Printout of Folders, Subdirectories, and Authorization Lists by Resource Name

This example shows how a master security officer or a security officer lists folder, subdirectory, and authorization list entries in the resource security file in alphabetic order by folder, subdirectory, or authorization list name. If a master security officer enters:

```
SECLIST RESFLDR,PRINTER,RNAME,ALL
```

The printout shown in Figure 3-9 is printed on the printer assigned to the display station where the master security officer is running the procedure.

Folder Resource Security by Resource Name
User ID DENNIS

A

B	C	D	E	F	G	H	I
	Users				Default	Authorization lists	
Resource	ID	Access	Type	Log	Access	Override	Primary
ACTION			Fldr	Y	None	DEPT48H	SALES
AUTH1	DENNIS	Owner	Auth				
	JOAN	Change					
	DANIEL	Update					
AUTH2	JOHN	Owner	Auth				
	PEGGY	Change					
	ELISE	Update					
DEPT48H	CHARLIE	Owner	Auth				
	DENNIS	Update					
	JANET	Update					
FOLDER1			Fldr	N	Read	AUTH1	AUTH2
/SUBDIR1			Subdir	N	None		AUTH2
/SUBDIR1/SUBDIR2/SUBDIR3/SUBDIR4/SUBDIR5/SUBDIR6/SUBDIR7			Subdir	Y	Update	AUTH2	AUTH1
FOLDER2			Fldr	Y	Update	AUTH1	AUTH2
PAY.FLDR			Fldr				
/CUSTOMER/EAST			Subdir	N	None		SALES
/CUSTOMER/WEST			Subdir	N	None		SALES
/SALES			Subdir	Y	None		DEPT48H
SALES	CHARLIE	Owner	Auth				
	KAREN	Read					
	KERRY	Read					
	BILL	None					
	JANET	None					

Records In Resource Security File

J	Folder records	3
K	Subdirectory records	12
L	Authorization list records	4
M	User records	14
N	Total	33
O	Other Records	2
P	Total Records Used	35
Q	Total Records Available	37
R	Total Records Defined	72
S	File Size in Blocks	1

Figure 3-9. Sample Printout of Folders, Subdirectory, and Authorization Lists by Resource Name

Description of Entries on Sample Printout of Folders, Subdirectories, and Authorization Lists by Resource Name

Ⓐ **User ID** indicates the user ID of the user who ran the SECLIST RESFLDR procedure.

Ⓑ **Resource** indicates the name of the authorization list, subdirectory, or secured folder.

Ⓒ **Users ID** indicates the user IDs of the users on the authorization list.

Ⓓ **Users Access** indicates the access level for each user on the authorization list.

Ⓔ **Type** indicates the type of the record:

Auth	Indicates that the record is for an authorization list.
Fldr	Indicates that the record is for a folder.
Subdir	Indicates that the record is for a subdirectory.

Ⓕ **Log** indicates whether successful accesses to the folder or subdirectory are to be recorded in the history file. Y is yes; N is no. Unsuccessful accesses are always recorded in the history file.

Ⓖ **Default Access** indicates the default access for the folder or subdirectory.

Ⓗ **Authorization lists, Override** indicates the name of the override authorization list securing the folder or subdirectory.

Ⓘ **Authorization lists, Primary** indicates the name of the primary authorization list securing the folder or subdirectory.

Ⓙ **Folders** indicates the number of secured folders in the resource security file.

Ⓚ **Subdirectory** indicates the number of secured subdirectories in the resource security file.

Ⓛ **Authorization lists** indicates the number of authorization lists in the resource security file.

Ⓜ **Users** indicates the number of user records for authorization lists in the resource security file.

Ⓝ **Total** indicates the total number of folders, subdirectories, authorization lists, and users on the authorization lists in the resource security file.

Ⓞ **Other Records** indicates the total number of other records in the resource security file.

Ⓟ **Total Records Used** indicates the total number of records in the resource security file that contain security information.

Q **Total Records Available** indicates the total number of unused records in the resource security file.

R **Total Records Defined** indicates the size of the file in records. This number includes used and unused records.

S **File Size in Blocks** indicates the number of disk blocks the resource security file is using.

Sample Printout of Folders, Subdirectories, and Authorization Lists by User ID

This example shows how a master security officer or a security officer lists in alphabetic order all of the user IDs and the folders, subdirectories, and authorization lists that users with those user IDs have access to. If a master security officer enters:

```
SECLIST RESFLDR,PRINTER,USERID,ALL
```

The printout shown in Figure 3-10 is printed on the printer assigned to the display station where the master security officer is running the procedure.

```
Folder Resource Security by User ID
User ID        DENNIS
```

(A) (B) (C) (D)

User ID	Access	Type	Resource
BILL	None	Auth	SALES
		Fldr	ACTION
			Folder- PAY.FLDR
		Subdir	/CUSTOMER/EAST
		Subdir	/CUSTOMER/WEST
CHARLIE	Owner	Auth	DEPT48H
		Fldr	ACTION
			Folder- PAY.FLDR
		Subdir	/SALES
	Owner	Auth	SALES
			Folder- PAY.FLDR
		Subdir	/CUSTOMER/EAST
		Subdir	/CUSTOMER/WEST
DANIEL	Update	Auth	AUTH1
		Fldr	FOLDER1
		Fldr	FOLDER2
			Folder- FOLDER1
		Subdir	/SUBDIR1/SUBDIR2/SUBDIR3/SUBDIR4/SUBDIR5/SUBDIR6/SUBDIR7
DENNIS	Owner	Auth	AUTH1
		Fldr	FOLDER1
		Fldr	FOLDER2
			Folder- FOLDER1
		Subdir	/SUBDIR1/SUBDIR2/SUBDIR3/SUBDIR4/SUBDIR5/SUBDIR6/SUBDIR7
	Update	Auth	DEPT48H
		Fldr	ACTION

Records In Resource Security File

(E) Folder records	3
(F) Subdirectory records	12
(G) Authorization list records	4
(H) User records	14
(I) Total	
(J) Other Records	2
(K) Total Records Used	35
(L) Total Records Available	37
(M) Total Records Defined	72
(N) File Size in Blocks	1

Figure 3-10. Sample Printout of Folders, Subdirectories, and Authorization Lists by User ID

Description of Entries on Sample Printout of Folders, Subdirectories, and Authorization Lists by User ID

(A) **User ID** indicates the user's ID.

(B) **Access** indicates the access level for the user.

(C) **Type** indicates the type of the record:

Auth	Indicates that the record is for an authorization list.
Fldr	Indicates that the record is for a folder.
Subdir	Indicates that the record is for a subdirectory.

(D) **Resource** indicates the name of the authorization list, secured folder, or subdirectory.

(E) **Folders** indicates the number of secured folders in the resource security file.

(F) **Subdirectory** indicates the number of secured subdirectories in the resource security file.

(G) **Authorization lists** indicates the number of authorization lists in the resource security file.

(H) **Users** indicates the number of user records for authorization lists in the resource security file.

(I) **Total** indicates the total number of folders, subdirectories, authorization lists, and users on the authorization lists in the resource security file.

(J) **Other Records** indicates the total number of other records in the resource security file.

(K) **Total Records Used** indicates the total number of records (office and other) in the resource security file that contain security information.

(L) **Total Records Available** indicates the total number of unused records in the resource security file.

(M) **Total Records Defined** indicates the size of the file in records. This number includes used and unused records.

(N) **File Size in Blocks** indicates the number of disk blocks the resource security file is using.

Sample Printout of Folders, Subdirectories, and Authorization Lists by Owner ID

This example shows how any user can list in alphabetic order the folders, subdirectories, and authorization lists that he or she owns. If the user enters:

```
SECLIST RESFLDR,PRINTER,OWNERID,USER
```

The printout shown in Figure 3-11 is printed on the printer assigned to the display station where the user is running the procedure.

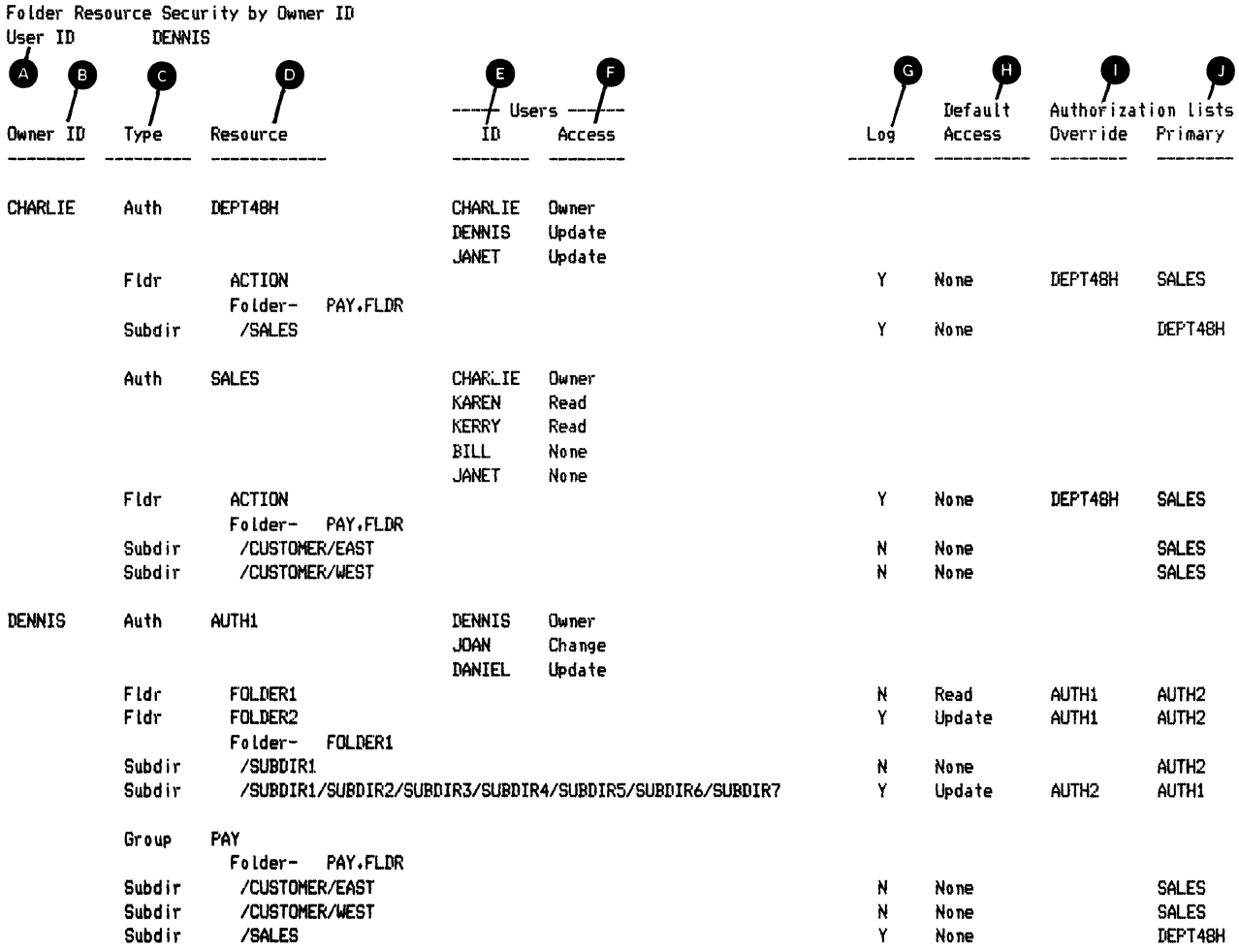


Figure 3-11. Sample Printout of Folders, Subdirectories, and Authorization Lists by Owner ID

Description of Entries on Sample Printout of Folders, Subdirectories, and Authorization Lists by Owner ID

Ⓐ **User ID** indicates the user ID of the user who ran the SECLIST RESFLDR procedure.

Ⓑ **Owner ID** indicates the owner of the resource.

Ⓒ **Type** indicates the type of the record:

Auth	Indicates that the record is for an authorization list.
Fldr	Indicates that the record is for a folder.
Subdir	Indicates that the record is for a subdirectory.

Ⓓ **Resource** indicates the name of the authorization list, secured folder, or subdirectory.

Ⓔ **Users ID** indicates the user IDs of the users on the authorization list.

Ⓕ **Users Access** indicates the access level for each user ID on the authorization list.

Ⓖ **Log All Accesses** indicates whether successful accesses to the folder or subdirectory are to be recorded in the history file. Y is yes; N is no.

Ⓗ **Default Access** indicates the default access for the folder or subdirectory.

Ⓘ **Authorization lists, Override** indicates the name of the override authorization list securing the folder or subdirectory.

Ⓙ **Authorization lists, Primary** indicates the name of the primary authorization list securing the folder or subdirectory.

Saving the Resource Security File

You should consider making a copy of the resource security file in case the original resource security file is somehow damaged or destroyed. The copy allows you to recover from intentional or unintentional destruction of your security information. The SECSAVE procedure allows you to copy the resource security file onto diskette, tape, tape cartridge, or onto another area on disk.

If password security is active, a master security officer can run the SECSAVE procedure from any display.

If password security is not active, anyone can run the SECSAVE procedure, but only from the system console.

Saving Copies on Diskette

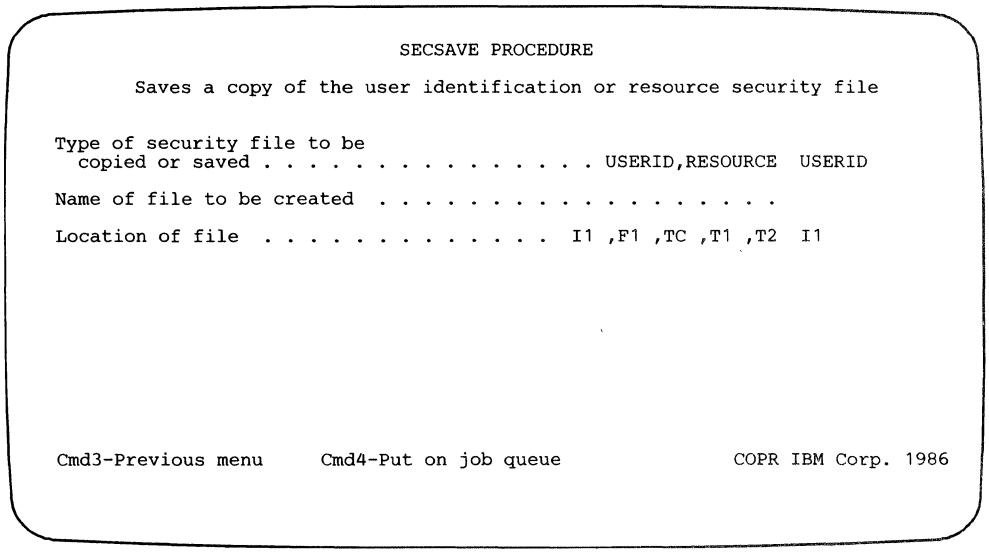
To copy the resource security file onto diskette, do the following:

1. On the command display, type:

   SECSAVE

   Press the Help key.

   The following display appears:



S9042578

2. Type RESOURCE over USERID.

3. Type a name for the file to be created. For example, you could call the copy RESFILE (resource security file).

4. You do not have to type the location of the file. I1 (the default value) indicates that the file is to be copied onto diskette.

