

# University Information Technology Security Program Standard

**July 2012**

**Version 3.0**

This standard establishes requirements and general principles for initiating, implementing, maintaining, and improving information security management for Virginia Tech. The standard lays out a set of controls that aids in setting objectives on the commonly accepted goals of information security management.

The Virginia Tech policy 7200 [<http://www.policies.vt.edu/index.php>] and this accompanying standard build on standards from the International Organization for Standards (ISO) and the International Electrotechnical Commission (IEC), the organizations that establish standards for a number of information technology areas, including security. Members of ISO and IEC come from all parts of the world and participate in the development and establishment of various standards for the technical community. The ISO/IEC 27002:2005 standard is entitled “Information technology – Security techniques – Code of practice for information security management.” ISO/IEC 27002:2005 contains best practices of control objectives to protect information assets against threats. ISO/IEC 27002:2005 [<http://www.iso.org>] is intended as a common basis and practical guideline for developing organizational security standards and effective security management practices.

This standard treats the following areas, stating what the university must do to protect its information technology resources:

- Risk assessment and treatment
- Security policy
- Organization for security management
- Asset management
- Human resource 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

## Risk Assessment and Treatment

The risk assessment process at Virginia Tech has been effective in helping identify potential risks, and areas that need to have attention. This process benefits both the individual department and the university as a whole by fostering understanding of risks in the information assets environment and how those risks can be reduced or eliminated.

### What the Information Technology organization must do

- Conduct an annual risk assessment
- Provide direction and procedures for information technology risk assessment university-wide  
The Office of Converged Technologies for Security, Safety, and Resilience (CTSSR) website ([www.it.vt.edu/organization/ctssr/risk\\_assessment/](http://www.it.vt.edu/organization/ctssr/risk_assessment/)) contains the information and forms needed to complete an IT risk assessment.
- Review all risk assessments university-wide and retain the documents
- Review industry standards and activities of relevant organizations in order to improve the risk assessment process

### What each university organization must do

- Management commitment and involvement is required, assuring that information from the risk assessment is shared with responsible individuals, and that appropriate actions are taken.
- Conduct a risk assessment at least every three years, as well as when there are major changes in their technology environment, such as relocation or new technology  
**Note:** Departments may find it more convenient to update the assessment annually.
- Send the completed assessment to CTSSR

### Responsibilities of specific university units

Units covered by Policy 7025, Safeguarding Nonpublic Customer Information, including the Office of Scholarships and Financial Aid and the office of the University Bursar must perform a risk assessment process annually.

### Resources

CTSSR is available to assist university departments in understanding the risk assessment process.

Virginia Tech risk assessment process and forms—[www.it.vt.edu/organization/ctssr/risk\\_assessment/](http://www.it.vt.edu/organization/ctssr/risk_assessment/)

OCTAVE<sup>®</sup> (Operationally Critical Threat, Asset, and Vulnerability Evaluation<sup>SM</sup>), a risk-based strategic assessment and planning technique for security available from the Carnegie Mellon Software Engineering Institute [<http://www.cert.org/octave/>]

The National Institute of Standards and Technology [from <http://csrc.nist.gov/index.html>, search for risk assessment]

EDUCAUSE [[www.educause.edu/security/](http://www.educause.edu/security/)]

## Security Policy

Information technology security-related policies provide management direction and support in accordance with business requirements, relevant laws and regulation (at the local, commonwealth, and national levels).

### What the Information Technology organization must do

- Manage university policies, standards, and guidelines dealing with information technology security, including the policy to which this standard pertains, “University Information Technology Security Program” [[www.policies.vt.edu/7200.pdf](http://www.policies.vt.edu/7200.pdf)], a board-approved policy for oversight of information technology security
- Assure that operational procedures are up-to-date and provide appropriate guidance to the university community

### What each university organization must do

- Comply with university policies and standards
- Establish unit procedures to support the compliance of each individual using university data and university resources or connecting to the university network

## Resources

Other university policies and standards impact information technology security and protecting data. The list includes:

