Security System

For Administrators with QUAD-A Access

M-DCPS

Technology Learning Center

TABLE OF CONTENTS

Miami-Dade County Public Schools
Information Technology Services

INTRODUCTION

This user guide is restricted to work site security authorizing administrators, Administrators with QUAD-A access only.

Authorizing administrators have been defined as: (1) all school principals; (2) administrators at the Director level and above in non-school site locations; or, (3) the senior administrator of work sites not having a Director or above.

Each work site administrator controls the access of employees at that work location to M-DCPS computer systems by indicating which applications each employee is authorized to use. This responsibility cannot be delegated.

The security system is entirely employee based. It allows M-DCPS employees to access only those mainframe and web applications which have been approved by work site administrators. Access to the computer systems, approved and designated by the work site administrator, is controlled by employee number, work location number and a personal employee generated password.

The personal employee password is known only to the individual employee. Each authorized employee is responsible for establishing and changing a personal password and for maintaining its confidentiality. This password shall not be revealed to another individual.

When an authorized employee has been cleared through the security screen and has accessed any one of the M-DCPS computer systems, all activity performed by the individual is recorded by the computer. Should any unauthorized, incorrect, or misuse of the systems or data occur, the employee will be held accountable. If you allow another person to access any application by giving him/her your password, or by "signing on" with your password and allowing another person to perform any activity, **YOU ARE RESPONSIBLE AND WILL BE HELD ACCOUNTABLE**.

The following topics related to authorizing employees to access M-DCPS computer systems are presented in this user guide:

1. "Sign on" procedures.
2. Personal Passwords.
3. Authorizing work site employees to access designated computer systems.
4. Canceling authorizations.
5. Reestablishing (resuming) access for an employee when revoked.
6. Requesting a new personal password for an employee.

> Reminder: Use the M-DCPS Password Management application to reset your passwords at any time. To be able to use Password Management you must complete the security questions and your profile with an external email and/or a mobile phone number. The M-DCPS Password Management hyperlink is located in dadeschools.net/employees.asp under the **Log in to Employee Portal** button. *[Go to e-Handbooks to view the M-DCPS Password Management for Employees user guide.]*

SIGNING ON

BlueZone terminal emulation software is required to access systems residing on the the *Miami-Dade County Public Schools (M-DCPS)* mainframe (CICS, DSIS, TRVL, etc.). Users can access the BlueZone installation from the *BlueZone Access To Mainframe* button located within the **APPS|SERVICES|SITES** section of the Employee Portal.

Apps | Services | Sites	Resources	Reports	Search this site...	

Welcome to Applications, Services, and Sites Page

Welcome to your Applications, Services, and Sites.

For easy access to your favorite applications, services, and sites click on the star appearing next to application. The application icon will appear on the Favorites Toolbar. To remove it, click on the star again, and the icon will be removed from the Favorites Toolbar.

Adult Ed. FOCUS Training
Training environment for FOCUS

eSAS Support Page
eSAS Tutorials and Help Files

PDMS - Professional Development Management Plan
Professional Development Management System

Alison
Free online professional typing tutor that helps increase typing speed and accuracy for all educators, students, and parents.

ESE-EMS
Exceptional Student Education Electronic Management System

PowerSchool
Formerly TeacherMatch

Attachment Manager
This application will allow you to temporarily store large files for e-mail distribution.

EVERFI
Critical skills resources for financial education, health & wellness, and STEM available for teachers and students.

PowerTyping
Free online typing tutor for QWERTY keyboards to improve typing skills for all educators, students, and parents.

Be a School Volunteer

FLDOE SSO Login
FLDOE SSO shortcut - search for Dade County

ProQuest
General reference collection of periodicals, digital media and research tools designed to support secondary users.

BlueZone Access to Mainframe
New access to Mainframe Sessions

GALE
A comprehensive collection of databases containing authoritative periodicals and scholarly journals.

ProQuest Homework Central

Please reach out to your site technician or submit an incident ticket if you have issues installing BlueZone on your computer or require additional assistance.