   Press the Enter key.

   The following display appears:

```
                              SECSAVE PROCEDURE

        Saves a copy of the user identification or resource security file

Type of security file to be
  copied or saved . . . . . . . . . . . . . . . USERID,RESOURCE  RESOURCE

Name of file to be created  . . . . . . . . . . . . . . . . . . RESFILE

Location of file  . . . . . . . . . . . . . . I1 ,F1 ,TC ,T1 ,T2  I1

Volume ID of diskette . . . . . . . . . . . . . . . . . . . . .

Retention days  . . . . . . . . . . . . . . . . . . . . . . . . 1-999  999

Location of diskette  . . . . . . . . . . . S1,S2,S3,M1.nn,M2.nn  S1

Automatic advance to next slot or magazine  . . . . NOAUTO,AUTO  NOAUTO


Cmd2-Page back      Cmd4-Put on job queue                  COPR IBM Corp. 1986
```

S9042579

5. Type the following information:

   a. The volume ID of the diskette that is to receive the copy. A volume ID must be specified.
   b. The number of days the diskette file is to be retained, any decimal number from 1 through 999. If you do not specify the number of retention days, 999 days are assumed. If 999 days are entered or assumed, the file is a permanent diskette file.
   c. The diskette slot or diskette magazine location containing the first diskette to be used. Any of the following can be specified:

      S1, S2, or *S3* specifies the diskette slot containing the first diskette to be used.

      M1.nn or *M2.nn* specifies the magazine location containing the first diskette to be used. M1 indicates the first magazine location, and M2 indicates the second magazine location. **nn** is a decimal number from 01 through 10 that identifies the location of the diskette in the magazine. Specifying M1 is the same as specifying M1.01; specifying M2 is the same as specifying M2.01.

   d. Whether the system is to automatically advance to the next diskette slot or magazine location. You can specify either AUTO or NOAUTO:

      NOAUTO specifies the following:
      1) If S1, S2, or S3 is specified, only the specified slot (S1, S2, or S3) is used. If more diskettes need to be processed, a message is displayed and you must insert the next diskette into the slot being used.
      2) If M1.nn or M2.nn is specified, only the specified magazine location (M1 or M2) is used. Processing begins with the diskette at the specified location within the magazine and continues through the last diskette in the magazine. If more diskettes need to be processed, a message is displayed and you must then insert the next magazine in the magazine location being used. Processing resumes at the first diskette location in the magazine.

      AUTO specifies the following:
      1) If S1, S2, or S3 is specified, all three slots (S1, S2, and S3) are used. Processing begins with the diskette in the specified slot and continues through the diskette in slot S3. If more diskettes need to be processed, a message is displayed and you must then insert the next diskettes. Processing resumes with the diskette in slot S1.
      2) If M1.nn or M2.nn is specified, both magazine locations (M1 and M2) are used. Processing begins with the diskette at the specified location and continues through the diskette in location M2.10. If more diskettes need to be processed, a message is displayed and you must then insert the next magazines. Processing resumes at location M1.01 and continues through M2.10.

Press the Enter key.

The SECSAVE procedure copies the resource security file onto diskette, and the procedure ends.

Example of Copying the Resource Security File on Diskette

This example shows the procedure and parameters a master security officer can use to copy the resource security file onto diskette. The volume ID of the diskette is VOL001, and the diskette is located in diskette slot S1. The name of the diskette file is RESFILE; the diskette file will be retained for 60 days.

```
SECSAVE RESOURCE,RESFILE,I1,VOL001,60,S1,NOAUTO
```

Saving Copies on Tape or Tape Cartridge

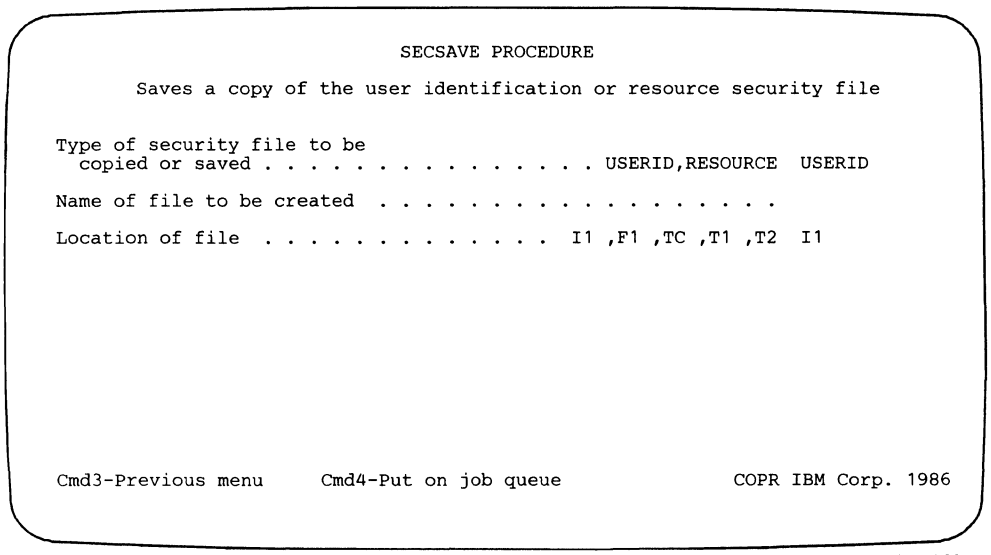
To copy the resource security file onto tape or tape cartridge, do the following:

1. On the command display, type:

   ```
   SECSAVE
   ```

   Press the Help key.

   The following display appears:



S9042580

2. Type RESOURCE over USERID.

3. Type a name for the file to be created. For example, you could call the copy RESFILE (resource security file).

4. Type T1 to specify that the file is to be copied onto a tape on the first tape drive, T2 to specify that the file is to be copied onto a tape on the second tape drive, or TC to specify that the file is to be copied onto a tape cartridge. You must type over the system default shown.

   Press the Enter key.

   The following display appears:

```
                              SECSAVE PROCEDURE

        Saves a copy of the user identification or resource security file

Type of security file to be
  copied or saved . . . . . . . . . . . . . . . . USERID,RESOURCE  RESOURCE

Name of file to be created  . . . . . . . . . . . . . . . . . . .  RESFILE

Location of file  . . . . . . . . . . . . . .  I1 ,F1 ,TC ,T1 ,T2  T1

Volume ID of tape . . . . . . . . . . . . . . . . . . . . . . . .

Retention days  . . . . . . . . . . . . . . . . . . . . . . . . . 1-999  999

Automatic advance to next tape drive  . . . . . . . . NOAUTO,AUTO  NOAUTO

End position of tape drive  . . . . . . . . . REWIND,LEAVE,UNLOAD  REWIND


Cmd2-Page back      Cmd4-Put on job queue                  COPR IBM Corp. 1986
```

S9042581

5. Type the following information:

   a. The volume ID of the tape or tape cartridge that is to receive the copy. A volume ID must be specified.
   b. The number of days the tape or tape cartridge file is to be retained, any decimal number from 1 through 999. If you do not specify the number of retention days, 999 days are assumed. If 999 days are entered or assumed, the file is a permanent tape file.
   c. Whether the system is to automatically advance to the next tape drive if the end of the first tape is reached:

      NOAUTO specifies that if the end of the tape is reached on the selected tape drive, processing continues with the same tape drive. If more tapes need to be processed, a message is displayed, and you must mount the next tape on the selected tape drive.

      Note: NOAUTO, the system default value, must be used if you are saving the resource security file on a tape cartridge.

      AUTO specifies that both tape drives can be used. If the end of the tape is reached on the selected tape drive, processing continues with the tape on the other tape drive. If the other drive is not available, the first drive is used again. If more tapes need to be processed, a message is displayed, and you must mount the next tape on the appropriate tape drive.

   d. The end position of the tape drive after the resource security file is copied. Any of the following can be specified:

      REWIND rewinds the tape to the beginning of the tape.

      LEAVE leaves the tape positioned at the end of the copied security file.

      UNLOAD rewinds the tape to the beginning and unloads the tape.

      Note: UNLOAD is defaulted to REWIND if you are saving the resource security file on a tape cartridge.

Press the Enter key.

The SECSAVE procedure copies the security file onto tape or tape cartridge, and the procedure ends.

Example of Copying the Resource Security File on Tape

This example shows the procedure and parameters a master security officer can use to copy the resource security file onto tape. The name of the tape file is RESFILE, the file will be copied to the tape on the first tape drive, both tape drives can be used if necessary, and the system will leave the tape positioned after the copied file.

```
SECSAVE RESOURCE,RESFILE,T1,VOL001,999,,AUTO,LEAVE
```

Saving Copies on Disk

To copy the resource security file onto another area on disk, do the following:

1. On the command display, type:

   SECSAVE

   Press the Help key.

   The following display appears:

```
                              SECSAVE PROCEDURE
        Saves a copy of the user identification or resource security file

Type of security file to be
  copied or saved . . . . . . . . . . . . . . . USERID,RESOURCE  USERID

Name of file to be created  . . . . . . . . . . . . . . . . . . .

Location of file  . . . . . . . . . . . . . .  I1 ,F1 ,TC ,T1 ,T2  I1









Cmd3-Previous menu      Cmd4-Put on job queue                COPR IBM Corp. 1986
```

S9042582

2. Type RESOURCE over USERID.

3. Type a name for the file to be created. For example, you could call the copy RESFILE (resource security file).

4. Type F1 to specify that the file is to be copied to another area on disk. You must type over the system default shown.

   Press the Enter key.

   The SECSAVE procedure copies the resource security file onto another area on disk, and the procedure ends.

Example of Copying the Resource Security File to Another Area on Disk

This example shows the procedure and parameters the master security officer can use to copy the resource security file into a disk file. The name of the disk file is RESFILE.

```
SECSAVE RESOURCE,RESFILE,F1
```

Restoring the Resource Security File

The SECREST procedure restores the resource security file with the copy that was created by the SECSAVE procedure.

When restoring the resource security file, it is not necessary to deactivate resource security, activate resource security, or perform an IPL. The resource security file that is currently on disk is replaced with the version created by the SECSAVE procedure.

If password security is active, a master security officer can run the SECREST procedure from any display station.

If password security is not active, anyone can run the SECREST procedure, but only from the system console.

Restoring Copies from Diskette

To restore the resource security file from diskette, do the following:

1. On the command display, type:

   SECREST

   Press the Help key.

   The following display appears:

```
                          SECREST PROCEDURE                    Optional-*
        Restores the user identification or resource security file

Security file to restore  . . . . . . . . . . . USERID,RESOURCE  USERID
Name of file to be restored . . . . . . . . . . . . . . . . . .
Size of file in records . . . . . . . . . . . . . . . . . . . .            *
Creation date of file to be restored  . . . . . . . . . . . . .            *
Location of file  . . . . . . . . . . . . . . I1 ,F1 ,TC ,T1 ,T2  I1




Cmd3-Previous menu                                  COPR IBM Corp. 1986
```

S9042583

2. Type RESOURCE over USERID.

3. Type the following information:

   a. The name of the diskette file that contains the copy of the resource security file that was created by the SECSAVE procedure. If the specified diskette file does not contain a copy of a resource security file, an error message is displayed.
   b. The number of records to allow in the newly restored resource security file. This number can be any decimal number from 72 through 63,992 for the resource security file. If the number you enter is too large for the system or too small to contain all the copied records, an error message is displayed. If no number is specified, the number of records that were copied is used.

      Note: The number of records in the newly restored resource security file might differ slightly from the number you specify. That is because the system rounds the number of records to the next greatest multiple of 80, and then subtracts 8. For example, if you specify 500 records, the actual number of records in the file will be 552 (that is, 560 - 8).

   c. The creation date of the diskette file that contains the copied resource security file. If no creation date is specified, and if more than one diskette file exists with the specified file name, the first (oldest) file is used.

      *Note: The creation date entered must be in the current session date format, either month-day-year (**mmddyy**), day-month-year (**ddmmyy**), or year-month-day (**yymmdd**). You can use the STATUS SESSION command to determine the session date format.*

   d. You do not have to type the location of the file. I1 (default value) indicates that the file is to be copied from diskette.

   Press the Enter key.

   The following display appears:

```
                          SECREST PROCEDURE                    Optional-*
        Restores the user identification or resource security file

Security file to restore  . . . . . . . . . . . USERID,RESOURCE  RESOURCE
Name of file to be restored . . . . . . . . . . . . . . . . . .  RESFILE
Size of file in records . . . . . . . . . . . . . . . . . . . .  100        *
Creation date of file to be restored  . . . . . . . . . . . . .           *
Location of file  . . . . . . . . . . . . . I1 ,F1 ,TC ,T1 ,T2   I1
Volume ID of diskette . . . . . . . . . . . . . . . . . . . . .           *
Location of diskette  . . . . . . . . . . . S1,S2,S3,M1.nn,M2.nn  S1
Automatic advance to next slot or magazine  . . . . AUTO,NOAUTO  NOAUTO


Cmd2-Page back     Cmd4-Put on job queue              COPR IBM Corp. 1986
```

S9042584

4. Type the following information:

   a. The volume ID of the diskette that contains the copied resource security file. If no volume ID is specified, the file is copied from the diskette in the specified location.
   b. The diskette slot or diskette magazine location containing the first diskette to be used. Any of the following can be specified:

      S1, S2, or *S3* specifies the diskette slot containing the first diskette to be used.

      M1.nn or *M2.nn* specifies the magazine location containing the first diskette to be used. M1 indicates the first magazine location, and M2 indicates the second magazine location. **nn** is a decimal number from 01 through 10 that identifies the location of the diskette in the magazine. Specifying M1 is the same as specifying M1.01; specifying M2 is the same as specifying M2.01.

   c. Whether the system is to automatically advance to the next diskette slot or magazine location. You can specify either AUTO or NOAUTO:

      NOAUTO specifies the following:
      1) If S1, S2, or S3 is specified, only the specified slot (S1, S2, or S3) is used. If more diskettes need to be processed, a message is displayed and you must then insert the next diskette into the slot being used.
      2) If M1.nn or M2.nn is specified, only the specified magazine location (M1 or M2) is used. Processing begins with the diskette at the specified location within the magazine and continues through the last diskette in the magazine. If more diskettes need to be processed, a message is displayed and you must insert the next magazine in the magazine location being used. Processing resumes at the first location in the magazine.

      AUTO specifies the following:
      1) If S1, S2, or S3 is specified, all three slots (S1, S2, and S3) are used. Processing begins with the diskette in the specified slot and continues through the diskette in slot S3. If more diskettes need to be processed, a message is displayed and you must insert the next diskettes. Processing resumes with the diskette in slot S1.
      2) If M1.nn or M2.nn is specified, both magazine locations (M1 and M2) are used. Processing begins with the diskette at the specified location and continues through the diskette in location M2.10. If more diskettes need to be processed, a message is displayed and you must insert the next magazines. Processing resumes at location M1.01 and continues through M2.10.

      Press the Enter key.

      The resource security file is restored by the SECREST procedure, the procedure ends, and a message is sent to the system console indicating that the resource security file was restored.

