OKLAHOMA CITY COMMUNITY COLLEGE

NO. 3061 ACCESS TO INTEGRATED INFORMATION SYSTEM DATA AND PASSWORDS

1.0 PURPOSE: Oklahoma City Community College ("OCCC") is committed to protecting system data from unauthorized access. Access to information system data is limited to those who need to use the information in the performance of their job responsibilities.

2.0 SCOPE: The Scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) or an IT system that resides at any OCCC facility, has access to the OCCC network, or stores any non-public OCCC information.

3.0 SYSTEM ACCESS: System access, based on user need, is requested via Tech Support (techsupport@occc.edu). Upon receiving the request, Information and Instructional Technology Services "IITS" will contact the appropriate employee for the requested system.

3.1 Requests for system access information will be directed to the following employees:

3.1.1 Student Data – College Registrar

3.1.2 Employee Data – Director of Compensation and Human Resources Systems

3.1.3 Core Data – Director of Finance

3.2 Access to student information will comply with the Family Educational Rights and Privacy Act (FERPA) guidelines for legitimate educational interest.

3.3 Access to employee information will comply with applicable state and federal laws and regulations regarding employee privacy.

3.4 Access to financial information will comply with generally accepted accounting principles and applicable financial disclosure laws and regulations.

3.5 Job requirements, as defined in employee's job description, will also be a consideration in granting access to student, employee, financial or core information.

3.6 Access to applications is assigned and disseminated to users by Information and Instructional Technology staff.

3.7 If request for system access is denied an employee may appeal to the Vice President for Enrollment and Student Services for access to student information; to the Vice President for Human Resources for employee information; to the Vice President for Business and Finance for access to financial information; or the Vice President for Information and Instructional Technology for Core access.

4.0 PASSWORDS: Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of an entire system or application. As such, all OCCC employees (including contractors and vendors with access to OCCC systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their password. The regular changing of information system passwords is a critical component of the comprehensive OCCC system security plan

4.1 GENERAL

4.1.1 All system-level passwords (e.g. root and system administrator accounts) must be changed every six (6) months.

4.1.2 All administrative-level passwords (e.g., administration accounts, etc.) must be changed every six (6) months.

4.1.3 All users must change their passwords (e.g., e-mail, voice-mail, Datatel, computer, applications, laptops or mobile devices, etc.) at least every ninety (90) days.

4.1.4 Only temporary passwords should be inserted into e-mail messages and should be changed immediately. Regular passwords should not be inserted into e-mail messages.

4.1.5 All passwords should conform to the guideline distributed in a reminder e-mail.

4.2 PASSWORD PROTECTION STANDARDS

4.2.1 Do not use the same password for OCCC accounts as for other non-OCCC access (e.g., personal Internet Service Provider or e-mail accounts). Where possible, do not use the same password for various OCCC access needs.

4.2.2 All passwords are to be treated as sensitive and confidential OCCC information.

4.2.3 List of Unacceptable Password Practices

4.2.3.1 Do not share OCCC passwords with anyone, including administrative assistants or co-workers per Policy 3058, Section 1.4.1, Network Acceptable Use;

4.2.3.2 Do not reveal a password over the telephone to anyone;

4.2.3.3 Do not reveal a password to your supervisor;

4.2.3.4 Do not hint at the format of a password (e.g., “my family name”);

4.2.3.5 Do not talk about a password in front of others;

4.2.3.6 Do not reveal a password on questionnaires or security forms;

4.2.3.7 Do not share a password with family members;

4.2.3.8 Do not reveal a password to co-workers while on vacation;

4.2.3.9 Do not write passwords down and store them anywhere in your office,

4.2.3.10 Do not store passwords in a file on ANY computer system (including but not limited to desktops, laptops, portable storage devices and mobile electronic devices, or similar devices) without encryption.

4.2.4 List of Required Password Practices

4.2.4.1 If someone demands a password, refer them to Policy 3061, Access to Integrated Information System Data and Passwords or have them contact the office of the Vice President for Information and Instructional Technology.

4.2.4.2 If an account or password is suspected to have been compromised, change your passwords immediately and report the incident to the office of the Vice President for Information and Instructional Technology.

5.0 ENFORCEMENT: Any employee found to have violated this policy will be subject to disciplinary action, up to and including termination of employment.

Effective: August 5, 2002
Revised: December 20, 2004
Revised: May 17, 2010