SIGNING ON

Once BlueZone is installed and launched, users should see a screen similar to the following:
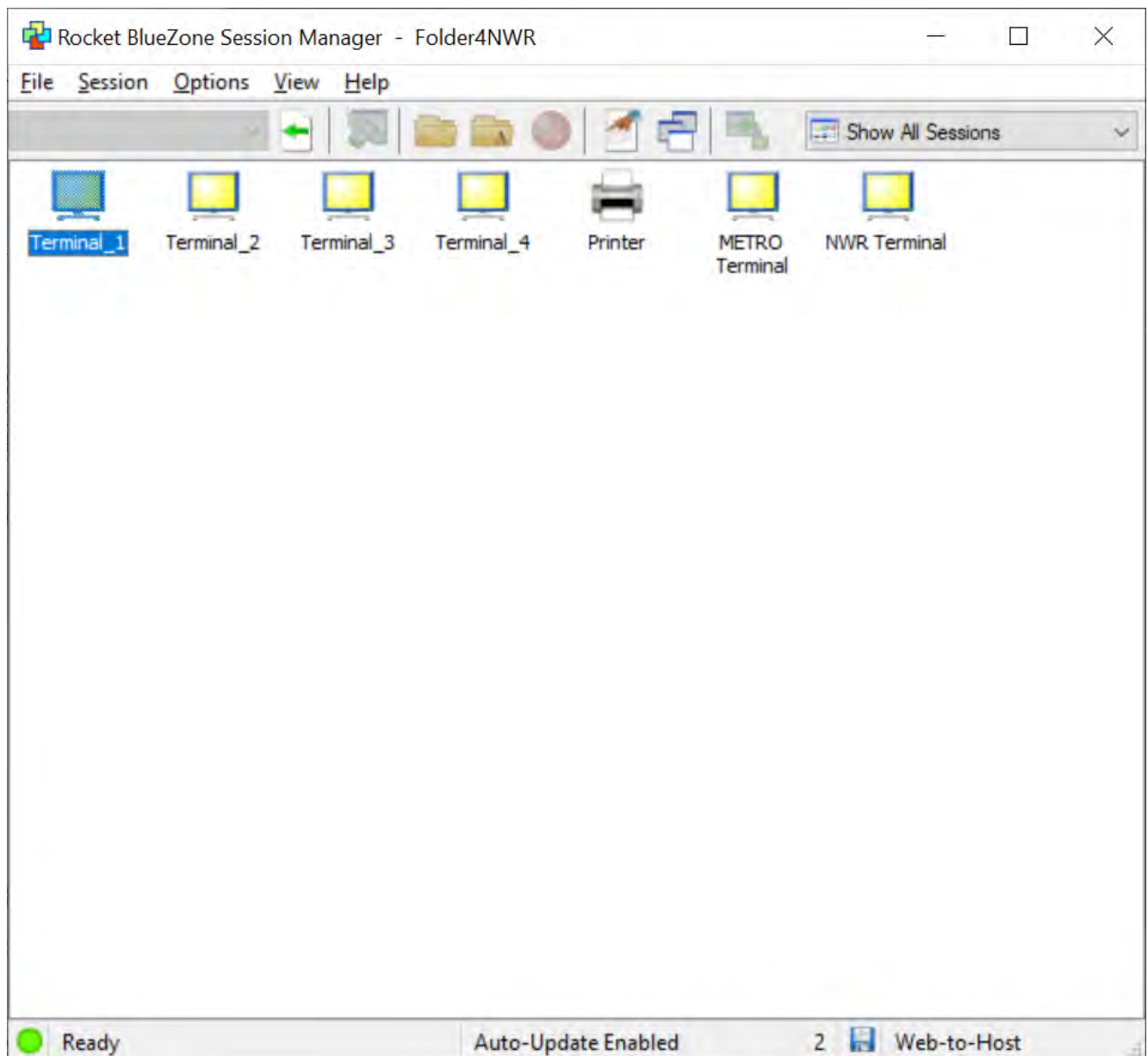
Please note that not all users will have the same number of terminal sessions listed in the Session Manager screen, and some terminals such as "METRO" and "NWR" may not be present.

Double click the icon for an available terminal listed on this screen to launch an emulation session. If you receive an error message when launching a terminal session, please contact your site technician or submit an incident ticket for additional assistance.