- 2010 [Release of Names and Addresses of Students, Faculty, Staff, and Alumni](#)
- 7000 [Acceptable Use of Computer and Communication Systems](#)
- [Acceptable Use Standard](#)
- 7010 [Policy for Securing Technology Resources and Services](#)
- 7025 [Safeguarding Nonpublic Customer Information](#)
- 7030 [Policy on Privacy Statements on Virginia Tech Web Sites](#)
- 7035 [Privacy Policy for Employees' Electronic Communications](#)
- 7040 [Personal Credentials for Enterprise Electronic Services](#)
- 7100 [Administrative Data Management and Access Policy](#)
- 7200 [University IT Security Program](#)
- 7205 [IT Infrastructure, Architecture and Ongoing Operations](#)
- 7210 [IT Project Management](#)
- 7215 [IT Accessibility](#)
- 10100 [Policy for the Purchase of Departmental-Based Computer Systems](#)
- [Security Standards for Social Security Numbers](#)
- [Standard for Protecting Sensitive University Information Used in Digital Form](#)
- [Standard for Securing Web Technology Resources](#)
- [Standard for Storing and Transmitting Personally Identifying Information](#)

## **Management framework for information security**

The organization should have a suitable information technology security structure to provide the services necessary to assist in providing and securing the technology environment.

### **What the Information Technology organization must do**

The Information Technology organization must ensure that sufficient management resources are available to maintain a secure technology environment. Currently, the structures in place include the Information Technology Security Office, the Office of Converged Technologies for Security, Safety, and Resilience, and the Secure Enterprise Technology Initiatives organization.

#### **Information Technology Security Office**

The Information Technology Security Office (IT Security Office) was established in 1998 to ensure proper directions for technology security are being taken by areas within the institution. The office provides technology tools and services, education, awareness, and guidance necessary for Virginia Tech to work towards a safe and secure information technology environment. The office is also responsible for the IT Security Lab. [<http://security.vt.edu>]

#### **Converged Technologies for Security, Safety, and Resilience**

Converged Technologies for Security, Safety and Resilience coordinates, integrates, and develops advancements that involve the intersection of information technology security and physical security activities, campus safety, and community/ regional resilience. The office is the primary liaison with the campus police and emergency management organizations, and coordinates continuity of operations plans and a business recovery plan for Information Technology. The office is also responsible for the Identity Management Services office. [[www.it.vt.edu/organization/ctssr/](http://www.it.vt.edu/organization/ctssr/)]

#### **Secure Enterprise Technology Initiatives**

The Secure Enterprise Technology Initiatives (SETI) group develops secure applications, middleware, and interfaces to support the university's computing and network services [[www.seti.it.vt.edu](http://www.seti.it.vt.edu)]. The department works in conjunction with the IT Security Office to enforce auditable security standards that address privacy issues while providing a balance between system usability and system security. SETI research and development initiatives exploit leading edge, innovative technologies to enhance the ability of Virginia Tech affiliates to interact securely with new and existing computing and networking services.

Other areas within the Information Technology organization that provide assistance in making sure we maintain a secure technology environment include the following:

#### **Information Technology Acquisitions**

Information Technology Acquisitions (ITA), the point of contact for purchases of information technology including vendors of hardware, software, and services, oversees the contractual relationships that ensure

that external parties providing information processing capabilities are secure and hold the university's information securely, with appropriate controls. [<http://www.policies.vt.edu/3015.pdf>; <http://www.ita.vt.edu>].

### **Network Infrastructure and Services**

Network Infrastructure and Services reviews contracts for the purchase of network equipment, including a review of security.

### **What each university organization must do**

- Assign each technology resource to an accountable individual who is responsible for ensuring the continued security of that resource. [[www.policies.vt.edu/7010.pdf](http://www.policies.vt.edu/7010.pdf)].
- Ensure that employees who are responsible for technology resources have opportunities for awareness and training in information technology security, as appropriate to their responsibilities.
- Maintain up-to-date network liaisons to Network Infrastructure and Services.

### **Resources:**

IT Security Office [www.security.vt.edu](http://www.security.vt.edu)

Secure Enterprise Technology Initiatives [www.seti.it.vt.edu](http://www.seti.it.vt.edu)

Information Technology Acquisitions [www.ita.vt.edu](http://www.ita.vt.edu)

[Converged Technologies for Security, Safety, and Resilience www.it.vt.edu/organization/ctssr/](http://www.it.vt.edu/organization/ctssr/)

## **Asset Management**

The university must ensure appropriate management and protection of organizational assets. Both fixed assets and information technology assets must be handled appropriately in the areas of inventories, management and disposal.

