Information Security Standard

5.1 - Information Security Program

Version: 2.0
Status: *Revised: 01/14//2013*
Contact: *Chief Information Security Officer*

PURPOSE OF VCCS SECURITY PROGRAM

The VCCS provides shared information technology resources and services to faculty, staff, and college patrons, collectively "Users," for activities supporting the VCCS mission. The purpose of this standard is to protect the integrity of VCCS Technology Resources and the Users thereof against unauthorized or improper use of those resources and to align the goals and principles of information security with VCCS's business strategy and objectives in accordance with VCCS's Information Security Policy. The following standard describes responsible behavior expected by those given access to the technology resources and services. The System Office Information Technology Office will provide practical guidelines for the application of this standard and general oversight to govern the implementation.

DEFINITION

As defined in 44 USC § 3542, Information Security at VCCS means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide:

- **integrity**, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;
- **confidentiality**, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
- **availability**, which means ensuring timely and reliable access to and use of information.

AUTHORITY

The authority for this information security standard is contained within the:

- Privacy Act of 1974, 5 U.S.C. § 552a, which governs the request of personal information and the safekeeping of records maintained on individuals;
- Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g; as reflected in 34 CFR Part 99, which is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education;
- Executive Order of Critical Infrastructure Protection, which ensures protection of information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems, in the information age;
- Federal Child Pornography Statute: 18 U.S.C. & 2252, which governs child pornography statutes;
- Virginia Computer Crime Act:
    - Code of Virginia, 18.2-152.3, Computer fraud and penalties
    - Code of Virginia, 18.2-152.4, Computer trespass and penalties
    - Code of Virginia, 18.2-152.5, Computer invasion of privacy and penalties
    - Code of Virginia, 18.2-152.6, Theft of computer services and penalties
- Library of Virginia Records Management Program, Code of Virginia, Title 42.1, Chapter 7, sec 42.1-85, which outlines the Duties of Librarian of Virginia; requires the agencies to cooperate; and requires the agencies to designate records officer
- Federal Information Security Management Act (FISMA), which Promotes the development of key security standards and guidelines to support the implementation of and compliance with the Federal Information Security Management Act
- Office of Management and Budget (OMB), Circular A-130, which contains numerous policy directives that address the need for development, maintenance, dissemination, and modification of agency public information products and for senior-level management oversight to assure that agencies establish and maintain high quality information systems.

ENFORCEMENT

In addressing the consequences of information security policy violations, VCCS governance recognizes there are federal laws for violations against federal programs or for inter-network activities and there are other specific state and local laws that govern violations which occur in those jurisdictions. Finally, the VCCS's enforcement of these Information Security Standards is independent of possible prosecution under the law. Such enforcement by VCCS may include disciplinary action up to and including loss of employment and benefits.

VCCS governance reserves the right without notice to limit or restrict any individual's access and to inspect, remove or otherwise alter any data, file, or system resource that may undermine the authorized use of any technology resource. VCCS governance also reserves the right to periodically check any system and take any other action necessary to protect its technology resources. VCCS disclaims responsibility for loss of data or interference with files resulting from its efforts to maintain the privacy and security of those technology resources.

SCOPE

This Information Security Standard is applicable to the System Office and Colleges, including all personnel whether employees, students or contractors; all information systems, data, and facilities maintained, whether leased or owned or created within the jurisdiction of the VCCS information technology functions. Hereafter this is collectively referred to as "VCCS Technology Resources." This includes, but is not limited to, information maintained or created by the following:

- Information Technology Services;
- College information processing facilities within the VCCS; e.g., local area networks, standalone microcomputers and other computing equipment that may or may not interact directly with the shared technology resources supported by the VCCS;
- Computer Users; e.g., individual or department, computer, or another application interacting with information processing resources, usually through timesharing, networking, and personal computer technologies and/or are assigned a user account;
- Consultants, contractors, or external processing services that provide processing of information for any division, department or section;
- All individuals who have physical access to information systems owned, leased, or managed by the VCCS;
- All hardware and software in support of and inclusive of any application or operating system regardless of processing mode, including:
    - Batch, remote, distributed processing, client server, networking, inter-networking, intra-networking; and
    - System and applications software, data files, program libraries, or special utility programs.

INFORMATION SECURITY PROGRAM OBJECTIVES

Information and information processing resources are valuable state assets. Access, use and processing of such resources, whether on state-provided devices or non-state-provided devices require adherence to applicable regulations, policies and standards. Information security functions as an enabler to achieve e-business and to avoid or reduce relevant risks. The objectives of information security at the VCCS are to:

- Ensure the processing of information in a secure environment, including all electronic communications;
- Guarantee that the cost of security is commensurate with the value of the information to both the information owner and a potential intruder;
- Guard against the unauthorized modification, destruction, or disclosure of information, whether accidental or intentional;
- Establish safeguards to guarantee the integrity and accuracy of vital information;
- Provide the ability for the colleges and the System Office to effectively recover from unplanned business interruptions or disasters;
- Teach employees local security policies and train them to support the policies; and
- Require compliance with all VCCS Information Security Standards, Policies and Procedures, and all appropriate federal regulations and requirements that relate to the control of and access to the VCCS information and information processing resources.