SIGNING ON

From the **Teleprocessing Network** screen,

```
                                                    Terminal= LDDAG6LH
                     Teleprocessing Network                      Page   1
Application Status                      13:55, Wednesday, April   04, 2018
APPLNAME STATUS          ! APPLNAME STATUS            ! APPLNAME STATUS
---------------------------------------------------------------------------
TSO      ONLINE  06:14   !                            !
CICS     ONLINE  04:01   !                            !
CTMS     ONLINE  06:14   !                            !
                         !                            !
                         !                            !
                         !                            !
                         !                            !
                         !                            !
                         !                            !
                         !                            !
                         !                            !
                         !                            !
---------------------------------------------------------------------------
Enter application name for connection. Enter TPNEWS for Network news.
       --Information Technology Services  HOTLINE (305) 995-3705----
==>  CICS
PF1=Help       PF3=Return                PF7=Backward       PF8=Forward
```

▼   **Type CICS**

▼   **Press Enter**

The **CICS** security log in screen will display.

```
** PRESS: PF1 FOR PHONE, BULLETIN BOARDS, S&D, A/V AND TEXTBOOK INFORMATION **
SIG1-11-66LH                                         04/04/2018 14.00.06
            PRODUCTION CICS    AT TERMINAL 66LH        PRINTER   66P4
            ====================================================
                 AT THIS TIME YOU MUST SIGN-ON

                 EMPLOYEE NUMBER:     123456

                 WORK LOCATION:       0000

                 PERSONAL PASSWORD:   ........

            (OPTIONAL)   APPLICATION:

            ====================================================

         IF YOU WISH TO CHANGE YOUR PASSWORD, PLEASE ENTER Y BELOW:

                            ==>

PF3 = EXIT CICS     ! BLANK APPLICATION = DISPLAYS APPLICATION LIST
PF1 FOR PHONE, BULLETIN BOARDS, S&D, A/V AND TEXTBOOK INFO   PF5=RACF DEF
```

▼   **Type your employee number**

▼   **Type your work location number**

▼   **Type your personal password**

▼   **Press Enter**

APPLICATION is optional.

The list of **CICS APPLICATIONS** you have access to will display.

> **NOTE: When logging in to CICS for the first time, the password to be used is the employee's birth month and year in the format MMYY; e.g., January 1960 = 0160; October 1982 = 1082.**

> **NOTE: Your password must be exactly eight (8) characters; contain at least one (1) letter and at least one (1) number. It is suggested that you select a combination of letters and numbers which are meaningful to you but cannot be easily guessed by others. You may not reveal your password to anyone.**

For additional information about creating and resetting personal passwords, please refer to user guide **M-DCPS Password Management for Employees** located in the **e-Handbooks** website. The link to the website is in the **APPS|SERVICES|SITES** tab, in the **Employee Portal.**

From the **CICS Applications** screen,

```
APPLICATION AAAA
SIG2-12-G6LH          IST FOR SAMPLE EMPLOYEE          AT 0000    04/09/2018 14.01.37

AAAA SECURITY ACCESS      WRPT WEB CNTL-D REPORTS
MAIL ELECTRONIC MAIL      WHRS WEB HUM RES SERV
ACES CHARTER SCHOOLS      WBS  WEB BUSINESS SERV
PARL PARS MAINTENANCE     WSS  WEB STUDENT SERVIC
PARS PAYROLL ABS RPT      WMSA WEB MSA SERVICES
RSTR PAYROLL APPROVAL
UWAY UNITED WAY
SUBS SUBSTITUTES
ARIS REAPPOINTMENT SYS
SUPP SUPPLEMENT SET UP
PERQ PERSONNEL QUERY
PERS PERSONNEL
PROJ PROJECT ACCOUNTING
PROP PROPERTY CONTROL
SDRQ S&D REQUISITIONS
TRVL TRAVEL
VACS VOC ADULT COMM SCH
WVS  WEB VOC SERVICES

PF1 FOR PHONE, BULLETIN BOARDS, S&D, A/V & TEXTBOOK INFO   PF5=RACF DEF
TYPE APPLICATION CODE OR "ALL" AND PRESS PF2 FOR SYSTEM AUTHORIZATION LIST
```