Example of Restoring the Resource Security File from Diskette

This example shows the procedure and parameters a master security officer can use to restore the resource security file from a copy on diskette. The name of the diskette file is RESFILE, the size of the resource security file is to be 200 records, the volume ID of the diskette is VOL001, and the diskette is located in diskette slot S1.

```
SECREST RESOURCE,RESFILE,200,,I1,VOL001,S1,NOAUTO
```

Restoring Copies from Tape or Tape Cartridge

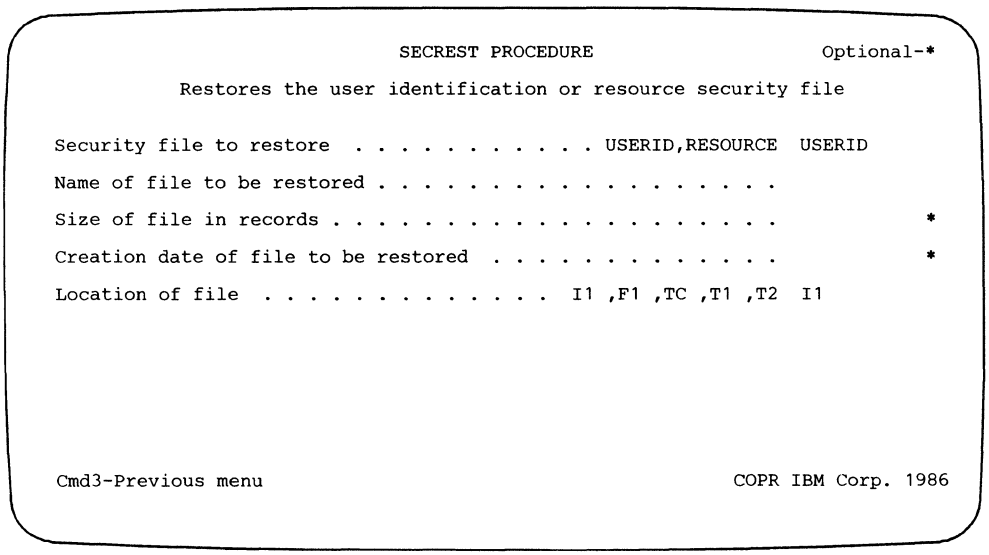
To restore the resource security file from tape or tape cartridge, do the following:

1. On the command display, type:

   ```
   SECREST
   ```

   Press the Help key.

   The following display appears:



S9042585

2. Type RESOURCE over USERID.

3. Type the following information:

   a. The name of the file that contains the copy of the resource security file that was created by the SECSAVE procedure. If the specified file does not contain a copy of a resource security file, an error message is displayed.
   b. The number of records to allow in the newly restored resource security file. This number can be any decimal number from 72 through 63,992 for the resource security file. If the number you enter is too large for the system or too small to contain all the records, an error message is displayed. If no number is specified, the number of records that were copied is used.

      Note: The number of records in the newly restored resource security file might differ slightly from the number you specify. That is because the system rounds the number of records to the next greatest multiple of 80, and subtracts 8. For example, if you specify 500 records, the actual number of records in the file will be 552 (that is, 560 - 8).

   c. The creation date of the tape or tape cartridge file that contains the copied resource security file. If no creation date is specified, and if more than one tape or tape cartridge file exists with the specified file name, the first (oldest) file is used.

      *Note: The creation date entered must be in the current session date format, either month-day-year (**mmddyy**), day-month-year (**ddmmyy**), or year-month-day (**yymmdd**). You can use the STATUS SESSION command to determine the session date format.*

d. T1 to specify that the file is to be copied from a tape on the first tape drive, T2 to specify that the file is to be copied from a tape on the second tape drive, or TC to specify that the file is to be copied from a tape cartridge. You must type over the system default shown.

Press the Enter key.

The following display appears:

```
                              SECREST PROCEDURE                    Optional-*
          Restores the user identification or resource security file

Security file to restore  . . . . . . . . . . . USERID,RESOURCE  RESOURCE
Name of file to be restored . . . . . . . . . . . . . . . . . .  RESFILE
Size of file in records . . . . . . . . . . . . . . . . . . . .  100        *
Creation date of file to be restored  . . . . . . . . . . . . .            *
Location of file  . . . . . . . . . . . . . .  I1 ,F1 ,TC ,T1 ,T2  T1
Volume ID of tape . . . . . . . . . . . . . . . . . . . . . . .            *
Automatic advance to next tape drive  . . . . . . . . AUTO,NOAUTO  NOAUTO
End position of tape drive  . . . . . . . . . REWIND,LEAVE,UNLOAD  REWIND


Cmd2-Page back     Cmd4-Put on job queue                COPR IBM Corp. 1986
```

S9042586

4. Type the following information:

   a. The volume ID of the tape or tape cartridge that contains the copied resource security file. If no volume ID is specified, the file is copied from the tape in the specified location.
   b. Whether the system is to automatically advance to the next tape drive if the end of the first tape is reached:

      NOAUTO specifies that if the end of the tape is reached on the selected tape drive, processing continues with the same tape drive. If more tapes need to be processed, a message is displayed and you must then mount the next tape on the selected tape drive.

      Note: NOAUTO, the system default value, must be used if you are restoring the resource security file from a tape cartridge.

      AUTO specifies that both tape drives can be used. If the end of the tape is reached on the selected tape drive, processing continues with the tape on the other tape drive. If the other drive is not available, the first drive is used again. If more tapes need to be processed, a message is displayed and you must then mount the next tape on the selected tape drive.

   c. The end position of the tape drive after the resource security file is restored. Any of the following can be specified:

      REWIND rewinds the tape to the beginning of the tape.

      LEAVE leaves the tape positioned at the end of the restored resource security file.

      UNLOAD rewinds the tape to the beginning and unloads the tape.

      Note: UNLOAD is defaulted to REWIND if you are restoring the resource security file from a tape cartridge.

   Press the Enter key.

   The resource security file is restored by the SECREST procedure, the procedure ends, and a message is sent to the system console indicating that the resource security file was restored.

Example of Restoring the Resource Security File from Tape

This example shows the procedure and parameters a master security officer can use to restore the resource security file from tape. The name of the tape file is RESFILE, the size of the restored resource security file is to be 200 records, its creation date is December 4, 1983, the file is to be restored from the tape on the first tape drive, both tape drives can be used if necessary, and the system will leave the tape positioned after the restored file.

```
SECREST RESOURCE,RESFILE,200,120483,T1,,,AUTO,LEAVE
```

Restoring Copies from Disk

To restore the resource security file from disk, do the following:

1. On the command display, type:

   SECREST

   Press the Help key.

   The following display appears:

```
                              SECREST PROCEDURE                    Optional-*
          Restores the user identification or resource security file

Security file to restore  . . . . . . . . . . . USERID,RESOURCE  USERID
Name of file to be restored . . . . . . . . . . . . . . . . . .
Size of file in records . . . . . . . . . . . . . . . . . . . .          *
Creation date of file to be restored  . . . . . . . . . . . . .          *
Location of file  . . . . . . . . . . . . . . I1 ,F1 ,TC ,T1 ,T2  I1




Cmd3-Previous menu                                   COPR IBM Corp. 1986
```

S9042587

2. Type RESOURCE over USERID.

3. Type the following information:

   a. The name of the disk file that contains the copy of the resource security file that was created by the SECSAVE procedure. If the specified disk file does not contain a copy of a resource security file, an error message is displayed.
   b. The number of records to allow in the newly restored resource security file. This number can be any decimal number from 72 through 63,992 for the resource security file. If the number you enter is too large for the system or too small to contain all the records, an error message is displayed. If no number is specified, the number of records that were copied is used.

      Note: The number of records in the newly restored resource security file might differ slightly from the number you specify. That is because the system rounds the number of records to the next greatest multiple of 80, then subtracts 8. For example, if you specify 500 records, the actual number of records in the file will be 552 (that is, 560 - 8).

   c. The creation date of the disk file that contains the copied resource security file. If no creation date is specified, and if more than one disk file exists with the specified file name, the first (oldest) file is used.

      *Note: The creation date entered must be in the current session date format, either month-day-year (**mmddyy**), day-month-year (**ddmmyy**), or year-month-day (**yymmdd**). You can use the STATUS SESSION command to determine the session date format.*

   d. F1 to specify that the file is to be copied from a disk file. You must type over the system default shown.

Press the Enter key.

The SECREST procedure restores the resource security file, the procedure ends, and a message is sent to the system console indicating that the resource security file was restored.

Example of Restoring the Resource Security File from a Disk File

This example shows the procedure and parameters a master security officer can use to restore the resource security file from a disk file. The name of the disk file is RESFILE, the size of the restored resource security file is to be 200 records, and its creation date is December 4, 1983.

```
SECREST RESOURCE,RESFILE,200,120483,F1
```

Changing the Size of the Resource Security File

You can increase the size of the resource security file if you want to. However, the system will increase the size of the resource security file when all the blank resource records are used, providing there is enough disk space available and the resource security file has not reached its maximum allowable size (63,992 records).

At some point, you might need to make available a certain amount of disk space. You can do so by decreasing the size of the resource security file by removing records you no longer need, then following these steps:

1. Run the SECDEF procedure to determine the current size of the resource security file. Enter the following:

   ```
   SECDEF RESOURCE,CREATE
   ```

   The size of the resource security file is displayed. Press command key 3 to end the SECDEF procedure.

2. Run the SECSAVE procedure to copy the resource security file onto a temporary disk file. For example:

   ```
   SECSAVE RESOURCE,TEMPRES,F1
   ```

   See "Saving the Resource Security File" earlier in this chapter for more information about the SECSAVE procedure.

3. Run the SECREST procedure to restore the temporary file back to the resource security file. When you run the SECREST procedure, you can specify a new size for the resource security file. To increase the size of the file, specify a number of records greater than the number of records contained in the original resource security file. To decrease the size of the file, specify a number of records fewer than the number of records contained in the original resource security file. If the specified size is too small to hold all the records in the file, a message is displayed with an option to make the file just large enough to contain the resource records and the user records.

   For example, if the current size of the file is 600, you can decrease that size to 500 by entering the following:

   ```
   SECREST RESOURCE,TEMPRES,500,,F1
   ```

   Note: The number of records in the newly restored resource security file might differ slightly from the number you specified in the SECREST procedure. That is because the system rounds the number of records to the next greatest multiple of 80, then subtracts 8. For example, if you specify 500 records, the actual number of records in the file will be 552 (that is, 560 - 8).

   For more information about the SECREST procedure, see "Restoring the Resource Security File" earlier in this chapter.

4. Use the DELETE procedure to remove the temporary file from the system. For example:

```
DELETE TEMPRES,F1
```

The DELETE procedure removes files from the system. For more information about the DELETE procedure, see the manual *System Reference*.

Deactivating Resource Security

If you deactivate resource security, although the resource security file still exists, your files, libraries, and folders are no longer secure, and anyone can access the information in those resources.

Care should be taken when you deactivate resource security. You should carefully evaluate whether unauthorized access to your data might cause you problems.

If you deactivate resource security, the resource security file remains on disk and information in the file is unchanged. When resource security is deactivated, information in the user ID file is also unchanged, and password security, menu security, communications security, and badge security are not affected. For example, if password security was active, it remains active.

You can deactivate resource security by running the SECDEF procedure. If password security is active, a master security officer can run the SECDEF procedure from any display station to deactivate resource security. If password security is not active, anyone can run the SECDEF procedure, but only from the system console.

To deactivate resource security, do the following:

1. On the command display, type:

   SECDEF

   Press the Help key.

   The following display appears:

```
                              SECDEF PROCEDURE

            Creates or removes the user identification file; creates
            or removes the resource security file; or activates
            or deactivates password, resource, or badge security.


Security type . . . . . . . . . . . . . . . . . USERID,RESOURCE  USERID









Cmd3-Previous menu                                        COPR IBM Corp. 1985
```

S9042588

2. Because you want to deactivate resource security, and because resource security uses the resource security file, type RESOURCE over USERID.

   Press the Enter key.

   The following display appears:

```
                              SECDEF PROCEDURE

              Creates or removes the user identification file; creates
              or removes the resource security file; or activates
              or deactivates password, resource, or badge security.

Security type . . . . . . . . . . . . . . . . . USERID,RESOURCE  RESOURCE

Option  . . . . . . . . . . . . . ACTRES,CREATE,DEACTRES,DELETE            *




Cmd2-Page back                                          COPR IBM Corp. 1985
```

S9042589

3. Using the display shown in step 2, you can choose one of several tasks:

   Activate resource security
   Create the resource security file
   Deactivate resource security
   Delete the resource security file

   Because you want to deactivate resource security, type DEACTRES, and press the Enter key.

   The following display appears:

```
                SECDEF: Deactivate resource security                    W1

                          ****************
                          **  WARNING  ***
                          ****************


                    Resource security is about to be deactivated.  If
                    you press the Enter key resource security will no
                    longer be active at the next IPL.  However, the
                    security information will remain in the
                    resource security file.


          Press the Enter key to schedule resource security to be deactivated.



     Cmd3-Return to previous menu          Cmd7-Cancel this request
                                                    COPR IBM Corp. 1985
```

S9042590

4. If you decide not to deactivate resource security, press command key 7. The SECDEF procedure does not deactivate resource security, and the procedure ends.

   To deactivate resource security, press the Enter key. The system displays a message indicating that resource security will be deactivated at the next IPL. To complete the SECDEF procedure, press command key 3 or the Enter key.

Resource security is deactivated after you IPL the system. For information on how to perform an IPL, see the manual *Operating Your System*.

Removing the Resource Security File from Disk

The resource security file can be removed from the system by using the SECDEF procedure. If password security is active, a master security officer can run the SECDEF procedure from any display station. If password security is not active, anyone can run the SECDEF procedure to remove the resource security file, but only from the system console.

Note: Before you remove the resource security file, we recommend that you create a copy on diskette, tape, or tape cartridge (see "Saving the Resource Security File" earlier in this chapter), or create a listing of the file (see "Listing the Resource Security File" earlier in this chapter). This will help you restore or rebuild the resource security file should you decide to use resource security again in the future.

You must deactivate resource security before you remove the resource security file. See "Deactivating Resource Security" earlier in this chapter for information about deactivating resource security.

Note: If you deactivate resource security and remove the resource security file, then restore a different resource security file and activate resource security again, any files that were secured by the first resource security file that do not have records in the second resource security file are still secured. When you attempt to access these files, you receive a message that information is missing from the resource security file, and you are not allowed to access the files. A master security officer or a security officer must enter information into the resource security file for those files before they can be accessed. This is something you might want to keep in mind if you ever use two different resource security files.

To remove the resource security file, do the following:

1. On the command display, type:

   SECDEF

   Press the Help key.

   The following display appears:

```
                              SECDEF PROCEDURE

            Creates or removes the user identification file; creates
            or removes the resource security file; or activates
            or deactivates password, resource, or badge security.

Security type . . . . . . . . . . . . . . . . . USERID,RESOURCE  USERID




Cmd3-Previous menu                                        COPR IBM Corp. 1985
```

S9042591

2. Because you want to remove the resource security file, type RESOURCE over USERID.

   Press the Enter key.

