TIDEWATER COMMUNITY COLLEGE
From here, go anywhere.™

No. 5200 Rev.: 1

Policies and Procedures Date: February 28, 2012

Subject: Information Technology Security Program

1. Purpose 1
2. Policy 1
   - 2.1. Program Elements 1
   - 2.2. Applicability and Scope 2
   - 2.3. TCC Prerogatives 2
   - 2.4. IT Security Committee 3
3. Responsibilities 3
4. Procedures 4
5. Definitions 4
6. References 5
7. Review Periodicity and Responsibility 5
8. Effective Date and Approval 5
9. Review and Revision History 5

1. Purpose

This policy sets forth Tidewater Community College's (TCC) Information Technology (IT) Security Program that complies with the requirements identified in the applicable Virginia Community College System (VCCS) Information Technology standards, guidelines, and best practices.

2. Policy

Tidewater Community College is committed to developing, maintaining, and improving an Information Technology (IT) Security Program that provides for the protection of and mitigation of risks to the college's information systems and data.

The TCC IT Security Program shall be based on the "Code of Practice for Information Security Management" published by the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC 17799), appropriately tailored to the specific circumstances of the VCCS and TCC. The program shall also incorporate security requirements of applicable regulations, such as the Family Educational Rights and Privacy Act, Gramm-Leach-Bliley Act, and Health Insurance Portability and Accountability Act.

2.1. Program Elements

The TCC IT Security Program shall include provisions for risk assessment and treatment and the eleven security control clauses that are included in the ISO 27000 IT security standard. This standard shall be regarded as a starting point for developing TCC specific security controls. Not all of the controls and guidance in ISO/IEC 17799 code of practice may be applicable to TCC. Furthermore, additional controls and guidelines not included in this standard may be required.

The TCC IT Security Program shall include the following component areas and shall apply to all college information systems and data:

- Information Technology Security Policy
- Risk Assessment and Treatment
- Organization of Information Security
- Asset Management
- Human Resources Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Information Systems Acquisition, Development, and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance

2.2. Applicability and Scope

The TCC IT Security Program shall apply to TCC faculty and staff in all departments and all locations where essential functions are conducted. The standards and procedures apply to all college information systems and data.

2.3. TCC Prerogatives

Tidewater Community College reserves the prerogative (with or without cause or notice) to:

- Monitor, access, and disclose all data created, sent, received, processed, or stored on Commonwealth of Virginia (COV) or TCC information systems;
- Limit or restrict any individual's access to COV, VCCS, and/or TCC systems;
- Inspect, remove, or otherwise alter any data, file, or system resource that may undermine the authorized use of VCCS or college information technology resources; and

- Review, remove, and/or confiscate (as needed) any equipment connected to a TCC-owned information systems device.

2.4. IT Security Committee

The IT Security Committee shall serve as the forum for communication and collaboration on decisions affecting the policy development, planning, implementation, and operation of IT security controls for the protection of and mitigation of risks to the college's information systems and data. The committee shall review and recommend for approval policies and procedures in the IT Security Program. The committee shall meet at least once each fall and spring semester and report through the Information Security Officer.

The committee shall include the following members:

- Director of Network Services and Support
- Director of Application Development and Support
- Office of Information Systems (OIS) IT Security Manager
- Director of Financial Information Systems and Operations
- Director of Human Resources
- Director of Safety and Security
- Director of Emergency Preparedness
- College Faculty Senate Chair or Designee

3. Responsibilities

The Vice President for Information Systems shall have overall responsibility for developing and maintaining the college's Information Technology Security Program and associated procedures that are consistent with this policy and comply with the applicable VCCS policies, standards, and guidelines.

The Vice President for Information Systems shall serve as college Information Security Officer (ISO). The ISO's duties are as follows:

- Develop and manage the college information technology security program for sensitive systems that meets or exceeds the requirements of VCCS IT security policies, standards, and guidelines in a manner commensurate with risk;
- Verify and validate that college IT systems and data are classified for sensitivity;
- Develop and maintain the information security awareness and training program for the college staff, including contractors and IT service providers;

- Implement and maintain the appropriate balance of preventive, detective, and corrective controls for college IT systems commensurate with data sensitivity, risk, and systems criticality;
- Mitigate and report all IT security incidents in accordance with §2.2-603 of the *Code of Virginia* and VCCS requirements and take appropriate actions to prevent recurrence;
- Coordinate with and provide IT security information to the VCCS ISO as required;
- Manage IT security audits and serve as the primary point of contact for all IT audits and work with the VCCS Chief Information Security Officer and the Director of Internal Audit;
- Oversee the IT Security Committee; and,
- Prepare an annual Statement of Compliance confirming that all appropriate actions have been taken, documents have been prepared in accordance with the VCCS Information Security Program, and that the college is in compliance with the applicable VCCS, State, and Federal requirements.

Faculty, staff, students, and other users of the college's information systems and data shall abide by all applicable Commonwealth of Virginia, Federal, VCCS, and college policies, standards, and guidelines that relate to the security and acceptable use of college computers, network and Internet access, information technology applications, data, and other IT resources.

4. Procedures

The college's Information Technology Security Plan provides security controls and procedures in each of the component areas for implementation of this policy. Distribution of the Information Technology Security Plan is limited to those college staff and external agencies with a need to know. The procedures shall incorporate the requirements, standards, guidelines, and best practices of the VCCS.

5. Definitions

Code of Practice for Information Security Management (ISO/IEC 17799): the international standard that defines guidelines and general principles for the effective management of information security within an organization.

Control: a means of managing risk, including policies, procedures, guidelines, practices, or organizational structures, which can be of administrative, technical, management, or legal nature.

Information Technology (IT) System: an interconnected set of IT resources under the same direct management control.

6. References

Code of Practice for Information Security Management (ISO/IEC 17799:2005), Second Edition, 06/15/2005.

VCCS Information Technology Security Policy, VCCS-ITS-08-5400, Sep. 18, 2008

VCCS Information Security Standard, Version 3.0, of 02/22/2010

VCCS Information Technology Standard: VCCS Information Security Program Annual Statement of Compliance, October 1, 2009

7. Review Periodicity and Responsibility

The College Information Security Officer 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 February 28, 2012.

Policy Approved:	Procedure Developed:
Deborah M. DiCroce President	Richard F. Andersen Vice President for Information Systems

9. Review and Revision History

The initial version of this policy was approved on May 6, 2010.

- Revision 1 updates TCC's IT security policy and plan to reflect the ISO 27000 IT security standard in the "Code of Practice for Information Security Management".

  Approved February 28, 2012 by President Deborah M. DiCroce