▼   **Type AAAA for Security Access**

▼   **Press Enter**

The **SECURITY ACCESS - EMPLOYEE SELECTION** screen will display.
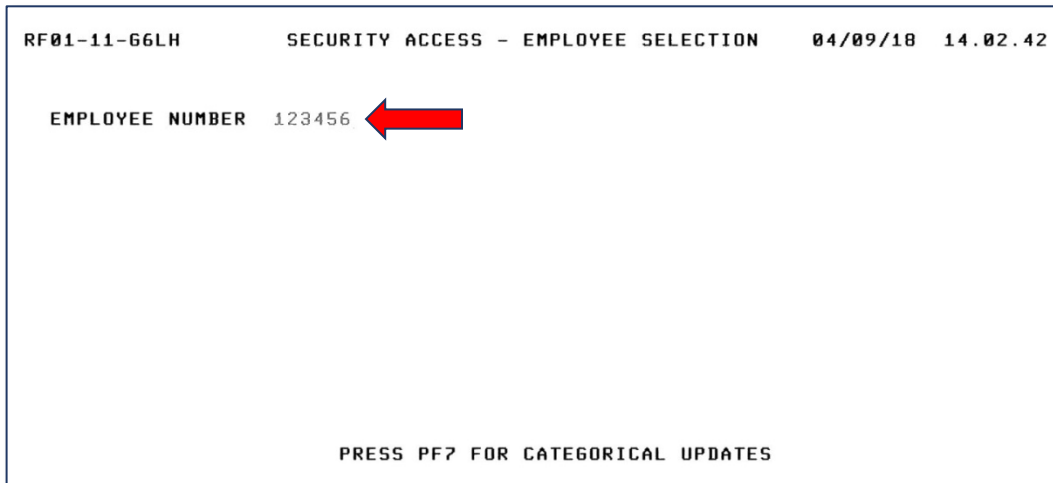
The **SECURITY ACCESS - EMPLOYEE SELECTION** screen shown below is used to indicate which employee at your work location you wish to authorize to use *M-DCPS* computer systems and to categorically authorize employees to access Web Applications.

From the **SECURITY ACCESS – EMPLOYEE SELECTION** screen,

```
RF01-11-66LH       SECURITY ACCESS – EMPLOYEE SELECTION    04/09/18  14.02.42


   EMPLOYEE NUMBER   123456   ⬅






                  PRESS PF7 FOR CATEGORICAL UPDATES
```
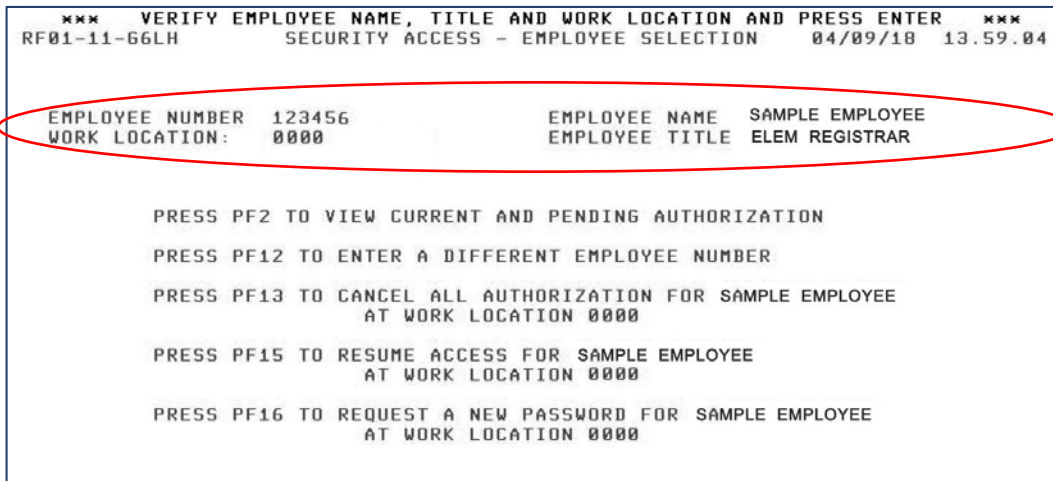
▼   **Type**   the employee number you are authorizing
▼   **Press**   Enter

