CCS Administrative Procedure
7.30.10-B Access Controls over Information Systems

Implementing Board Policy 7.30.10
Contact: District Director of Fiscal Services, 434-5210

1.0 Purpose

This procedure addresses the access security controls over the applications within the HP3000. Access security controls restrict authorized users to the application(s) or application function(s) they need to do their jobs, supporting an appropriate segregation of duties. This procedure provides for reviews of user profiles that permit or restrict access.

2.0 Limitations and Requirements

2.1 All information including personal, financial or academic data and files residing on CCS information systems is confidential and subject to state and federal laws and regulations regarding privacy, confidentiality and disclosure.

2.2 Users are responsible for protecting all information from unauthorized use including personal, financial or academic data residing on CCS information systems, user names or identification, pin numbers and passwords.

2.3 Users must sign a confidentiality statement to document their understanding of the Code of Responsibility for Security and Confidentiality of Records and Files.

2.4 Users must complete an Application Security form when adding or changing a user profile.

2.5 Application Security forms must be signed by the user's supervisor and security coordinator(s).

2.6 Supervisors must immediately notify Information Systems to terminate access when a user leaves CCS or when a change in a user's job duties and/or employment status (full/part time) requires a modification to the user's existing account.

3.0 Definitions

3.1 User - full-time employee, part-time employee, work study student, volunteer or student intern.

3.2 Applications - software designed to help the user perform singular or multiple related specific tasks to process business transactions. Applications used by CCS include:

3.2.1 Student Management Systems (SMS) – includes the modules and functions of Course-Class Management, Admissions, Registration, Program Enrollment, Grades and Transcripts, Student Progress, State, Federal and Other Reporting Web Applications and College Parameters and SMS Screen Descriptions. CampusCE, a web based application, shares information with SMS.

3.2.2 Financial Aid System (FAS) - includes needs analysis, application tracking, award management, student loans, student work monitoring, external reporting, and disbursements as well as Financial Aid Management (FAM), a third party software application.

3.2.3 Financial Management System (FMS) – includes the modules and functions of Accounts Payable, Budget, Cashiering, Control Tables and Chart of Accounts, Customer Accounts, Fixed Assets (FAE), General Ledger Accounting, Web Applications, IPEDS Reporting and FMS Query.

3.2.4 Payroll/Personnel Management System (PPMS) – includes the modules and functions of Applicant Tracking, Control Tables, Employee Contracts, Employee Maintenance, Government Reporting, Leave Accounting, Payroll Processing, Position Control and Salary Forecasting.

3.2.5 Database Reporting (currently DATAX only).

3.2.6 Job Scheduling.

3.2.7 Account Management – includes Degree Audit and Financial Aid Management (FAM).

4.0 User Responsibilities

4.1 Secure computer systems passwords, personal account passwords (e.g. Network ID passwords) and personal identification numbers (PINs) at all times. The user will be held accountable for any activities linked to their account(s).

4.1.1 The user must follow established CCS standards for maintaining and managing passwords.

4.1.2 Account passwords for individual accounts must not be shared with others.

4.2 Be aware of and employ security practices established by CCS to prevent unauthorized access to computers. Security breaches can often be linked to the actions individuals take or fail to take when using information technology resources (e.g., not locking computers while away from desks, storing written copies of passwords in obvious places, using insecure methods for transferring information and sharing passwords.

4.3 Protect the security and confidentiality of CCS information and information systems as required by CCS policies and state and federal regulations (e.g., not transmitting social security numbers or other sensitive information on email, USB/Thumb drives, CDs, PDAs or laptops).

4.4 Secure personally-owned computers or other network devices.

4.5 Report security breaches to Information Systems immediately.

4.6 Non-compliance with established policies and practices may result in loss of computing privileges and/or disciplinary action.

5.0 Supervisor Responsibilities

5.1 Verify that the user receives access to application(s) or application function(s) needed to do their job and to support an appropriate segregation of duties.

5.2 Verify the user has the appropriate access level needed for the specific application function(s).

5.3 Ensure the user's password(s) is not shared with other users.

5.4 Notify Information Systems immediately when a change in a user's job duties and/or employment status (full/part time) requires a modification to the user's existing access.

5.5 Notify Information Systems immediately when a user leaves CCS.

5.6 Report security breaches to Information Systems immediately.

6.0 Security Coordinator Responsibilities

6.1 Review the completeness and accuracy of the Application Security form.

6.2 Verify access is appropriate to the user's job responsibilities and that the user does not have unnecessary access to sensitive data or application functions.

6.3 Perform periodic review of user profiles.

7.0 Periodic Review of User Profiles

7.1 On a periodic basis, District Information Systems staff will review the database and:

7.1.1 Remove access for users with a separation code in PPMS, or

7.1.2 Inactivate access for users who have not accessed the application(s) for five (5) consecutive quarters or fifteen (15) months and have not been separated in PPMS. Unused or unneeded user accounts should be removed promptly.

7.2 On a rotational basis, the security coordinator will perform a review of user profiles for their given application(s).

7.2.1 SMS-SFCC and FAS/FAM-SFCC during the Fall quarter of each year beginning in October.

7.2.2 SMS-IEL, FMS and PPMS during Summer quarter each year beginning in August.

7.2.3 SMS-SCC and FAS/FAM-SCC during Winter quarter each year beginning in February.

7.2.4 The review will consist of ensuring all user profiles currently reflect the user's accesses are appropriate through:

7.2.4.1 Interviews with users and supervisors, and

7.2.4.2 Review of system generated reports showing access activity.

8.0 Related information

8.1 Administrative Procedure 2.10.06-A General Ethics for Employees and Officers

8.2 Administrative Procedure 7.30.10-B Acceptable Use of Information Technology Resources

8.3 Computer Account Request, on-line form

8.4 Application Security form, CCS 1436

8.5 Security and Confidentiality Statement, CCS 1441

8.6 Protecting Department Computing Resources

Originated: June 2010
Cabinet approval: June 14, 2010