   The following display appears:

```
                              SECDEF PROCEDURE

            Creates or removes the user identification file; creates
            or removes the resource security file; or activates
            or deactivates password, resource, or badge security.

Security type . . . . . . . . . . . . . . . . . USERID,RESOURCE  RESOURCE
Option  . . . . . . . . . . . . . ACTRES,CREATE,DEACTRES,DELETE            *




Cmd2-Page back                                            COPR IBM Corp. 1985
```

S9042592

3. Using the display shown in step 2, you can choose one of several tasks:

   Activate resource security
   Create the resource security file
   Deactivate resource security
   Delete the resource security file

   Because you want to remove the resource security file, type DELETE, and press the Enter key.

   The following display appears:

```
SECDEF: Remove the resource security file                    W1

                **********
                **  WARNING  ***
                **********

          The resource security file currently exists.

          If you continue, it will be removed and all
          records in it will be erased.  If you wish to
          save a copy of the resource security file
          before removing it, use the SECSAVE utility.


       Press the Enter key to remove the resource security file.



Cmd3-Return to previous menu          Cmd7-Cancel this request
                                                COPR IBM Corp. 1985
```

S9042593

4. If you decide not to remove the resource security file, press command key 7. The SECDEF procedure does not remove the resource security file, and the SECDEF procedure ends.

   To remove the resource security file, press the Enter key. The system displays a message indicating that the resource security file was removed. To complete the SECDEF procedure, press command key 3 or the Enter key.

Appendix A. Required Access Levels for Using the System Programming

This appendix shows the required access levels an operator must have to use the system programming. The required access levels are shown for:

- User programs
- OCL statements and procedure control expressions
- Procedures and commands

Use this appendix to determine the minimum access levels required to run programs or procedures that use secured files and libraries.

For example, suppose an entry in the resource security file is used to secure a file named NEWFILE, which is not yet created. The FILE OCL statement or the BLDFILE procedure is used to create NEWFILE. If you did not know the required access level to create the file using the FILE statement or the BLDFILE procedure, you could use this appendix to look up the access level. You would find that the operator who attempts to create the file must have a minimum access level of change (C).

Access Levels for User Programs

To create a new file, an operator must have an access level of *change* or *owner*.

To add, change, or remove records from a file, an operator must have an access level of *update*, *change*, or *owner*.

To read records from a file, an operator must have an access level of *read*, *update*, *change*, or *owner*.

OCL Statements and Procedure Control Expressions

Statement	Minimum Access Level
COMM	**Run** access to the library that contains the program for which the operator is assigning a communications line or a phone list.
COMPILE	**Read** access to the input library; **update** access to the output library.
EVOKE	**Run** access to the library containing the procedure that is to be started (evoked).
FILE	**Change** access to create a new file. **Read** access to read records from a file. **Update** access to add, change, or delete records from a file.
IMAGE	**Read** access to the library that contains the print belt image member or the translation table member.
INCLUDE	**Run** access to the library that contains the procedure member to be placed into the job stream.
JOBQ	**Run** access to the library that contains the procedure to be placed on the job queue.
LIBRARY	**Run** access to the library that is to be the session library.
LOAD	**Run** access to the library that contains the program that is to be loaded.
MEMBER	**Run** access to the library that contains the message member to be used for the procedure or program.
MENU	**Run** access to the library that contains the menu that is to be displayed.
PROMPT	**Run** access to the library that contains the display format member.
IF SOURCE	**Run** access to the library that contains the member that is to be tested.
IF PROC	**Run** access to the library that contains the member that is to be tested.
IF LOAD	**Run** access to the library that contains the member that is to be tested.
IF SUBR	**Run** access to the library that contains the member that is to be tested.
RESET	**Run** access to the library that contains the procedure to be called.

Procedures and Commands

The following chart lists some tasks involving procedures and commands that use secured resources and the minimum access level required to use the resource.

Tasks Using a Secured Resource	Minimum Access Level
Archiving	Read
Browsing/viewing	Read
Changing physical size	Change
Compiling a program	Read access to library containing source members
	Update access to library containing object members
Condensing	Update
Copying	Read access to resource being copied
	Update access to resource receiving data
Creating a secured resource (file, library, or folder)	Change
Creating library members or folder members	Update
Deleting a secured resource	Change
Displaying menus	Run
Enabling a subsystem	Read access to library containing subsystem's configuration member
Placing jobs on job queue	Run
Printing/listing	Read
Removing folder members	Update access to folder and folder member
Removing library members	Update access to library
Renaming	Update access for folder members; owner access for all other resources
Restoring	Change
Running a program or procedure	Run
Saving	Read
Sorting	Read access to file being sorted
	Change access to file being created
	Run access to library containing sort specifications
	Update access to output file if file already exists
Updating/changing data in resource	Update

Appendix B. Planning Forms for the Security Files

This page is intentionally left blank.

User Identification Form

Customer Name _____
Customer Number _____

Name _____

Position _____

Responsibilities _____

_____

Optional=*

User ID _ _ _ _ _ _ _ _

Password _ _ _ _

Security classification? _
(M, S, O, C, D)

Service aid authority? _
(Y, N)

*Default sign-on procedure _ _ _ _ _ _ _ _

Procedure mandatory? _
(Y, N)

*Default user menu _ _ _ _ _ _

Menu mandatory? _
(Y, N)

*Default library _ _ _ _ _ _ _ _

Beginning help menu _ _ _ _ _ _ _ _
(MAIN)

*Comment _

_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

*Badge number
(00000000-99999999) _ _ _ _ _ _ _ _

M = Master security officer
S = Security officer
O = System console operator
C = Subconsole operator
D = Display station operator

S9446016-3

User Identification Form

Customer Name _____
Customer Number _____

Name _____

Position _____

Responsibilities _____

_____

Optional=*

User ID _ _ _ _ _ _ _ _

Password _ _ _ _

Security classification? _
(M, S, O, C, D)

Service aid authority? _
(Y, N)

*Default sign-on procedure _ _ _ _ _ _ _ _

Procedure mandatory? _
(Y, N)

*Default user menu _ _ _ _ _ _

Menu mandatory? _
(Y, N)

*Default library _ _ _ _ _ _ _ _

Beginning help menu _ _ _ _ _ _ _ _
(MAIN)

*Comment _

_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

*Badge number _ _ _ _ _ _ _ _
(00000000-99999999)

M = Master security officer
S = Security officer
O = System console operator
C = Subconsole operator
D = Display station operator

S9446016-3

P

Resource Security Form

Customer Name ____________
Customer Number ____________

File ____________ Library ____________ Resource Group ____________

Application ____

Purpose ____

____

Optional = *

Resource name _ _ _ _ _ _ _ _

*Special resource type __
(A,G,S)

Default access __
(O, C, U, R, E, N)

*Parent resource name _ _ _ _ _ _ _ _

Is the parent resource a group resource record?__
(Y,N)

Log successful accesses? __
(Y,N)

A = The file is an alternative index.
G = The files and libraries are secured as a group.
S = The library is #LIBRARY.

O = Owner
C = Change
U = Update
R = Read
E = Run
N = No access

User ID	Access allowed (O,C,U,R,E,N)	User ID	Access allowed (O,C,U,R,E,N)
_ _ _ _ _ _ _ _	__	_ _ _ _ _ _ _ _	__
_ _ _ _ _ _ _ _	__	_ _ _ _ _ _ _ _	__
_ _ _ _ _ _ _ _	__	_ _ _ _ _ _ _ _	__
_ _ _ _ _ _ _ _	__	_ _ _ _ _ _ _ _	__
_ _ _ _ _ _ _ _	__	_ _ _ _ _ _ _ _	__
_ _ _ _ _ _ _ _	__	_ _ _ _ _ _ _ _	__
_ _ _ _ _ _ _ _	__	_ _ _ _ _ _ _ _	__
_ _ _ _ _ _ _ _	__	_ _ _ _ _ _ _ _	__

S9446017-2

P Resource Security Form (reverse side)

Customer Name ____________
Customer Number ____________

Resource name ____________
File ____________ Library ____________
Application ____________
Purpose ____________

Resource name ____________
File ____________ Library ____________
Application ____________
Purpose ____________

Resource name ____________
File ____________ Library ____________
Application ____________
Purpose ____________

Resource name ____________
File ____________ Library ____________
Application ____________
Purpose ____________

Resource name ____________
File ____________ Library ____________
Application ____________
Purpose ____________

Resource name ____________
File ____________ Library ____________
Application ____________
Purpose ____________

Resource name ____________
File ____________ Library ____________
Application ____________
Purpose ____________

Resource name ____________
File ____________ Library ____________
Application ____________
Purpose ____________

Resource name ____________
File ____________ Library ____________
Application ____________
Purpose ____________

Resource name ____________
File ____________ Library ____________
Application ____________
Purpose ____________

S9446029-0

P **Resource Security Form**

Customer Name ____________
Customer Number ____________

File ________ Library ________ Resource Group ________

Application ____

Purpose ____

____

Optional = *

Resource name _ _ _ _ _ _ _ _

*Special resource type __

(A,G,S)

Default access __

(O, C, U, R, E, N)

*Parent resource name _ _ _ _ _ _ _ _

Is the parent resource a group resource record?__

(Y,N)

Log successful accesses? __

(Y,N)

A = The file is an alternative index.
G = The files and libraries are secured as a group.
S = The library is #LIBRARY.

O = Owner
C = Change
U = Update
R = Read
E = Run
N = No access

User ID	Access allowed (O,C,U,R,E,N)	User ID	Access allowed (O,C,U,R,E,N)
_ _ _ _ _ _ _ _	__	_ _ _ _ _ _ _ _	__
_ _ _ _ _ _ _ _	__	_ _ _ _ _ _ _ _	__
_ _ _ _ _ _ _ _	__	_ _ _ _ _ _ _ _	__
_ _ _ _ _ _ _ _	__	_ _ _ _ _ _ _ _	__
_ _ _ _ _ _ _ _	__	_ _ _ _ _ _ _ _	__
_ _ _ _ _ _ _ _	__	_ _ _ _ _ _ _ _	__
_ _ _ _ _ _ _ _	__	_ _ _ _ _ _ _ _	__
_ _ _ _ _ _ _ _	__	_ _ _ _ _ _ _ _	__

S9446017-2

P

Resource Security Form (reverse side)

Customer Name ____________
Customer Number ____________

Resource name ____________
File ____________ Library ____________
Application ____________
Purpose ____________
____

Resource name ____________
File ____________ Library ____________
Application ____________
Purpose ____________
____

Resource name ____________
File ____________ Library ____________
Application ____________
Purpose ____________
____

Resource name ____________
File ____________ Library ____________
Application ____________
Purpose ____________
____

Resource name ____________
File ____________ Library ____________
Application ____________
Purpose ____________
____

Resource name ____________
File ____________ Library ____________
Application ____________
Purpose ____________
____

Resource name ____________
File ____________ Library ____________
Application ____________
Purpose ____________
____

Resource name ____________
File ____________ Library ____________
Application ____________
Purpose ____________
____

Resource name ____________
File ____________ Library ____________
Application ____________
Purpose ____________
____

Resource name ____________
File ____________ Library ____________
Application ____________
Purpose ____________
____

S9446029-0

S **Location Identification Form**

Name of Local System ______________

Local Location Name ______________

Customer Name ______________

Customer Number ______________

Name of remote system ______________
Remote location name ______________
Location password _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
Require user passwords to start procedure? (Y,N) ___
Comment ______________

Name of remote system ______________
Remote location name ______________
Location password _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
Require user passwords to start procedure? (Y,N) ___
Comment ______________

Name of remote system ______________
Remote location name ______________
Location password _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
Require user passwords to start procedure? (Y,N) ___
Comment ______________

Name of remote system ______________
Remote location name ______________
Location password _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
Require user passwords to start procedure? (Y,N) ___
Comment ______________

Name of remote system ______________
Remote location name ______________
Location password _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
Require user passwords to start procedure? (Y,N) ___
Comment ______________

Name of remote system ______________
Remote location name ______________
Location password _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
Require user passwords to start procedure? (Y,N) ___
Comment ______________

Name of remote system ______________
Remote location name ______________
Location password _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
Require user passwords to start procedure? (Y,N) ___
Comment ______________

Name of remote system ______________
Remote location name ______________
Location password _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
Require user passwords to start procedure? (Y,N) ___
Comment ______________

Name of remote system ______________
Remote location name ______________
Location password _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
Require user passwords to start procedure? (Y,N) ___
Comment ______________

Name of remote system ______________
Remote location name ______________
Location password _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
Require user passwords to start procedure? (Y,N) ___
Comment ______________

S9446028-2

S Location Identification Form

Name of Local System ____________	**Customer Name** ____________
Local Location Name ____________	**Customer Number** ____________

Name of remote system ____________ Remote location name ____________ Location password _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ Require user passwords to start procedure? (Y,N) ___ Comment ____________	Name of remote system ____________ Remote location name ____________ Location password _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ Require user passwords to start procedure? (Y,N) ___ Comment ____________
Name of remote system ____________ Remote location name ____________ Location password _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ Require user passwords to start procedure? (Y,N) ___ Comment ____________	Name of remote system ____________ Remote location name ____________ Location password _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ Require user passwords to start procedure? (Y,N) ___ Comment ____________
Name of remote system ____________ Remote location name ____________ Location password _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ Require user passwords to start procedure? (Y,N) ___ Comment ____________	Name of remote system ____________ Remote location name ____________ Location password _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ Require user passwords to start procedure? (Y,N) ___ Comment ____________
Name of remote system ____________ Remote location name ____________ Location password _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ Require user passwords to start procedure? (Y,N) ___ Comment ____________	Name of remote system ____________ Remote location name ____________ Location password _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ Require user passwords to start procedure? (Y,N) ___ Comment ____________
Name of remote system ____________ Remote location name ____________ Location password _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ Require user passwords to start procedure? (Y,N) ___ Comment ____________	Name of remote system ____________ Remote location name ____________ Location password _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ Require user passwords to start procedure? (Y,N) ___ Comment ____________

S9446028-2

T Security For Folders

Customer Name ____________

Customer Number ____________

Folder

Folder name ___ ___ ___ ___ ___ ___ ___ ___

Purpose ______________________

Primary authorization list ___ ___ ___ ___ ___ ___ ___ ___

Override authorization list ___ ___ ___ ___ ___ ___ ___ ___

Default access level
(O, C, U, R, N) ___

Log successful accesses
Yes (1) or No (2) ___

Members Within Folder

Subdirectory ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Folder member name ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Default access level ___

Primary authorization list ___ ___ ___ ___ ___ ___ ___ ___

Override authorization list ___ ___ ___ ___ ___ ___ ___ ___

Members Within Folder

Subdirectory ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Folder member name ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Default access level ___

Primary authorization list ___ ___ ___ ___ ___ ___ ___ ___

Override authorization list ___ ___ ___ ___ ___ ___ ___ ___

Members Within Folder

Subdirectory ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Folder member name ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Default access level ___

Primary authorization list ___ ___ ___ ___ ___ ___ ___ ___

Override authorization list ___ ___ ___ ___ ___ ___ ___ ___

Folder

Folder name ___ ___ ___ ___ ___ ___ ___ ___

Purpose ______________________

Primary authorization list ___ ___ ___ ___ ___ ___ ___ ___

Override authorization list ___ ___ ___ ___ ___ ___ ___ ___

Default access level
(O, C, U, R, N) ___

Log successful accesses
Yes (1) or No (2) ___

Members Within Folder

Subdirectory ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Folder member name ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Default access level ___