The employee name, location number and actions will display. The message: **VERIFY EMPLOYEE NAME, TITLE AND WORK LOCATION AND PRESS ENTER** will display at the top of the screen.

```
  ***  VERIFY EMPLOYEE NAME, TITLE AND WORK LOCATION AND PRESS ENTER  ***
RF01-11-66LH        SECURITY ACCESS – EMPLOYEE SELECTION    04/09/18  13.59.04


  EMPLOYEE NUMBER  123456          EMPLOYEE NAME    SAMPLE EMPLOYEE
  WORK LOCATION:   0000            EMPLOYEE TITLE   ELEM REGISTRAR


       PRESS PF2 TO VIEW CURRENT AND PENDING AUTHORIZATION

       PRESS PF12 TO ENTER A DIFFERENT EMPLOYEE NUMBER

       PRESS PF13 TO CANCEL ALL AUTHORIZATION FOR  SAMPLE EMPLOYEE
                 AT WORK LOCATION 0000

       PRESS PF15 TO RESUME ACCESS FOR  SAMPLE EMPLOYEE
                 AT WORK LOCATION 0000

       PRESS PF16 TO REQUEST A NEW PASSWORD FOR  SAMPLE EMPLOYEE
                 AT WORK LOCATION 0000
```

▼   **Press**   Enter

A list of applications for which the Authorizing Administrator is authorized will display.

Using the tab key, position the cursor to the left of each application for which the employee is to be granted access.

▼ **Type**   **A** next to the applications

When all the applications have been designated with an **A.**

▼ **Press**   **Enter**

The message **"TRANSACTION ACCEPTED"** will display.

If the message, **"PRESS ENTER FOR MORE SYSTEMS"** appears at the top of the screen, this indicates that there are more applications selections to be considered for authorization for this employee.

▼ **Press**   **Enter**

Repeat the procedures described above, to add or cancel selections.

When you have finished, you may press **PF2** to verify the authorizations just made for the employee; press **PF12** to authorize a different employee or press **Clear** to return to the **APPLICATIONS** screen.

> **Note:**   **The function displayed at the bottom of the screen, ✳✳✳ PRESS PF12 TO ENTER A DIFFERENT EMPLOYEE NUMBER✳✳✳, will take you back to the**

When authorizations for an employee are added or canceled, they become pending transactions until the next day.

PENDING TRANSACTIONS AND/OR CURRENT AUTHORIZATIONS may be displayed by pressing the **PF2** key on the **SECURITY ACCESS – SYSTEM SELECTION** screen.

The employee cannot access the new (pending) applications until the next day.

Press enter to view **CURRENT AUTHORIZATIONS.**

To view a different employee's current/pending authorizations, press the **PF12** key on the **SECURITY ACCESS – EMPLOYEE SELECTION** screen.

To return to the **SECURITY ACCESS** screen, press the **Clear** key.

CANCELING ALL APPLICATION AUTHORIZATIONS FOR AN EMPLOYEE

In some circumstances, an administrator may need to cancel all systems authorizations for an employee.

From the **SECURITY ACCESS – EMPLOYEE SELECTION** screen,

```
***    VERIFY EMPLOYEE NAME, TITLE AND WORK LOCATION AND PRESS ENTER    ***
RF01-11-66LH          SECURITY ACCESS - EMPLOYEE SELECTION     04/09/18  13.59.04


  EMPLOYEE NUMBER   123456            EMPLOYEE NAME    SAMPLE EMPLOYEE
  WORK LOCATION:    0000              EMPLOYEE TITLE   ELEM REGISTRAR


        PRESS PF2 TO VIEW CURRENT AND PENDING AUTHORIZATION

        PRESS PF12 TO ENTER A DIFFERENT EMPLOYEE NUMBER

        PRESS PF13 TO CANCEL ALL AUTHORIZATION FOR SAMPLE EMPLOYEE
                  AT WORK LOCATION 0000

        PRESS PF15 TO RESUME ACCESS FOR SAMPLE EMPLOYEE
                  AT WORK LOCATION 0000

        PRESS PF16 TO REQUEST A NEW PASSWORD FOR SAMPLE EMPLOYEE
                  AT WORK LOCATION 0000
```

▶   **Press PF13 to cancel all authorizations**

The screen shown above will remain and the message "**TRANSACTION ACCEPTED**" will display at the top of the screen.

The cancellations will be effective on the next day.

The security system allows users 5 consecutive password attempts to correctly enter their employee number, work location number and personal password. After the fifth unsuccessful try, user ID is revoked. Usually, the employee is not entering the personal password correctly and should be advised to ensure that the caps lock key is not on.

It is the responsibility of the work site administrator (school principal or designated administrator in non-school sites) to determine if the employee is or is not authorized to continue access to M-DCPS computer systems. If authorization should continue, the administrator must restore access and request a new password for the employee.

