TIDEWATER COMMUNITY COLLEGE
From here, go anywhere.™

No. 5201 Rev: 2

Policies and Procedures

Date: July 21, 2016

Subject: Access to Information Systems Containing Sensitive Data

1. Purpose

This policy designates Tidewater Community College's System/Data Owners for information systems containing sensitive data, such as the Student Information System (SIS), in order to protect and preserve the confidentiality, integrity, and availability of their data and to comply with the applicable information technology standards of the Virginia Community College System.

2. Policy

The designated System/Data Owners for Tidewater Community College's information systems containing sensitive data shall have the authority to approve access to these

systems.

2.1. Designation of System/Data Owners

The following Executive Staff members are designated as System/Data Owners for information systems containing sensitive data.

2.1.1. Student Information System (SIS)

a. Student Records Module

Vice President for Academic Affairs & Chief Academic Officer

Vice President for Student Affairs

Vice President for Workforce Solutions

Vice President for Institutional Advancement

Vice President for Public Affairs & Communications

Director of Institutional Effectiveness

Executive Director of Real Estate Development & Chief Operating Officer for Facilities

Campus Provosts

b. Student Financials Module

Vice President for Finance

c. Financial Aid Module

Vice President for Finance

2.1.2. Administrative Information System (AIS)

Vice President for Finance

2.1.3. Human Resources Management System (HRMS)

a. HRMS Manager Role

Vice President for Finance

Vice President for Academic Affairs & Chief Academic Officer

Vice President for Student Affairs

Vice President for Workforce Solutions

Vice President for Public Affairs & communications

Vice President for Institutional Advancement

Executive Director of Real Estate Development & Chief Operating Officer for Facilities

Director of Institutional Effectiveness

Executive Assistant to the President

Campus Provosts

b. All Other HRMS Roles

Associate Vice President for Human Resources

2.1.4. ImageNow Document Imaging System

a. Admissions and Advising Drawers

Vice President for Student Affairs

Vice President for Academic Affairs & Chief Academic Officer

Vice President for Public Affairs & Communications

Campus Provosts

b. Student Financial Aid Drawers

Vice President for Finance

c. Accounts Receivable and Business Office Drawers

Vice President for Finance

d. Human Resources Drawers

Associate Vice President for Human Resources

e. Center for Military Education/Veteran Administration Drawers

Vice President for Academic Affairs & Chief Academic Officer

f. IT Security Drawers

Vice President for Information Systems

2.1.5. CS Gold Campus Card System

a. CS Cardlink Module

Associate Vice President for Human Resources

Campus Provosts

b. CS Entitlements and CS Stored Value & Credit Modules

Vice President for Finance

c. CS Access/Action & Response Management Modules

Vice President for Public Affairs & Communications

2.1.6. APEX Disabilities Database

Vice President for Academic Affairs

2.1.7. Workforce Enrollment System (WES)

Vice President for Workforce Solutions

2.2. Requests for Access to Information Systems Containing Sensitive Data

Requests for access to information systems containing sensitive data shall be granted on a “least privilege” basis to only those privileges necessary to perform the individual’s normal work duties.

Executive Staff members who are designated as System/Data Owners shall review requests for access to information systems containing sensitive data from staff members under their administrative authority; validate that users are granted access on a “least privilege” basis to only those privileges necessary to perform their normal work duties; approve requests by signing the Security Access Requests as System/Data Owner; and forward the request forms as needed for approval by other System/Data Owners.

The President shall review and approve Security Access Requests for Executive Staff members who have been designated System/Data Owners.

The Vice President for Student Affairs shall review and approve Security Access Requests for the SIS Student Records Module for staff members in the Office of Information Systems and the Office of Finance.

2.3. Removal of Access to Information Systems Containing Sensitive Data

Executive Staff members shall ensure that supervisors promptly notify the Information Technology (IT) Security Manger when user access to an information system is no longer required or when a user’s access level should be updated based on a change in the employee’s core duties.

The IT Security Manger shall be notified immediately via electronic mail upon termination of an employee that serves in a position that provides enrollment panel or “super user” access (such as a security administrator) or in the event of an employee’s involuntary termination. Notification of routine terminations, transfers to another college department, or changes in duties shall be submitted within five business days.

2.4. Review of Access to Information Systems Containing Sensitive Data

An annual review of all user accounts for the SIS, AIS, and other sensitive IT systems shall be conducted to assess the continued need for the accounts and associated access level. Staff members and their supervisors must sign the audit form confirming that the access is appropriate for the staff and still needed.

A review of the user accounts with access to the SIS Enrollment Panel, SIS Superuser role, AIS Correction role, or WES Power User shall be conducted every 120 days to ensure that the access is still required and that appropriate records are being maintained.

3. Responsibilities

The Vice President for Information Systems shall have overall responsibility for developing and maintaining procedures that are consistent with this policy and comply with the applicable standards of the Virginia Community College System.

4. Procedures

Appendix D to the Information Technology Security Plan (Logical Access Control) provides procedures for requesting access to college information systems.

5. Definitions

Data: any information within Tidewater Community College's purview, including student record data, personnel data, financial data (budget and payroll), student life data, departmental administrative data, legal files, institutional research data, proprietary data, and all other data that pertains to, or supports the administration of the college.

Information System: the total components and operations of a record-keeping process, including information collected or managed by means of computer networks and the Internet, whether automated or manual, containing personal information and the name, personal number, or other identifying particulars of a data subject. (Tidewater Community College Policy 1104 - Privacy)

Sensitive Data: any information which, if compromised with respect to confidentiality, integrity, or availability, could adversely affect the Commonwealth's interests, the conduct of agency programs, or the privacy to which individuals are entitled. Data is classified as sensitive if compromise of that data results in a material and significant adverse affect of the Commonwealth's interest, the inability of the affected agency to conduct its business, and breach of privacy expectations. (Tidewater Community College Policy 1104 - Privacy)

6. References

Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)

Financial Services Modernization Act (Gramm-Leach-Bliley Act) (15 U.S.C. § 6801 *et seq*.)

Health Insurance Portability and Accountability Act (HIPAA) (Public Law 104-191)

Tidewater Community College Policy No. 1104 – Privacy

Tidewater Community College Information Technology Security Plan

VCCS Security Standard 11.2: Access Control – User Account Management

VCCS Technology Standard: Personnel Security – Access Determination and Control

VCCS Technology Standard: Logical Access Control – Account Management

7. Review Periodicity and Responsibility

The Vice President for Information Systems shall review this policy annually and, if necessary, recommend revisions.

8. Effective Date and Approval

This policy is effective upon its approval by the College President on July 21, 2016.

Policy Approved:	Procedure Developed:
Edna V. Bahre-Kolovani, Ph.D. President	Curtis K. Aasen Interim Vice President for Information Systems

9. Review and Revision History

The initial version of this policy was approved on July 17, 2008.

- Revision 1 updates the policy to reflect changes in the administrative organization of the college and addition of new information systems containing sensitive data.

  Approved February 14, 2012 by President Deborah M. DiCroce

- Revision 2 updates the policy with corrected titles of Vice Presidents cited in the policy and added new Executive staff members to areas now requiring their signatures. Removed requirement for Data Owners to sign annual audit form. Added statement that staff and supervisors must sign annual audit form. Removed hyperlinks and versions from References.

  Approved July 21, 2016 by President Edna V. Baehre-Kolovani