

Information Security Standard

Version: 2.0

Status: Approved

Effective Date: 07/01/08

Contact: Director, Technology Administration Services

PUBLICATION DESIGNATION

VCCS Standards Manual. Colleges should prominently display Attachment C, "VCCS Information Technology Acceptable Use Guideline," in computer labs and place in handbooks and catalogs.

SUBJECT

Information Security, IT System Security, Risk Management, IT Contingency Planning, Logical Access Control, Data Protection, Facilities Security, Personnel Security, Threat Management, and IT Asset Management.

AUTHORITY

Authority for this security standard lies in 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, 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; agencies to cooperate; 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.

In addition there are federal laws for violations against federal programs or for inter-network activities. Other specific state and local laws that govern violations that occur in those jurisdictions are in effect. Finally, the VCCS' enforcement of the Standards of Conduct is independent of possible prosecution under the law.

The Virginia Information Technology Agency (VITA) [COV ITRM Standard SEC501-01](#), "Information Technology Security Management Standard" requires that Risk Management, to identify , analyze, prioritize, and mitigate risks that could compromise VCCS systems, and Contingency Planning, to plan for and execute recovery and restoration of VCCS systems and data, processes be established by the VCCS.

The VITA will provide copies of this standard upon request or download the standard from the VITA website at <http://www.vita.virginia.gov/library/default.aspx?id=537#securityPSGs>.

SCOPE

This standard statement applies to all personnel, systems, and facilities maintained, leased or created within the jurisdiction of the VCCS information technology functions, hereafter referred to collectively 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.

This standard further applies to all hardware and software in support of and inclusive of any application or operating system regardless of processing mode, including but not limited to the following:

- Batch, remote, distributed processing, client server, networking, inter-networking and intra-networking;
- System and applications software, data files, program libraries, or special utility programs.

PURPOSE

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. 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.

GENERAL RESPONSIBILITY

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.

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 signed Information Technology Employee Acceptable Use Agreements on file. Each college president is also responsible for ensuring that all active students and patrons using VCCS Technology Resources or the college local computer resources have acknowledged acceptance of the 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.

DEFINITION

The term "VCCS Technology Resources" refers to and includes any and all forms of the data, software, computers, communications networks, and other technology that support the VCCS; the procedures, equipment, facilities, software and data which are designed, built, operated and maintained to collect, record, process, store, retrieve, display and transmit information; data and the processes used to convert this into useful information, the equipment and technology required to use this information and the people involved in making the best use of this information.

Users of the VCCS Technology Resources must agree to comply with and be subject to all applicable [an employee, for instance, would not be subject to the students system security standard policy] VCCS policies. These policies include the Information Security Standard, the VCCS Personnel Security Standard, The Student Information System Security Standard, the Information Technology Employee Acceptable Use Agreement, the Information Technology Student/Patron Acceptable Use Agreement, and the Information Technology Acceptable Use Standard. The VCCS reserves the right to amend these conditions and standards at any time without prior notice.

Academic instruction and research systems, as noted in the SEC501-01 Security Standard, are defined as those systems used by institutions of higher education for the purpose of providing instruction to students or faculty for the purpose of conducting research. For VCCS purposes, this definition includes all desktop computers, notebook computers, computer labs, classrooms, and related infrastructure used by all college faculty and instruction-related personnel responsible for providing direct instructional support to students and faculty. Per SEC501-01, section 1.6c, academic instruction or research systems are explicitly exempt from complying with the SEC501-01 standards. This exemption, however, does not relieve these academic institution or research systems from meeting the requirements of any other state or federal law or act or requirements of VCCS standards, policies, and procedures to which they are subject.

INFORMATION SECURITY OBJECTIVES

The term "VCCS Technology Resources" refers to and includes any and all forms of the data, software, computers, communications networks, and other technology that support the VCCS; the procedures, equipment, facilities, software and data which are designed, built, operated and maintained to collect, record, process, store, retrieve, display and transmit information; data and the processes used to convert this into useful information, the equipment and technology required to use this information and the people involved in making the best use of this information.

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. Access to confidential information is strictly limited and tightly controlled. The objectives of information security are to:

- Ensure the processing of information in a secure environment.
- 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.
- Require compliance with all Commonwealth of Virginia Standards and appropriate federal requirements that relate to the control of and access to the VCCS information and information processing resources.
- Ensure the security of all VCCS electronic communications.
- Protect VCCS information technology assets and provide inventory management controls throughout the assets life cycle.

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.

RELATED LINKS

[Enhanced Security Management for Desktop/Notebook Computers](#)