From the **SECURITY ACCESS – EMPLOYEE SELECTION** screen,

```
***    VERIFY EMPLOYEE NAME, TITLE AND WORK LOCATION AND PRESS ENTER    ***
RF01-11-G6LH            SECURITY ACCESS - EMPLOYEE SELECTION    04/09/18  13.59.04


   EMPLOYEE NUMBER  123456          EMPLOYEE NAME   SAMPLE EMPLOYEE
   WORK LOCATION:   0000            EMPLOYEE TITLE  ELEM REGISTRAR


        PRESS PF2 TO VIEW CURRENT AND PENDING AUTHORIZATION

        PRESS PF12 TO ENTER A DIFFERENT EMPLOYEE NUMBER

        PRESS PF13 TO CANCEL ALL AUTHORIZATION FOR SAMPLE EMPLOYEE
               AT WORK LOCATION 0000

        PRESS PF15 TO RESUME ACCESS FOR SAMPLE EMPLOYEE
               AT WORK LOCATION 0000

        PRESS PF16 TO REQUEST A NEW PASSWORD FOR SAMPLE EMPLOYEE
               AT WORK LOCATION 0000
```

▼   **Press**   **PF15** to resume access for employee

The message **TRANSACTION ACCEPTED** will display at the top of the screen.

This action is effective immediately.

REQUESTING A NEW PERSONAL PASSWORD FOR AN EMPLOYEE

The following are situations when the authorizing administrator must request a new password for an employee:

- The access has been revoked by the system and subsequently restored by the authorizing administrator; this typically occurs as a result of too many invalid password attempts.
- The employee forgets his/her personal password.
- There has been a breach of security and someone other than the employee has learned the password.

From the **SECURITY ACCESS – EMPLOYEE SELECTION** screen,

```
***    VERIFY EMPLOYEE NAME, TITLE AND WORK LOCATION AND PRESS ENTER    ***
RF01-11-G6LH            SECURITY ACCESS - EMPLOYEE SELECTION    04/09/18  13.59.04


     EMPLOYEE NUMBER  123456            EMPLOYEE NAME   SAMPLE EMPLOYEE
     WORK LOCATION:    0000             EMPLOYEE TITLE  ELEM REGISTRAR


         PRESS PF2 TO VIEW CURRENT AND PENDING AUTHORIZATION

         PRESS PF12 TO ENTER A DIFFERENT EMPLOYEE NUMBER

         PRESS PF13 TO CANCEL ALL AUTHORIZATION FOR  SAMPLE EMPLOYEE
                    AT WORK LOCATION 0000

         PRESS PF15 TO RESUME ACCESS FOR  SAMPLE EMPLOYEE
                    AT WORK LOCATION 0000
         PRESS PF16 TO REQUEST A NEW PASSWORD FOR  SAMPLE EMPLOYEE
                    AT WORK LOCATION 0000
```

▼   **Press**   **PF15** to resume access for employee

The message **TRANSACTION ACCEPTED** will display at the top of the screen.

▼   **Press**   **PF16** to request a new password for employee

The message **TRANSACTION ACCEPTED** will display again.

The authorizing administrator must then advise the employee to sign in using his/ her birth month and year (MMYY) as the personal password. The employee must follow the procedures for creating a new personal password.

REQUESTING ADDITIONAL AUTHORIZATION AS AN ADMINISTRATOR

It may be necessary for you to request access to additional applications as an authorizing administrator.

If you can justify such access to additional applications, please create a Self Service Incident via ISM. You can access ISM by clicking on the *ISM* button located within the **APPS|SERVICES|SITES** section of the Employee Portal. To submit a request for additional authorizations, select Operational Services as the ISM service and then select RACF Authorization as the category. The Data Security Team will review your request and notify you when the addition(s) have been completed as appropriate.

WHOM TO CONTACT FOR ASSISTANCE

For additional assistance or questions not addressed within this document pertaining to BlueZone, AAAA, or any related systems, users should submit an ISM Self Service incident by clicking on the *ISM* button located within the **APPS|SERVICES|SITES** section of the Employee Portal. For issues with BlueZone installation, please select the ISM category "Site Based" from the list of available options. For issues within the application itself, missing authorizations, issues authorizing staff, etc., please select the ISM category "Application" from the available options.