Primary authorization list ___ ___ ___ ___ ___ ___ ___ ___

Override authorization list ___ ___ ___ ___ ___ ___ ___ ___

Members Within Folder

Subdirectory ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Folder member name ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Default access level ___

Primary authorization list ___ ___ ___ ___ ___ ___ ___ ___

Override authorization list ___ ___ ___ ___ ___ ___ ___ ___

Members Within Folder

Subdirectory ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Folder member name ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Default access level ___

Primary authorization list ___ ___ ___ ___ ___ ___ ___ ___

Override authorization list ___ ___ ___ ___ ___ ___ ___ ___

R9480029-7

Security For Folders (reverse side)

Customer Name _____
Customer Number _____

Authorization List

Authorization list name _ _ _ _ _ _ _ _ _ _

Purpose _____

User ID	Access Allowed (O, C, U, R, N)
_ _ _ _ _ _ _ _ _ _	_
_ _ _ _ _ _ _ _ _ _	_
_ _ _ _ _ _ _ _ _ _	_
_ _ _ _ _ _ _ _ _ _	_
_ _ _ _ _ _ _ _ _ _	_
_ _ _ _ _ _ _ _ _ _	_
_ _ _ _ _ _ _ _ _ _	_
_ _ _ _ _ _ _ _ _ _	_
_ _ _ _ _ _ _ _ _ _	_
_ _ _ _ _ _ _ _ _ _	_
_ _ _ _ _ _ _ _ _ _	_
_ _ _ _ _ _ _ _ _ _	_
_ _ _ _ _ _ _ _ _ _	_
_ _ _ _ _ _ _ _ _ _	_
_ _ _ _ _ _ _ _ _ _	_
_ _ _ _ _ _ _ _ _ _	_
_ _ _ _ _ _ _ _ _ _	_
_ _ _ _ _ _ _ _ _ _	_

S9446040-0

T Security For Folders

Customer Name ____________
Customer Number ____________

Folder	Folder
Folder name ________ Purpose ________ Primary authorization list ________ Override authorization list ________ Default access level (O, C, U, R, N) __ Log successful accesses Yes (1) or No (2) __	Folder name ________ Purpose ________ Primary authorization list ________ Override authorization list ________ Default access level (O, C, U, R, N) __ Log successful accesses Yes (1) or No (2) __
Members Within Folder	**Members Within Folder**
Subdirectory ________ ________ Folder member name ________ Default access level __ Primary authorization list ________ Override authorization list ________	Subdirectory ________ ________ Folder member name ________ Default access level __ Primary authorization list ________ Override authorization list ________
Members Within Folder	**Members Within Folder**
Subdirectory ________ ________ Folder member name ________ Default access level __ Primary authorization list ________ Override authorization list ________	Subdirectory ________ ________ Folder member name ________ Default access level __ Primary authorization list ________ Override authorization list ________
Members Within Folder	**Members Within Folder**
Subdirectory ________ ________ Folder member name ________ Default access level __ Primary authorization list ________ Override authorization list ________	Subdirectory ________ ________ Folder member name ________ Default access level __ Primary authorization list ________ Override authorization list ________

R9480029-7

Security For Folders (reverse side)

Customer Name _____
Customer Number _____

Authorization List

Authorization list name _ _ _ _ _ _ _ _ _ _

Purpose _____

User ID	Access Allowed (O, C, U, R, N)
_ _ _ _ _ _ _ _ _ _	_
_ _ _ _ _ _ _ _ _ _	_
_ _ _ _ _ _ _ _ _ _	_
_ _ _ _ _ _ _ _ _ _	_
_ _ _ _ _ _ _ _ _ _	_
_ _ _ _ _ _ _ _ _ _	_
_ _ _ _ _ _ _ _ _ _	_
_ _ _ _ _ _ _ _ _ _	_
_ _ _ _ _ _ _ _ _ _	_
_ _ _ _ _ _ _ _ _ _	_
_ _ _ _ _ _ _ _ _ _	_
_ _ _ _ _ _ _ _ _ _	_
_ _ _ _ _ _ _ _ _ _	_
_ _ _ _ _ _ _ _ _ _	_
_ _ _ _ _ _ _ _ _ _	_
_ _ _ _ _ _ _ _ _ _	_
_ _ _ _ _ _ _ _ _ _	_
_ _ _ _ _ _ _ _ _ _	_

S9446040-0

Appendix C. Converting System/34 Security Files to System/36 Security Files

This appendix explains how to convert your IBM System/34 security files (either the password security file, the resource security file, or both) to the System/36 user identification file and resource security file.

Do the following to convert your System/34 security files to System/36 security files:

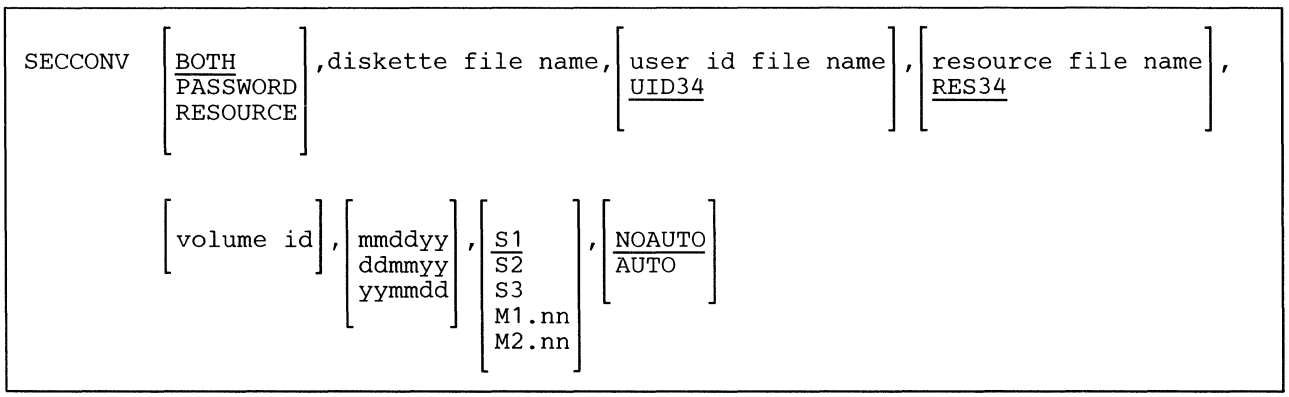
1. On the System/34, run the PRSAVE procedure to copy the security files onto a diskette. See the *IBM System/34 System Support Reference Manual*, SC21-5155, for information about running the PRSAVE procedure.

2. On the System/36, run the SECCONV procedure to copy the System/34 diskette file and convert it to the System/36 security files on disk. See "Using the SECCONV Procedure," later in this appendix for information on running the procedure.

3. On the System/36, run the SECREST procedure to restore the converted security files into the user ID file and resource security file. See "Restoring the User ID File" in Chapter 2 for information about restoring the user ID file to disk. See "Restoring the Resource Security File" in Chapter 3 for information about restoring the resource security file to disk. You may have to run the SECREST procedure twice, once for the user ID file and again for the resource security file.

Using the SECCONV Procedure

The SECCONV procedure is a System/36 procedure that copies a diskette file (containing IBM System/34 security files), converts the file into System/36 security files, and places these files on disk. The SECCONV procedure allows you to convert just the password security file, just the resource security file, or both security files with one running of the procedure. The disk files created by the SECCONV procedure can then be copied into the user ID and resource security files with the SECREST procedure.



S9042014-0

BOTH, PASSWORD, and **RESOURCE** specify the type of file to be converted.

BOTH specifies that both the System/34 password file and the System/34 resource file are to be converted and placed in disk files. If no parameter is specified, BOTH is assumed.

PASSWORD specifies that only the System/34 password file is to be converted to a System/36 user ID file and placed in a disk file.

RESOURCE specifies that only the System/34 resource file is to be converted to a System/36 resource security file and placed in a disk file.

diskette file name specifies the name of the diskette file that contains the System/34 security files.

user ID file name specifies the name to assign the converted password file. You use this name in the SECREST procedure to restore the user ID file. If no user ID file name is specified, and the System/34 password file is to be converted, the name UID34 is assumed.

resource file name specifies the name to assign the converted resource file. You use this name in the SECREST procedure to restore the resource security file. If no resource file name is specified, and the System/34 resource file is to be converted, the name RES34 is assumed.

volume id specifies the volume ID of the diskette that contains the System/34 security files.

mmddyy, ddmmyy, and **yymmdd** specify the date the diskette file was created. The date must be specified in the current session date format. You can use the STATUS SESSION command to display the date format (see the manual *System Reference* for more information about the STATUS command). If no date is specified, and more than one file exists on the diskette with the same name, the first (oldest) file on the diskette is used.

S1, S2, or **S3** specifies the diskette slot containing the first diskette from which members are to be processed. If no parameter is specified, S1 is assumed.

M1.nn or **M2.nn** specifies the magazine location containing the first diskette from which members are to be processed. M1 indicates the first magazine location, and M2 indicates the second magazine location. **nn** is a decimal number from 01 through 10 that identifies the location of the diskette in the magazine. (Specifying M1 is the same as specifying M1.01; specifying M2 is the same as specifying M2.01.)

NOAUTO specifies the following:

- If S1, S2, or S3 is specified, only the specified slot (S1, S2, or S3) is used. If more diskettes need to be processed, a message is displayed and you must insert the next diskette into the slot being used.

- If M1.nn or M2.nn is specified, only the specified magazine location (M1 or M2) is used. Processing begins with the diskette at the specified location within the magazine and continues through the last diskette in the magazine. If more diskettes need to be processed, a message is displayed and you must insert the next magazine in the magazine location being used. Processing resumes at the first location in that magazine.

If no parameter is specified, NOAUTO is assumed.

AUTO specifies the following:

- If S1, S2, or S3 is specified, all three slots (S1, S2, and S3) are used. Processing begins with the diskette in the specified slot and continues through the diskette in slot S3. If more diskettes need to be processed, a message is displayed and you must then insert the next diskettes. Processing resumes with the diskette in slot S1.

- If M1.nn or M2.nn is specified, both magazine locations (M1 and M2) are used. Processing begins with the diskette at the specified location and continues through the diskette in location M2.10. If more diskettes need to be processed, a message is displayed and you must then insert the next magazines. Processing resumes at location M1.01 and continues through M2.10.

This example shows how to convert System/34 security files to System/36 security files.

1. Use the PRSAVE procedure to copy both the System/34 password security file and the System/34 resource security file onto diskette. These files are saved in a diskette file named S34SECUR; the diskette's volume ID is 999999.

   ```
   PRSAVE 999999,S34SECUR
   ```

2. Use the SECCONV procedure to copy the System/34 diskette file onto disk and convert the file to the System/36 security files. The System/36 user identification file is named USERCONV and the System/36 resource security file is named RESCONV.

   ```
   SECCONV BOTH,S34SECUR,USERCONV,RESCONV
   ```

3. Use the SECREST procedure to copy the converted security files into the actual System/36 user ID and resource security files. The user ID file is to contain 100 records; the resource security file is to contain 300 records.

```
SECREST USERID,USERCONV,100,,F1
SECREST RESOURCE,RESCONV,300,,F1
```

4. Use the SECDEF procedure to activate password security and resource security.

```
SECDEF USERID,ACTPW
SECDEF RESOURCE,ACTRES
```

5. Use the DELETE procedure to remove the converted System/34 security files from the System/36 disk after the conversion is tested.

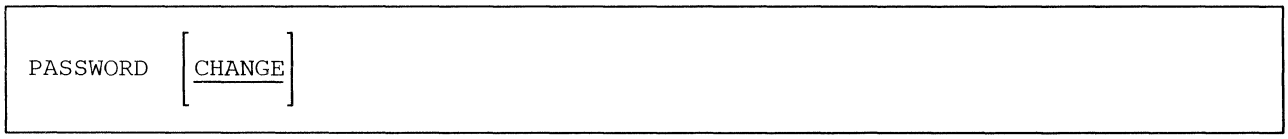
```
DELETE USERCONV,F1
DELETE RESCONV,F1
```

Appendix D. Security Procedures

This appendix contains the system security procedures. You can use these procedures in place of the system help menus if you prefer.

PASSWORD Procedure

The PASSWORD procedure can be used by any user to change his or her password.

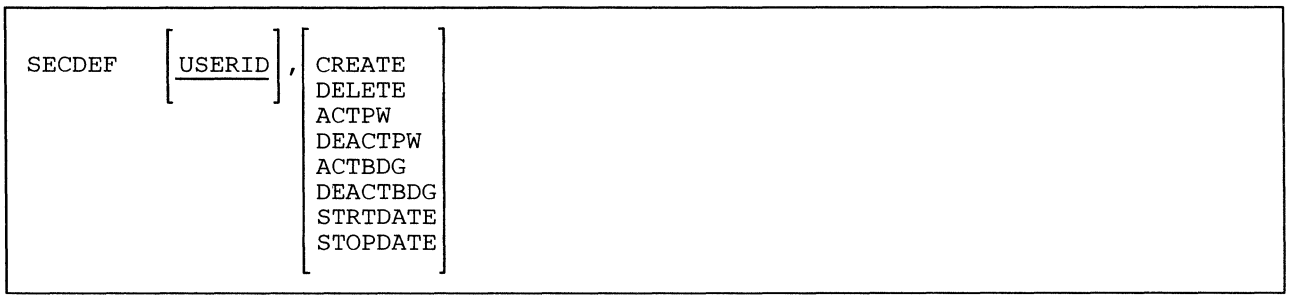


S9020511-1

SECDEF Procedure (User Identification File)

The SECDEF procedure can be used to:

- Create the user identification file on disk
- Remove the user identification file from disk
- Activate password security
- Deactivate password security
- Activate badge security
- Deactivate badge security
- Start the date checking function
- Stop the date checking function

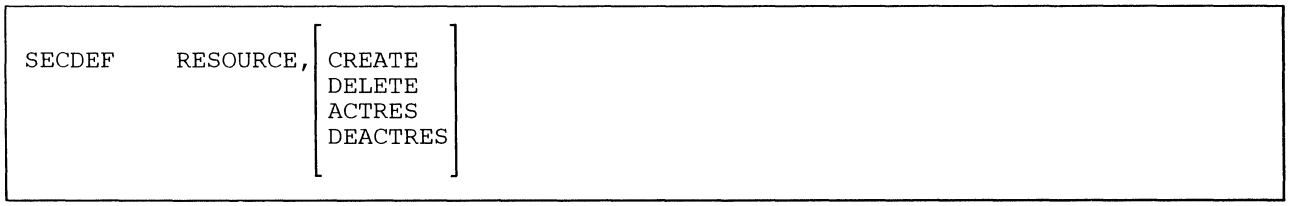


S9020232-1

SECDEF Procedure (Resource Security File)

The SECDEF procedure can be used to:

- Create the resource security file on disk
- Remove the resource security file from disk
- Activate resource security
- Deactivate resource security