FRAMEWORK FOR CONTROL OBJECTIVES AND CONTROLS

The requirements for the VCCS Information Security Program are derived from three main sources:

1) The first source is through a formal risk assessment and treatment process; which includes identification of threats, evaluation of vulnerabilities and their likelihood of occurrence, potential impact of exploitation, and controls to remediate;
2) The second source is the legal, statutory, regulatory, and contractual requirements that VCCS has to satisfy; and
3) The third source is the particular set of principles, objectives and business requirements for information processing that VCCS has developed to support its operations.

VCCS governance has adopted ISO/IEC 27001:2005 Information Technology – Security Techniques – Information Security Management Systems – Requirements and ISO/IEC 27002:2005(E) Information Technology – Security Techniques – Code of Practice for Information Security Management as the framework to be used in developing the Information Security control objectives and controls.

VCCS governance has also determined that the VCCS Information Security Program will align with VCCS's strategic risk management approach which is based on ISO/IEC 27005:2008 Information Technology – Security Techniques – Information Security Risk Management and has directed that the VCCS Information Security Program will be established and maintained within the context of that strategic risk management approach.

SECURITY POLICIES, STANDARDS, AND COMPLIANCE REQUIREMENTS

VCCS governance considers it essential to communicate its information security requirements throughout the organization to all users in a form that is relevant, accessible, current, and understandable to any reader. VCCS governance has chosen the Internet to be the communication vehicle. All VCCS information security standards, procedures, guidelines and templates are available at:

http://system.vccs.edu/its/InformationSecurityProgram/

This includes legal, regulatory, and contractual requirements; security awareness training; and business continuity management.

RESPONSIBILITIES

The System Office Information Technology Services Office is responsible for the establishment and coordination of all information security requirements on a system-wide basis. The Vice Chancellor for Information Technology Services is responsible for the VCCS Technology Resources and for developing system-wide information security standards, information security acceptance models and the related information security plans. Each college president is responsible for the development, implementation and enforcement of local information security plans to satisfy the objectives set forth in this standard. VCCS Information Technology Services Office will provide models to assist colleges in the development of these plans.

The Assistant Vice Chancellor for Human Resource Services and Affirmative Action is responsible for ensuring that all System Office employees have a signed Information Technology Employee Computer Acceptable Use Agreements on file. Vice Chancellors are responsible for authorizing their subordinate staff to view, add, or modify information located on or supported by VCCS Technology Resources on a need-to-know basis.

Each college president is responsible for ensuring that all VCCS employees working at the college have a signed Information Technology Employee Acceptable Use Agreements on file. Each college president is also responsible for ensuring that active information channels are established that for all active students and patrons using VCCS Technology Resources or the college local computer resources. The information channels must clearly communicate the terms of Information Technology Student/Patron Acceptable Use Agreements. Finally each college president is responsible for establishing approval mechanisms for authorizing staff and students to view, add, or modify local college information located on VCCS Technology Resources on a need-to-know basis.

Requirement: (Review of the information security policy and standard) - §5.1.2

The information security policy and standard should be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

This information security standard is owned by the Chancellor of the Virginia Community College System and that person has approved management responsibility for the development, review, and evaluation of the security policy, standards, guidelines and procedures. The review process which the Chancellor can delegate includes assessing opportunities for improvement of VCCS's information security program and approach to managing information security in response to changes to the VCCS organizational environment, business circumstances, legal conditions, or technical environment.

The review of the VCCS information security program, including the security policy and security standard will occur annually during the first quarter of the calendar year (Jan – Mar) and will include as input, the following items:

- Feedback received from any interested parties;
- Results of independent reviews;
- Status of preventive and corrective;
- Results of previous management reviews;
- Process performance and information security policy compliance;
- Changes that could affect VCCS's approach to managing information security, including changes to VCCS's environment, business circumstances, resource availability, contractual, regulatory, and legal conditions, or to the technical environment;
- Trends related to threats and vulnerabilities;
- Reported information security incidents as output; and
- Recommendations provided by relevant authorities.

A documented record of the management review will be maintained and will reflect any decisions and actions related to:

- Improvement of VCCS's approach to managing information security and its process;
- Improvement of control objectives and controls;
- Improvement in the allocation of resources and/or responsibilities; and
- Will contain management's approval should the security policy or security standard require revision.

REFERENCES

ISO/IEC 27001:2005 Information Technology – Security Techniques – Information Security Management Systems – Requirements, First Edition, dated 2005-10-15

ISO/IEC 27002:2005(E) Information Technology – Security Techniques – Code of Practice for Information Security Management, Second edition, dated 2005-06-15 incorporating corrigendum no. 1

ISO/IEC 27005:2008 Information Technology – Security Techniques – Information Security Risk Management, First Edition, dated 2008-06-15

Additional supporting documentation including more detailed security policies and procedures for specific information systems or security rules and be found at:

http://system.vccs.edu/its/InformationSecurityProgram/

ADEQUACY STANDARD

This standard statement and all supporting standards, models, procedures and guidelines issued in support of the standard shall serve as an adequacy standard and as the foundation for the review of information security safeguards.

Review and Approval:

Reviewed By: CISO, VCCS

Reviewed Date: 01/11/13

Next Scheduled Review: 02/16/14
