ADMINISTRATIVE PROCEDURE

INFORMATION TECHNOLOGY SERVICES
EMPLOYEE IDENTITY AND
ACCESS MANAGEMENT

0703
Procedure No.

July 1, 2019
Date

I. **PURPOSE:** To provide standards for usernames and passwords used on all PGCPS computer networked systems and related technology.

II. **INFORMATION:** As an employee of Prince George's County Public Schools, all staff will need access to computer based systems. Access will be required to manage school system information including but not limited to student information, Human Resources, Payroll, Benefits, Finance, Purchasing, and Email.

III. **BACKGROUND:** All employee accounts are automatically provisioned with basic access once they are onboarded through Oracle Human Resources Management System (HRMS). Elevated access specific to certain job functions are added subject to this procedure.

IV. **DEFINITIONS:**

A. Enterprise Resource Planning (ERP) or Oracle E-Business Suite (EBS), is a software that PGCPS uses to manage business information related to Human Resources, Payroll, Benefits, Finance and Purchasing.

B. Student Information System (SIS) is a web based application, used by PGCPS to manage data related to student course registration, attendance, grade reporting and transcripts. Username (UserID) is a unique identifier used with a password to gain access to PGCPS computer based systems.

C. Password is a secret sequence of letters, numbers and other symbols needed along with a username to gain access to the system.

D. Single Sign-On (SSO) Login is a mechanism that allows a user to access multiple applications with one Username and Password.

E. DISA is an acronym for Departmental Information Security Administrator. This person is responsible for ensuring all personnel in their department have appropriate access to information on the ERP system.

V. **PROCEDURES:**

A. **Central Office Staff**

1. Before an ERP (Oracle) account can be obtained, training in Payroll, iProcurement, or Financial Applications must be completed. Training information can be obtained at:

https://sites.google.com/a/pgcps.org/training/.

2. All administrative staff that requires access to the ERP system must complete an Oracle Authorization Form located at https://sites.google.com/a/pgcps.org/oracle/forms. Select the authorization you need, open the document and print it out. Complete the form, sign it, and forward it for appropriate signatures.

   Administrative accounts are signed by the supervisor and the Departmental Information Security Administrator (DISA). When the form is complete, the DISA will forward the original signed form to Information Technology, Sasscer Administration Building, Room 135.

3. All initial account applications should have the '**new account**' box checked. When access is no longer desired for an employee (due to transfer, etc.), a form should be submitted for that employee with the '**remove access**' box checked. **This step is very important to maintain the security of our data.**

4. **Before a SIS account can be obtained an authorization form must be submitted. SIS authorization forms are located at:** https://sites.google.com/a/pgcps.org/schoolmax/forms.

   All initial account applications should have the 'new account' box checked. If access is to be changed, a new form indicating 'update existing account' should be submitted. When access is no longer desired for an employee (due to transfer, etc.) a Help Desk ticket should be opened by the Supervisor requesting that the account be terminated. Central Office accounts are authorized by the employee's Supervisor.

B. School Staff

1. Before an Oracle ERP account can be obtained, training in Payroll, iProcurement, or Financial Applications must be completed. Training information can be obtained at https://sites.google.com/a/pgcps.org/training/.

2. All school staff that requires access to the ERP system must complete an Oracle Authorization Form located at https://sites.google.com/a/pgcps.org/oracle/forms. Select the authorization you need, open the document and print it out. Complete the form, sign it, and forward it for appropriate signatures. School staff forms requesting

financial access are signed by the Principal. Payroll access must be authorized by the Principal and Instructional Director. When the form is complete it should be faxed to Enterprise Systems at (301) 952-6211.

3. Before a SIS account can be obtained an authorization form must be submitted. SIS authorization forms are located at: https://sites.google.com/a/pgcps.org/schoolmax/forms.

4. SIS (SchoolMax) access must be authorized by the Principal. When the form is complete, please fax it to Enterprise Systems at (301) 952-6211.

5. All initial account applications should have the 'new account' box checked. If access is to be changed, a new form indicating 'update existing account' must be submitted. When access is no longer desired for an employee (due to transfer, etc.) a Help Desk ticket should be opened by the Supervisor requesting that the account be terminated. School Staff accounts are authorized by the School's Principal.

C. **Usernames (USERIDS)**

1. All usernames are automatically generated for staff.

2. All usernames must have a password.

3. User accounts for terminated personnel will be end-dated immediately.

4. User accounts for retiring personnel will be end-dated on retirement date.

5. Usernames are assigned to one individual only. In the event that the user severs employment and returns at a later date, their original username will be reinstated.

6. Usernames are **NOT** to be shared under any circumstance. Employees are responsible for any and all activity conducted under their username.

D. **Passwords**

1. Each individual with approved access to PGCPS computer systems will create unique passwords for their account and will safeguard and protect all passwords.

2. Password Rules

   a. Passwords **must** be a minimum of 8 characters.

   b. Passwords **must** contain at least 1 number.

   c. Passwords **must** be changed every 90 days.

   d. Passwords must not be similar to your current password, logon name and/or legal name.

   e. Passwords **cannot** contain repeated characters (aa22bb).

   f. Passwords must not match one of your last 10 passwords.

3. Password Creation Recommendations

   a. Choose a line or two from a song, slogan, quote, or poem, and use the first letter of each word.

   b. Alternate between one consonant and one or two vowels. This provides nonsense words that are usually pronounceable and easily remembered.

   c. Choose two short words and link them together with a punctuation character between them.

   d. Use a password of a phrase you can recall easily and use the first letter of each word. For example: tpomwh2c – "the picture on my wall has 2 cats".

   e. **Do not** use your spouse's or child's name.

   f. **Do not** use other information easily obtained about you, such as your house number, street address, license plate, your dog or cat's name, etc.

   g. **Do not** use words that are in the dictionary or well-known phrases; there are programs that can 'crack' these passwords.

VI. **MONITORING AND COMPLIANCE**: Designated staff in the Division of Information Technology will monitor compliance with AP using appropriate Identity Management and Password Policy Enforcement tools.

VII. **RELATED PROCEDURES:** Administrative Procedure 0700, Information Technology Services-Acceptable Usage Guidelines and Administrative Procedure 0701, Information Technology Services-Employee E-Mail Procedure.

VIII. **MAINTENANCE AND UPDATE OF THESE PROCEDURES:** This Administrative Procedure originates with the Division of Information Technology and will be updated, as needed.

IX. **CANCELLATIONS AND SUPERSEDURES:** This Administrative Procedure cancels and supersedes Administrative Procedure 0703, dated August 1, 2006.

X. **EFFECTIVE DATE:** July 1, 2019.

Distribution: Lists 1, 2, 3, 4, 5, 6, 7, 9 and 10