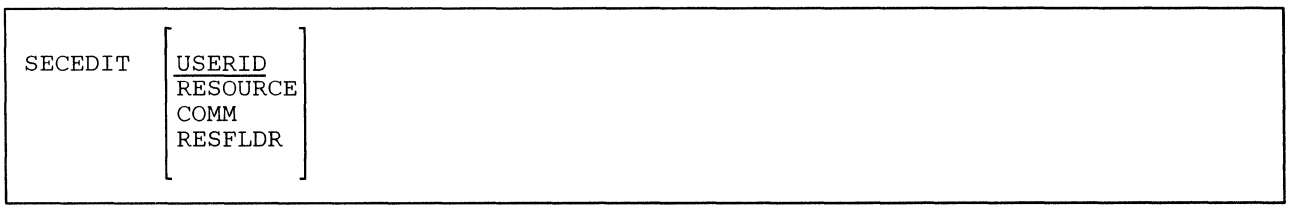


S9020233-0

SECEDIT Procedure

The SECEDIT procedure can be used to:

- Add, change, or remove user profiles in the user identification file
- Add, change, or remove location profiles in the user identification file
- Add, change, or remove file, library, and group resource records and user records in the resource security file
- Add, change, or remove authorization lists and security information for folders, subdirectories, and folder members



S9020234-1

SECLIST Procedure (User Identification File)

The SECLIST procedure can be used to:

- Print or display user profile information in the user identification file

```
SECLIST  USERID,[PRINTER/CRT],[NOPW/PW]
```

S9020235-0

- Print or display location profile information in the user identification file

```
SECLIST  COMM,[PRINTER/CRT]
```

S9020237-0

SECLIST Procedure (Resource Security File)

The SECLIST procedure can be used to:

- Print or display file, library, and group resource records and user records in the resource security file

```
SECLIST  RESOURCE,[PRINTER/CRT],[OWNERID/RNAME/USERID],[USER/ALL]
```

S9020236-0

- Print or display folder security or subdirectory secure information and authorization lists in the resource security file

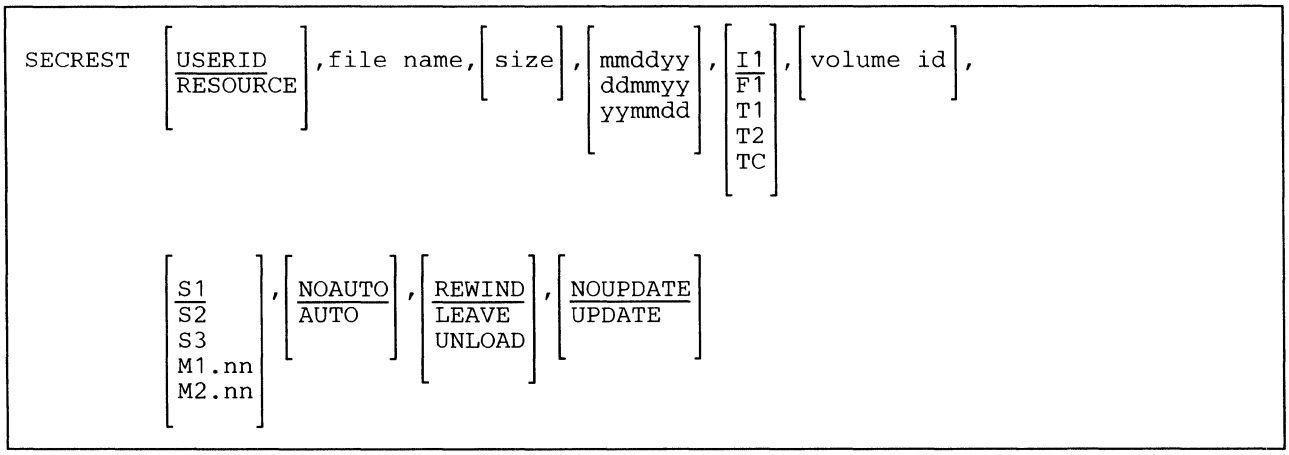
```
SECLIST  RESFLDR,[PRINTER/CRT],[OWNERID/RNAME/USERID],[USER/ALL]
```

S9020238-1

SECREST Procedure

The SECREST procedure can be used to:

- Restore a copy of the user identification file or the resource security file from diskette, tape, or tape cartridge to the original on disk
- Restore a copy of the user identification file or the resource security file from disk to the original on disk

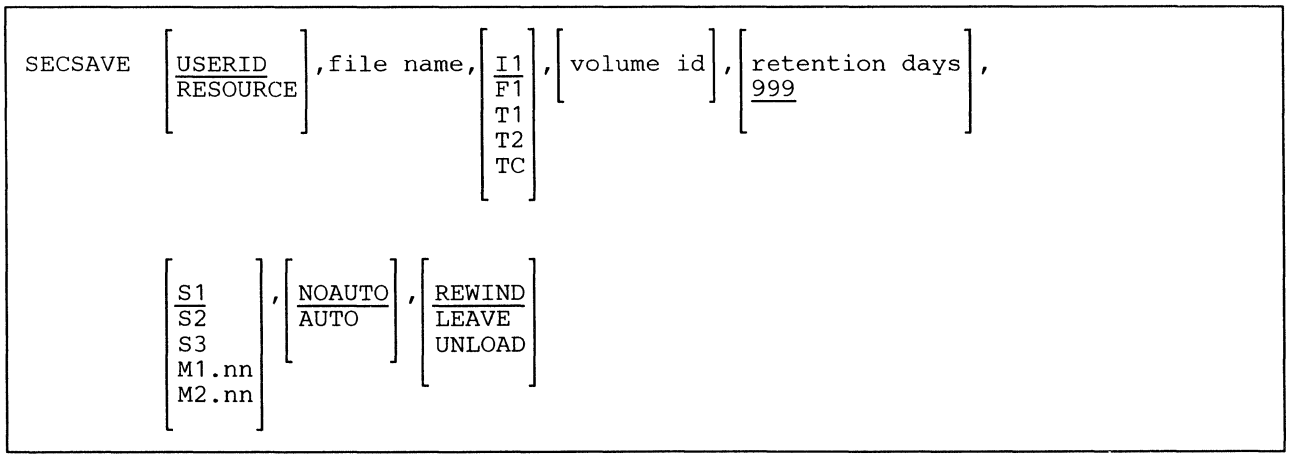


S9020239-1

SECSAVE Procedure

The SECSAVE procedure can be used to:

- Save a copy of the user identification file or the resource security file on diskette, tape, or tape cartridge
- Save a copy of the user identification file or the resource security file on another area on disk



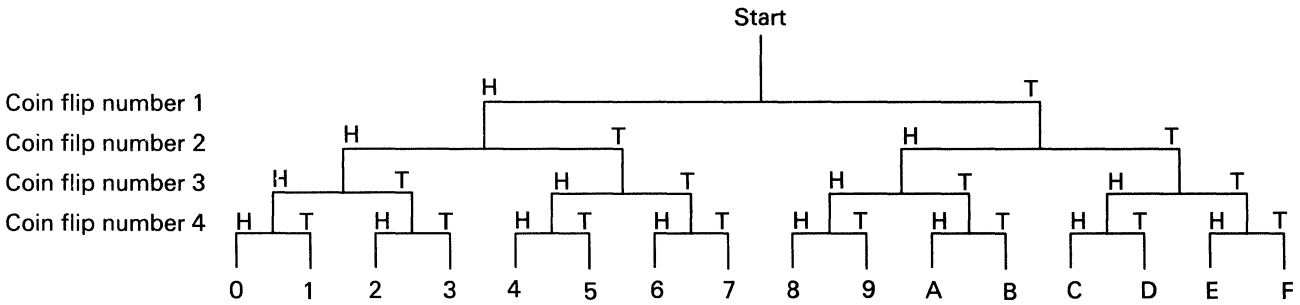
S9020240-1

Appendix E. Generating Random Hexadecimal Location Passwords

This appendix describes one way to manually create a random hexadecimal location password. The method described in this appendix uses a coin.

Note: It is important to use this or a similar method to avoid using a trivial password.

The following illustration shows how one random hexadecimal character is derived from four flips of a coin.



Legend:

H = Heads

T = Tails

S9042008-0

An example of how this works follows:

1. On the first flip of the coin, the coin comes up heads.
2. On the second flip of the coin, the coin comes up heads.
3. On the third flip of the coin, the coin comes up tails.
4. On the fourth flip of the coin, the coin comes up heads.
5. The resulting hexadecimal character is a 2.

For a 16-character hexadecimal location password, you need to flip a coin 64 times.

If you want the system to generate a random hexadecimal location password for you, use command key 6 while running the SECEDIT COMM procedure. Command key 6 is described under "Changing Location Profiles" in Chapter 2.

Glossary

#LIBRARY. The library, provided with the system, that contains the System Support Program Product. See *system library.*

access. To get at or obtain; to go to or reach.

access level. The level of authority an operator has in order to use a secured file, library, folder, or folder member.

Advanced Peer-to-Peer Networking (APPN). A communications feature that routes data in a network between two or more APPC systems that are not directly attached. See also *node* and *network node.*

advanced program-to-program communications (APPC). Communications support that allows System/36 to communicate with other systems having the same support. APPC is the way that System/36 puts the IBM SNA LU-6.2 protocol into effect.

allocate. To assign a resource, such as a disk file or a diskette file, to perform a specific task.

alphabetic character. Any one of the letters A through Z (uppercase and lowercase). Some program products extend the alphabet to include the special characters #, $, and @. (COBOL) A character that is one of the 26 uppercase characters of the alphabet, or a space. (FORTRAN) Any one of the uppercase letters A through Z, or the special character $.

alphameric. Consisting of letters, numbers, and other symbols, such as punctuation marks and mathematical symbols.

alphanumeric. See *alphameric.*

alternative index. An index that is built after a physical file is created and that provides a different order for reading or writing records in the file. Contrast with *primary index.*

alternative system console. A command display station that can be designated as the system console.

American National Standard Code for Information Interchange (ASCII). The code developed by ANSI for information interchange among data processing systems, data communications systems, and associated equipment. The ASCII character set consists of 7-bit control characters and symbolic characters.

American National Standards Institute (ANSI). An organization sponsored by the Computer and Business Equipment Manufacturers Association for establishing voluntary industry standards.

ANSI. See *American National Standards Institute (ANSI).*

APPC. See *advanced program-to-program communications (APPC).*

application. (1) A particular business task, such as inventory control or accounts receivable. (2) A group of related programs that apply to a particular business area, such as the Inventory Control or the Accounts Receivable application.

application program. A program used to perform an application or part of an application.

APPN. See *Advanced Peer-to-Peer Networking (APPN).*

archive. To copy a folder member onto tape, diskette, or disk file.

archived member. A folder member that has been saved on a disk, diskette or tape file. can be an identifier for a numeric elementary item, a numeric literal, such identifiers and literals separated by an arithmetic operator, or an arithmetic expression enclosed in parentheses.

ASCII. See *American National Standard Code for Information Interchange (ASCII).*

authority. The right to communicate with or use a resource.

authorization list. A list of user identifications and access levels for secured folders and folder members.

authorize. To give a user the right to use a resource.

back up. To copy information, usually onto diskette or tape, for safekeeping.

backup copy. A copy, usually of a file, library member, or folder, that is kept in case the original is unintentionally changed or destroyed.

badge security. A System Support Program Product option that helps prevent the unauthorized use of a display station by checking the data from a magnetic stripe on a badge before allowing an operator to sign on.

beginning of tape. A reflective marking near the beginning of a tape reel that indicates where the system can begin recording data.

block. (1) A group of records that is recorded or processed as a unit. Same as *physical record.* (2) Ten sectors (2560 bytes) of disk storage. (3) In data communications, a group of records that is recorded, processed, or sent as a unit. (DSU) A sequential group of statements (defined using line commands) that is treated as a unit. (DW/36) A sequential string of text (defined using cursor movement keys or line commands) that is treated as a unit.

call. (1) To activate a program or procedure at its entry point. Compare with *load.* (2) In data communications, the action necessary in making a connection between two stations on a switched line.

cancel. To end a task before it is completed.

change authority. The right to create, add, change, and remove files, libraries, and folders. (PerSrv36) See *update authority.*

character. A letter, digit, or other symbol. (COBOL) One of a set of indivisible symbols that can be arranged in sequence to express information.

character key. A keyboard key that allows the user to enter the character shown on the key. Compare with *command key* and *function key.*

child. Pertaining to a secured resource, either a file or library, that uses the user list of a parent resource. A child resource can have only one parent resource. Contrast with *parent.*

code. (1) Instructions for the computer. (2) To write instructions for the computer. Same as *program.* (3) A representation of a condition, such as an error code.

column. (1) A character position within a print line or on a display. The positions are numbered from 1, by 1, starting at the leftmost character position and extending to the rightmost position. (2) A group of data that is aligned vertically (usually with tabs) within a list or table. See *position.* (Query/36) A list of values in a report. Each field in the report is a single column.

command. A request to the system to perform an operation or a procedure.

command display. A display that allows an operator to display and send messages, and use control commands and procedure commands to start and control jobs. Contrast with *standby display.* See also *console display* and *subconsole display.*

command display station. A display station from which an operator can start and control jobs. A command display station can become an alternative system console, can be designated as a subconsole, and can also be used as a data display station. See also *alternative system console, data display station,* and *subconsole.*

command key. A keyboard key that is used to request specific programmed actions. Compare with *character key* and *function key.*

command line. The blank line on a display where commands or option numbers can be entered.

comment. Words or statements in a program or on a display that serve as documentation rather than as instructions, choices, or prompts. (COBOL) A note in the Identification Division or Procedure Division of a COBOL source program. A comment is ignored by the compiler. As an IBM extension, comments may be included at any point in a COBOL source program.

communications security. A System Support Program Product option that allows the identity of a remote location to be verified before that location can run programs on your system.

communications subsystem. See *subsystem.*

compile. To translate a program written in a high-level programming language into a machine language program.

concept. An idea generalized from particular instances.

configure. (1) To describe (to the system) the devices, optional features, and program products installed on a system. (2) To describe to SSP-ICF both the communications facilities connected to System/36 and the attributes of the subsystem and remote system.

console. A device used for communication between an operator and the system.

console display. A display that can be requested only at the system console. From a console display an operator can display, send, and reply to messages and use all control commands.

control station. The primary or controlling computer on a multipoint line. The control station controls the sending and receiving of data.

creation date. The program date at the time a file is created. See also *program date*, *session date*, and *system date*.

cursor. A movable symbol on a display, used to indicate to the operator where to type the next character.

data display station. A display station from which an operator can only enter data. A data display station is acquired and controlled by a program. Contrast with *command display station*.

deactivate. To make ineffective. For example, to deactivate security.

default. See *default value*.

default value. A value stored in the system that is used when no other value is specified.

direct file. A disk file in which records are referenced by the relative record number. Contrast with *indexed file* and *sequential file*.

directory. See *network resource directory (NRD)*. (PerSrv36) A file containing such information as a name, address, and telephone number for each user of Personal Services/36. Indirect users and individuals or organizations that do not use Personal Services/36 may also be listed in the directory.

disk. A storage device made of one or more flat, circular plates with magnetic surfaces on which information can be stored.

disk drive. The mechanism used to read and write information on disk.

disk file. A set of related records on disk that is treated as a unit. See also *record file* and *stream file*.

diskette. A thin, flexible magnetic plate that is permanently sealed in a protective cover. It can be used to store information copied from the disk or to exchange information with other computers.

diskette drive. The mechanism used to read and write information on diskettes.

diskette magazine drive. A diskette drive that holds up to two magazines plus three individual diskettes.

display. (1) A visual presentation of information on a display screen. (2) To show information on the display screen.

display station. A device that includes a keyboard from which an operator can send information to the system and a display screen on which an operator can see the information sent to or the information received from the system.

document. One or more lines of text that can be named and stored as a member in a folder.

document folder. (DW/36) A folder that is used to store documents. Contrast with *mail folder*.

edit. (1) To modify the form or format of data; for example, to insert or remove characters for dates or decimal points. (2) To check the accuracy of information that has been entered, and to indicate if an error is found. (3) To make changes to a document by adding, changing, or removing text.

end of tape. A reflective marking near the end of a tape reel that indicates where the system must stop recording data.

enter. To type in information from a keyboard and press the Enter key to send the information to the computer.

enter/update mode. (SEU) The mode that is used to enter new statements into a source or procedure member, or to change statements that already exist in a source or procedure member.

field. One or more characters of related information (such as a name or an amount). Records are comprised of fields.

file name. The name used by a program to identify a file. See also *label*.

folder. A named area on disk that contains documents, profiles, mail, or data definitions used by office products. Compare with *library*.

folder directory. An area, in a folder, that contains information about each member in the folder; for example, the member name and the location.

folder member. A named collection of records or statements in a folder. A document is an example of a folder member.

format. (1) A defined arrangement of such things as characters, fields, and lines, usually used for displays, printouts, files, or documents. (2) To arrange such things as characters, fields, and lines. (3) In BASIC, a representation of the correct form of a command or statement. (4) In IDDU, a group of related fields, such as a record, in a file.

function key. A keyboard key that requests an action but does not display or print a character. The cursor movement and Help keys are examples of function keys. Compare with *command key* and *character key.*

group. A list of names that are known together by a single name.

group resource record. A record in the resource security file that secures a group of files and/or libraries.

Help key. A function key that, when pressed, displays online information or some part of the system help support.

help support. See *system help support.*

help text. The part of the system help support that supplies information about menus, prompts, and messages.

hex. See *hexadecimal.*

hexadecimal. Pertaining to a system of numbers to the base sixteen; hexadecimal digits range from 0 (zero) through 9 (nine) and A (ten) through F (fifteen).

history file. A file that contains a log of system actions and operator responses.

ID. Identification.

identifier. (1) A sequence of bits or characters that identifies a program, device, or system to another program, device, or system. (2) In COBOL, a data name that is unique or is made unique by the correct combination of qualifiers, subscripts, or indexes. (3) In Personal Services/36, a name that identifies the type of member in a group. The identifier can be a calendar, a user ID, or another group.

ideographic. Pertaining to 2-byte characters consisting of pictograms, symbolic characters, and other types of symbols.

IGC. See *ideographic.*

index. (1) A table containing the key value and location of each record in an indexed file. (2) A computer storage position or register, the contents of which identify a particular element in a set of elements.

indexed file. A file in which the key and the position of each record are recorded in a separate portion of the file called the index. Contrast with *direct file* and *sequential file.*

initial program load (IPL). The process of loading the system programs and preparing the system to run jobs.

interactive communications feature (SSP-ICF). A group of communications features of the System Support Program Product that allows a program to interactively communicate with another program or system.

IPL. See *initial program load (IPL).*

job. (1) A unit of work to be done by a system. (2) One or more related procedures or programs grouped into a procedure.

job queue. A list of jobs waiting to be processed by the system.

Keylock feature. A security feature in which a lock and key can be used to restrict the use of the display station.

label. (1) The name in the disk or diskette volume table of contents or on a tape that identifies a file. See also *file name.* (2) The name that identifies a statement. (BASIC) The name that identifies a BASIC program line.

library. (1) A named area on disk that can contain programs and related information (not files). A library consists of different sections, called library members. Compare with *folder.* (2) The set of publications for a system.

library control sector. In a library directory, the first sector, which contains a record of the used and available space in the library.

library member. A named collection of records or statements in a library. The types of library members are *load member, procedure member, source member,* and *subroutine member.*

load. (1) To move data or programs into storage. Compare with *call* (2) To place a diskette into a diskette drive or a diskette magazine into a diskette magazine drive. (3) To insert paper into a printer. (4) To mount a tape or insert a tape cartridge into a tape drive.

load member. A library member that contains information in machine language, a form that the system can use directly. Contrast with *source member.*

load module. A program in a form that can be loaded into main storage and run. The load module is the output of the overlay linkage editor.

local. Pertaining to a device, file, or system that is accessed directly from your system, without the use of a communications line. Contrast with *remote.*

location name. In interactive communications, the identifying name associated with a particular system or device.

location password. A string of hexadecimal characters that allows the system to verify the identity of a remote location.

location profile. A profile in the user identification file that contains information about a remote system that is allowed to access resources on your system.

log. (1) To record; for example, to log all messages on the system printer. (2) See *mail log.*

M-byte. See *megabyte.*

magazine. A container that holds up to 10 diskettes.

magnetic stripe reader. A device, attached to a display station, that reads data from a magnetic stripe on a badge before allowing an operator to sign on.

mail. (PerSrv36) Any correspondence (online or hard copy) that is sent between users.

mail folder. (PerSrv36) A folder used to store documents sent and received as mail. Contrast with *document folder.*

mail log. (PerSrv36) A record of all the mail sent or received by the user.

master file. A collection of permanent information, such as a customer address file.

master security officer. A person who is designated to control all of the security tasks that are provided with the System Support Program Product. A master security officer can, for example, deactivate password, badge, or resource security, or add, change, or remove security information about any system operator. Contrast with *security officer.*

megabyte. One million bytes.

member. See *library member.*

memo slip. (PerSrv36) A brief communication

menu. A displayed list of items from which an operator can make a selection.

menu security. A System Support Program Product option that restricts an operator to selecting items from a particular menu.

message. (1) Information sent to one or more users or display stations from a program or another user. A message can be either displayed or printed. (2) An indication of the condition of the system sent by the system. (3) For IMS/IRSS, a unit of data sent over the communications line.

mode. A method of operation. For an example, see *enter/update mode.*

network node. A node which is capable of performing intermediate routing functions, directory services, and route selection services in an APPC network.

network resource directory (NRD). An area on disk that lists the files on remote systems that can be accessed using Distributed Data Management (DDM).

node. (1) An addressable location in a communications network that provides the host processing services. (2) A point where packets are received, stored, and forwarded to another node (DTE) according to a routing method the network has defined.

nondisplay. A field attribute that prevents the displaying of data.

null. See *null character.*

null character. The character hex 00, used to represent the absence of a displayed or printed character.

numeric. Pertaining to any of the digits 0 through 9.

office products. A group of IBM-supplied programs that work together to help an office operate more efficiently. The office products are DisplayWrite/36 (DW/36), Personal Services/36 (Personal Services/36), and Query/36. The interactive data definition utility (IDDU) can be used to define files used by DW/36 and Query/36.

OFFICE/36. The group of office products: DisplayWrite/36 (DW/36), Personal Services/36, and Query/36.

offline. Neither controlled directly by, nor communicating with, the computer, or both. Contrast with *online.*

online. Being controlled directly by, or directly communicating with, the computer, or both. Contrast with *offline.*

online information. Information, read on the display screen, that explains displays, messages, and programs. For some programs, the online information is similar to a printed manual and may contain a table of contents, guide information, help text, a glossary, and an index.

operation control language (OCL). A language used to identify a job and its processing requirements to the System Support Program Product.

operator. (1) A person who operates a device. (2) A symbol that represents an operation to be done.

override. (1) A parameter or value that replaces a previous parameter or value. (2) To replace a parameter or value.

override user ID. A user identification that is used to sign on to the system if the user identification file is destroyed.

owner authority. The right to create, add, change, remove, and rename files, libraries, and folders. (PerSrv36) The right to add, change, read (view), and delete items.

parameter. A value supplied to a procedure or program that either is used as input or controls the actions of the procedure or program. (COBOL) A variable or a literal that is used to pass data values between calling and called programs.

parent. Pertaining to a secured resource, either a file or library, whose user list is shared with one or more other files or libraries. Contrast with *child.*

password. A string of characters that, when entered along with a user ID, allows an operator to sign on to a secured system.

password security. A System Support Program Product option that helps prevent the unauthorized use of system services by checking the password entered by each operator at sign-on.

physical file. A file that contains data records.

physical record. (1) A group of records that is recorded or processed as a unit. Same as *block.* (2) A unit of data that is moved into or out of the computer.

position. The location of a character in a series, as in a record, a displayed message, or a computer printout. See also *column.*

primary index. The index that is built when a file is created. Contrast with *alternative index.*

printout. Information from the computer that is produced by a printer.

procedure. A set of related operation control language statements (and, possibly, utility control statements or procedure control expressions) that cause a specific program or set of programs to be run. (COBOL) One or more successive paragraphs or sections within the Procedure Division, which directs the computer to perform some action or series of actions.

procedure member. A library member that contains the statements (such as operation control language statements) necessary to perform a program or set of programs.

profile. Data that describes the characteristics of a user, program, device, or remote location.

program. (1) A sequence of instructions for a computer. See *source program* and *load module.* (2) To write a sequence of instructions for a computer. Same as *code.*

program date. The date associated with a program (job step). See also *creation date, session date,* and *system date.*

prompt. A displayed request for information or operator action. (PerSrv36) Lines on a display that ask you for information or tell you what action is needed.

record. A collection of fields that is treated as a unit.

record file. (BASIC) A file on disk in which the data is read and written in records. Contrast with *stream file.*

remote. Pertaining to a device, file, or system that is accessed by your system through a communications line. Contrast with *local.*

resource. Any part of the system required by a job or task, including main storage, input and output devices, the processing unit, and files, libraries, and folders.

resource security. A System Support Program Product option that restricts the use of information in files, libraries, folders, and folder members to specified users.

resource security file. A security file that contains information that restricts access to files, libraries, and folders.

restore. Return to an original value or image. For example, to restore a library from diskette.

run. To cause a program, utility, or other machine function to be performed.

security. The protection of data, system operations, and devices from accidental or intentional ruin, damage, or exposure. See also *system security.*

security officer. A person who is designated to control many of the system security tasks that are provided with the System Support Program Product. A security officer can, for example, add, change, or remove security information about system console operators, subconsole operators, and display station operators. A security officer cannot, however, deactivate password, badge, or resource security. Contrast with *master security officer.*

sequential file. A file in which records occur in the order in which they were entered. Contrast with *direct file* and *indexed file.*

session. (1) The logical connection by which a System/36 program or device can communicate with a program or device at a remote location. (2) The length of time that starts when an operator signs on the system and ends when the operator signs off the system.

session date. The date associated with a session. See also *creation date, program date,* and *system date.*

shared folder facility. A function of PC Support/36 that allows multiple System/36 and personal computer users concurrent access to a folder.

sign off. To end a session at a display station.

sign on. (Verb) To enter a user identification to begin a session at a display station.

sign-on. (Noun) The action an operator uses at a display station in order to begin working at the display station.

source. A system, a program within a system, or a device that makes a request to a target. Contrast with *target.*

source member. A library member that contains information in the form in which it was entered, such as RPG specifications. Contrast with *load member.*

source program. A set of instructions that are written in a programming language and that must be translated to machine language before the program can be run.

special character. A character other than an alphabetic or numeric character. For example; *, +, and % are special characters. (COBOL) A character that is neither numeric nor alphabetic. Special characters in COBOL include the space ( ), and the period (.), as well as the following: + - * / = $, ") (; < >.

standby display. A display that allows an operator to enter data only. When a standby display appears, the display station can be acquired by a program. Contrast with *command display.*

stream file. (BASIC) A file on disk in which data is read and written in consecutive fields. Contrast with *record file.*

subconsole. A display station that controls a printer or printers.

subconsole display. A display that can be requested only from a command display that appears on a subconsole. From a subconsole display an operator can display and send messages, and enter all control commands except those that can be entered only at the system console. See also *console display.*

subdirectory. (S/36) A part of a folder that contains the names, descriptions, member types, and security information for other directories (subdirectories) and folder members. Subdirectories are a part of shared folder facility. See also *shared folder facility.* (PC) A succession of directories under the root directory.

subdirectory level. Subdirectories within folders or within other subdirectories in a folder are assigned a level based on the number of subdirectories in the path. If a subdirectory is the first in a folder, it is assigned level 1. If the subdirectory is within another subdirectory, it is assigned level 2, 3, etc. based on how many subdirectories precede it.

subroutine member. A library member that contains information that must be combined with one or more members before being run by the system. (BASIC) A library member that contains a BASIC program in the form in which it appears within the computer.

subsystem. The part of communications that handles the requirements of the remote system, isolating most system-dependent considerations from the application program.

system. The computer and its associated devices and programs.

system administrator. A person that sets up and maintains systems, for example, directories, office authorizations, communications, and so on.

system configuration. A process that specifies the machines, devices, and programs that form a particular data processing system.

system console. A display station from which an operator can keep track of and control system operation.

system date. The date assigned by the system operator during the initial program load procedure. See also *creation date, program date,* and *session date.*

system help support. The part of the System Support Program Product that uses menus, prompts, and descriptive text to aid an operator.

system library. The library, provided with the system, that contains the System Support Program Product and is named #LIBRARY.

system security. A system function that restricts the use of files, libraries, folders, folder members, and display stations to certain users.

system unit. The part of the system that contains the processing unit, the control panel, the disk drive and the disk, and either a diskette drive or a diskette magazine drive.

tape. A thin, flexible magnetic strip on which data can be stored. It can be used to store information copied from the disk.

tape cartridge. A case containing a reel of magnetic tape arranged for insertion into a tape drive.

tape drive. A mechanism used to read and write information on magnetic tapes.

tape reel. A round device on which magnetic tape is wound.

target. A system, a program within a system, or a device that interprets, rejects or satisfies, and replies to requests received from a source. Contrast with *source.* (DSU) A line command that indicates the location for statements to be moved, copied, or included.

unique. The only one.

update authority. The right to add, change, or remove items in a file, library, or folder. (PerSrv36) The right to add, change, delete, or cancel items.

update file. A disk file from which a program reads a record, updates fields in the record, and writes the record back into the location it came from.

user ID. See *user identification (user ID).*

user identification (user ID). A string of characters that identifies a user to the system.

user identification file (user ID file). A file containing information about which operators can use certain system functions, which menu is displayed when an operator signs on to the system, and which library is assigned to an operator when the operator signs on to the system.

user list. A list, containing the user identification and access levels, of all operators who are allowed to use a specified file or library.

user profile. A profile in the user identification file that contains information about someone who is allowed to sign on to the system.

user record. A record in the resource security file that allows access to the resource at a specific access level.

valid. (1) Allowed. (2) True, in conforming to an appropriate standard or authority.

view. To look at information on a display screen without being able to change that information. (BGU/36) To show a graph or chart on a display.

work station. A device that lets people transmit information to or receive information from a computer; for example, a display station or printer.

Index

Special Characters

*NULL
password 2-6
user ID 1-9, 2-29, 3-3, 3-31
user profile 2-29

A

access levels
default 3-1
for files, libraries, and groups
change 3-2
none 3-2
owner 3-2
read 3-2
run 3-2
update 3-2
for folders and folder members 3-15
change 3-16
none 3-17
read 3-17
update 3-16
for folders, subdirectories,members
run 3-17
for folders, subdirectory, and folder members
owner 3-15
for user programs A-1
for using the system programming A-1
minimum
to run programs or procedures A-1
OCL statements A-2
procedure control expressions A-2
procedures and commands A-3
access, limit
to system room 1-1
to system unit 1-2
activating
badge security 2-20
password security 2-10
resource security 3-22
add
authorization lists 3-59
location profiles 2-44
security information for
folders and folder members 3-59
user profiles 2-34
alternative index file
create over physical file secured by a group 3-7
create over secured physical file 3-6
create over unsecured physical file 3-7
secure over secured physical file 3-6
alternative index files 3-6
APPC 1-9, 2-30
authorization lists
adding 3-59
changing 3-59
entering into resource security file 3-32
example 3-11
subdirectories 3-13
override 3-11
primary 3-11
remove 3-59

B

badge number
in user profile 2-5, 2-28
badge security
activating 2-20
deactivating 2-83
general description 1-7
magnetic stripe reader 1-7
beginning help menu
changing using command key 24 2-5
in user profile 2-5, 2-29

C

changing
authorization lists 3-59
location profiles 2-44
passwords 2-42
security information for
folder members 3-59, 3-75
folders 3-59
user profiles 2-34
changing the size of
resource security file 3-122
user ID file 2-75
child
files and libraries, example of 3-3
child and parent concept
example of 3-4

command keys
folder members 3-73, 3-76, 3-78
folders 3-69, 3-74
location profiles 2-44
user profiles 2-37
commands
required access level A-3
comment
in location profile 2-6, 2-33
in user profile 2-5, 2-28
communications security
general description 1-9
communications security information
in location profile 2-6
converting System/34 security files C-1
copying
resource security file 3-106
user ID file 2-57
creating
resource security file 3-18
user ID file 2-7

D

data security
badge security 1-7
communications security 1-9
general description 1-3
menu security 1-5
password security 1-4
resource security 1-9
date password last changed
in user profile 2-2
deactivating
badge security 2-83
password security 2-76
resource security 3-124
default access level
for files, libraries, and groups 3-1
for folders and folder members 3-11
default library
in user profile 2-4, 2-29
default sign-on procedure
in user profile 2-4
default user menu
changing using command key 23 2-4
in user profile 2-4, 2-28
delete
security information for
subdirectory 3-70
DFA procedure 2-3
diagrams, syntax
PASSWORD procedure D-1
SECDEF procedure D-2
SECEDIT procedure D-3
SECLIST procedure D-4
SECREST procedure D-5
SECSAVE procedure D-5
disk
example of copying user ID file on 2-63
example of restoring the resource security file from 3-121
example of restoring user ID file from 2-74
restoring resource security file from 3-120
diskette
example of copying resource security file on 3-109
example of restoring the resource security file on 3-116
example of restoring user ID file from 2-67
restore resource security file from 3-113
display
authorization lists 3-59
location profiles 2-44
security information for
folders and folder members 3-59
user profiles 2-34
display station operator
security classification 2-3, 2-28
DUMP procedure 2-3

E

entering
authorization lists 3-32
location profiles 2-30
security information for
files and libraries 3-26
folders and folder members 3-32
user profiles 2-23
example of
copying resource security file on diskette 3-109
copying the resource security file on tape 3-111
copying user ID file on disk 2-63
copying user ID file on tape 2-62
parent and child concept 3-4
restoring the resource security file from disk 3-121
restoring the resource security file from diskette 3-116
restoring the resource security file from tape 3-119
restoring user ID file from disk 2-74
restoring user ID file from diskette 2-67
restoring user ID file from tape 2-72

F

files
- alternative index 3-6
- entering security information for 3-26
- listing security information for 3-79
- parent and child 3-3
- resource security 3-1
- securing 3-1
- user ID 2-1

folder members
- changing security information for 3-59, 3-75
- entering security information for 3-32
- securing 3-10

folders
- changing security information for 3-59
- entering security information for 3-32
- in groups 3-8
- listing security information for 3-93
- securing 3-10

Form O completed 2-24
Form P completed 3-26
Form S completed 2-31
Form T completed 3-33, 3-34, 3-35, 3-36

forms, planning
- completed Form O 2-24
- completed Form P 3-26
- completed Form S 2-31
- completed Form T 3-33, 3-34, 3-35, 3-36

G

generating random hexadecimal location passwords E-1

groups
- listing security information for 3-79
- securing 3-1
- special resource type 3-8

H

hexadecimal location passwords E-1

I

information in user profile 2-1

introduction to
- location profiles 2-6
- resource security file 3-1
- system security 1-1
- user ID file 2-1
- user profiles 2-1

K

keylock
- system unit 1-2

keys, command
- folder members 3-73, 3-76, 3-78
- folders 3-69, 3-74
- location profiles 2-44
- user profiles 2-37

L

libraries
- entering security information for 3-26
- listing security information for 3-79
- parent and child 3-3
- securing 3-1

limit access
- to system room 1-1
- to system unit 1-2

listing
- location profiles 2-54
- resource security file 3-79
- security information for
  - files, libraries, and groups 3-79
  - folders 3-93
- user ID file 2-46
- user profiles 2-46

location password
- generating manually E-1
- hexadecimal E-1
- in location profile 2-6, 2-33
- system generated 2-33

location profiles
- add 2-44
- changing 2-44
- comment 2-6
- display 2-44
- entering 2-30

location profiles *(continued)*
in user ID file 2-1, 2-6
listing 2-54
location password 2-6
remote location name 2-6
scan 2-44
user password required 2-6

M

magnetic stripe reader 1-7
mandatory menu
in user profile 2-4
mandatory procedure
in user profile 2-4
manuals
related x
master security officer
security classification 2-2, 2-28
menu mandatory
general description 1-5
in user profile 2-29
menu security
general description 1-5
menu, mandatory
in user profile 2-4
minimum access levels
to run programs or procedures A-1

O

OCL statements
required access level A-2
other manuals x
override
authorization lists 3-11
password 2-13
user ID 2-13

P

parent
files and libraries, example of 3-3
parent and child concept 3-3
example of 3-4
password
*NULL 2-6
changing 2-42
password *(continued)*
generating hexadecimal location E-1
how to specify 1-4
in user profile 2-2, 2-27
override 2-13
password date checking function
starting 2-16
stopping 2-80
PASSWORD procedure
syntax diagrams D-1
using to
change password 2-42
password security
activating 2-10
deactivating 2-76
general description 1-4
in user profile 2-2
PATCH procedure 2-3
physical security 1-1
diskettes and tapes 1-3
system room 1-1
system unit 1-2
planning forms
completed Form O 2-24
completed Form P 3-26
completed Form S 2-31
completed Form T 3-33, 3-34, 3-35, 3-36
extra B-1
primary authorization lists 3-11
print
location profiles 2-54
security information for
files, libraries, and groups 3-79
folders 3-93
user profiles 2-46
printout
files, libraries, and groups
description of entries 3-84, 3-88, 3-92
folders and authorization lists
description of entries 3-98, 3-102, 3-105
location profiles 2-55
description of entries 2-56
user profiles 2-49, 2-51
description of entries 2-52
printout of files, libraries, and groups
by owner ID 3-90
by resource name 3-82
by user ID 3-86
printout of folders and authorization lists
by owner ID 3-103
by resource name 3-96
by user ID 3-100
procedure control expressions
required access level A-2

procedure, mandatory
in user profile 2-4
procedures
DFA 2-3
DUMP 2-3
PASSWORD D-1
PATCH 2-3
PTF (PATCH parameter only) 2-3
SECDEF D-2
SECEDIT D-3
SECLIST D-4
SECREST D-5
SECSAVE D-5
procedures and commands
required access level A-3
profiles
location 2-6
user 2-1
PTF (PATCH parameter only) procedure 2-3

R

related manuals x
remote location name
in location profile 2-6, 2-33
remove
authorization lists 3-59
location profiles 2-44
resource security file 3-127
security information for
folder members 3-59, 3-75
folders 3-59
user ID file 2-86
user profiles 2-34
required access levels
for user programs A-1
for using the system programming A-1
OCL statements A-2
procedure control expressions A-2
resource security 3-1
activating 3-22
deactivating 3-124
general description 1-9
resource security file
changing the size of 3-122
creating 3-18
entering authorization lists 3-32
entering security information for
files and libraries 3-26
folders and folder members 3-32
introduction 3-1
listing 3-79
removing from disk 3-127
restoring 3-113
from disk 3-120
resource security file *(continued)*
restoring 3-113 *(continued)*
from diskette 3-113
from tape 3-116
saving 3-106
on disk 3-112
on diskette 3-106
on tape 3-109
on tape cartridge . 3-109
restoring
resource security file
from disk 3-120
from diskette 3-113
from tape 3-116
user ID file
from disk 2-73
from diskette 2-64
from tape 2-68
from tape cartridge 2-68
revise
security information for
subdirectory 3-70

S

sample
sign on display
with badge security active 1-7
with security active 1-5
sample, printout
files, libraries, and groups
by owner ID 3-90
by resource name 3-82
by user ID 3-86
folders and authorization lists
by owner ID 3-103
by resource name 3-96
by user ID 3-100
saving
resource security file
on disk 3-112
on diskette 3-106
on tape 3-109
on tape cartridge 3-109
user ID file
on disk 2-63
on diskette 2-57
on tape 2-60
on tape cartridge 2-60
scan
authorization lists 3-59
location profiles 2-44
security information for
folders and folder members 3-59

scan *(continued)*
user profiles 2-34
SECCONV procedure
example C-3
using to convert System/34 security files C-1
SECDEF procedure
syntax diagrams D-2
using to
activate badge security 2-20
activate password security 2-10
activate resource security 3-22
create resource security file 3-18
create user ID file 2-7
deactivate badge security 2-83
deactivate password security 2-77
deactivate resource security 3-124
remove resource security file 3-128
remove user ID file 2-86
SECEDIT procedure
syntax diagram D-3
using to
change authorization lists 3-55, 3-60
change location profiles 2-44
change security information for files, libraries, groups 3-55
change security information for folders and folder members 3-60
change user profiles 2-35
enter location profiles 2-32
enter security information for files, libraries, and groups 3-28
enter user profiles 2-26
secure folder members 3-50
SECLIST procedure
syntax diagrams D-4
using to
list file, library, and group security information 3-80
list folder security information 3-93
list location profiles 2-54
list user profiles 2-47
SECREST procedure
syntax diagram D-5
using to
restore resource security file from disk 3-120
restore resource security file from diskette 3-113
restore resource security file from tape 3-116
restore user ID file from disk 2-73
restore user ID file from diskette 2-64
restore user ID file from tape 2-68
SECSAVE procedure
syntax diagram D-5
using to
save resource security file on disk 3-112
save resource security file on diskette 3-106
save resource security file on tape 3-109
SECSAVE procedure *(continued)*
using to *(continued)*
save resource security file on tape cartridge 3-109
save user ID file on disk 2-63
save user ID file on diskette 2-57
save user ID file on tape 2-60
securing
diskettes 1-3
files 3-1, 3-28
folder members 3-10, 3-32, 3-50
folders 3-10, 3-32
groups 3-1, 3-28
libraries 3-1, 3-28
subdirectories 3-32
tapes 1-3
security
badge 1-7
communications 1-9
data 1-3
menu 1-5
password 1-4
physical 1-1
procedures D-1
resource 1-9
syntax diagrams D-1
security classification
display station operator 2-3
in user profile 2-2, 2-28
master security officer 2-2
security officer 2-2
subconsole operator 2-3
system console operator 2-3
security officer
security classification 2-2, 2-28
service aid authority
in user profile 2-3, 2-28
service aid procedures
DFA 2-3
DUMP 2-3
PATCH 2-3
PTF (PATCH parameter only) 2-3
sign on display
badge security active 1-7
password security active 1-5
size of user ID file
calculating 2-9
special resource types
alternative index files 3-6
groups 3-8
system library 3-10
starting
password date checking function 2-16
stopping
password date checking function 2-80

subconsole operator
security classification 2-3, 2-28
subdirectory
changing security information for 3-70
syntax diagrams
PASSWORD procedure D-1
SECDEF procedure D-2
SECEDIT procedure D-3
SECLIST procedure D-4
SECREST procedure D-5
SECSAVE procedure D-5
system console operator
security classification 2-3, 2-28
system library 3-10
system security
introduction 1-1

T

tape
example of copying the resource security file on 3-111
example of copying user ID file on 2-62
example of restoring the resource security file from 3-119
example of restoring user ID file from 2-72
restore user ID file from 2-68
restoring resource security file from 3-116
saving resource security file on 3-109
saving user ID file on 2-60
tape cartridge
restore user ID file from 2-68
restoring resource security file from 3-116
saving resource security file on 3-109
saving user ID file on 2-60

U

user ID
how to specify 1-4
in user profile 2-2, 2-27
override 2-13
user ID file
calculating the size of 2-9
changing profiles in 2-34
changing the size of 2-75
creating 2-7
entering profiles into 2-23
introduction 2-1
listing 2-46
removing 2-86
user ID file *(continued)*
restoring 2-64
from disk 2-73
from diskette 2-64
from tape 2-68
from tape cartridge 2-68
saving 2-57
on disk 2-63
on diskette 2-57
on tape 2-60
on tape cartridge 2-60
user password required
in location profile 2-6, 2-33
user profiles
add 2-34
badge number 2-5
beginning help menu 2-5
changing 2-34
comment 2-5
date password last changed 2-2
default library 2-4
default sign-on procedure 2-4
default user menu 2-4
display 2-34
entering 2-23
password security not active 2-23
in user ID file 2-1
information contained in 2-1
listing 2-46
mandatory menu 2-4
mandatory procedure 2-4
password 2-2
remove 2-34
scan 2-37
security classification 2-2
service aid authority 2-3
user ID 2-2
when password security is active 2-1
when password security is not active 2-1
user programs
required access level A-1

READER'S COMMENT FORM

Please use this form only to identify publication errors or to request changes in publications. Direct any requests for additional publications, technical questions about IBM systems, changes in IBM programming support, and so on, to your IBM representative or to your IBM-approved remarketer. You may use this form to communicate your comments about this publication, its organization, or subject matter, with the understanding that IBM may use or distribute whatever information you supply in any way it believes appropriate without incurring any obligation to you.

☐ If your comment does not need a reply (for example, pointing out a typing error), check this box and do not include your name and address below. If your comment is applicable, we will include it in the next revision of the manual.

☐ If you would like a reply, check this box. Be sure to print your name and address below.

Page number(s): Comment(s):

Please contact your IBM representative or your IBM-approved remarketer to request additional publications.

Name _____

Company or Organization _____

Address _____

_____
City State Zip Code

Phone No. _____
Area Code

No postage necessary if mailed in the U.S.A.

Cut Along Line

Fold and tape. **Please do not staple.**

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST CLASS / PERMIT NO. 40 / ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

International Business Machines Corporation
Information Development
Department 245
Rochester, Minnesota, U.S.A. 55901

Fold and tape. **Please do not staple.**

Cut Along Line

IBM®

IBM®

International Business Machines Corporation

System Security Guide

File Number
S36-36

Order Number
SC21-9042-4

Part Number
59X3971

Printed in U.S.A.