*All university personnel* who use university data are responsible for protecting their access privileges and for proper use of the university data they access.

The Fixed Assets and Equipment Inventory Services (FAEIS) section of the Controller's Office is responsible for maintaining and managing the university's official fixed asset system. FAEIS strives to ensure the university's assets are properly acquired, safeguarded, controlled, recorded and disposed in accordance with state and federal regulations, audit requirements, and applicable accounting pronouncements [ [http://www.co.vt.edu/financial\\_reporting/fixed\\_assets/index.html](http://www.co.vt.edu/financial_reporting/fixed_assets/index.html)].

### **What the Information Technology organization must do**

- Maintain an accurate record of the fixed assets for which it is responsible that can be reviewed by FAEIS on a regular basis
- Publish and maintain acceptable procedures for disposal of devices containing data and software
- Convene and coordinate a university-wide group that reviews data management practice
- Consider and implement necessary security controls for data

### **What each university organization must do**

- Maintain an accurate record of the fixed assets for which it is responsible that can be reviewed by FAEIS on a regular basis
- Ensure that data and software have been appropriately cleaned from devices when they leave their control for transfer or surplus

### **Responsibilities of specific university units or roles**

Data stewards must define and document procedures for requesting and authorizing access to limited-access data elements, must monitor and periodically review security implementation and authorized access; and must define and implement procedures that assure data are backed up and recoverable in response to events that compromise data integrity.

### **Resources**

Fixed Asset Accounting [www.policies.vt.edu/3950.pdf](http://www.policies.vt.edu/3950.pdf)

Transfer of Equipment [www.policies.vt.edu/3951.pdf](http://www.policies.vt.edu/3951.pdf)

Management of Surplus Material [www.policies.vt.edu/3955.pdf](http://www.policies.vt.edu/3955.pdf)

Administrative Data Management and Access Policy [www.policies.vt.edu/7100.pdf](http://www.policies.vt.edu/7100.pdf)

Standard for Administrative Data Management

[www.it.vt.edu/publications/pdf/Administrative\\_data\\_management\\_standard\\_2011-March-23.pdf](http://www.it.vt.edu/publications/pdf/Administrative_data_management_standard_2011-March-23.pdf)

Safeguarding Nonpublic Customer Information [www.policies.vt.edu/7025.pdf](http://www.policies.vt.edu/7025.pdf)

## Human Resource Security

Upon employment or enrollment at Virginia Tech, individuals must understand their responsibilities when using technology resources that belong to the institution. Training must be provided, building on policies, procedures, and guidelines, so that individuals can understand their responsibilities, possible threats and concerns, and actions that can be taken.

The IT Security Office works with Human Resources, the admissions offices, New Student Orientation, and related areas to ensure that training on information technology security is a part of the initial awareness of every newcomer to the university community.

*All individuals using university information technology resources* must comply with the Acceptable Use Standard.

### What the Information Technology organization must do

- Make training and security discussions available to university units
- Provide information technology security updates to Faculty Development Institute track sessions
- Host a workshop for technical support personnel across the university that includes updates and reminders on security
- Work with university departments to provide the necessary specialized training for their areas (for example, Gramm-Leach-Bliley, HIPAA, and FERPA)
- Maintain a security website to provide all users with a source of information that can help keep an individual and their resources safe

### What each university organization must do

- Encourage individual staff and faculty members to attend security awareness training and to stay familiar with the latest threats

### Responsibilities of specific university units and roles

University offices with data responsibilities for regulated data provide training to personnel need that data (Gramm-Leach-Bliley, HIPAA, FERPA).

### Resources

Acceptable Use Policy <http://www.policies.vt.edu/7000.pdf>

Acceptable Use Standard <http://www.vt.edu/about/acceptable-use.html>

Security web site [http://security.vt.edu/Reading\\_gateway.html](http://security.vt.edu/Reading_gateway.html) and look under the Go To Class section.

Faculty Development Institute <http://www.fdi.vt.edu/>

Catalog of Information Technology Services [www.computing.vt.edu](http://www.computing.vt.edu)



## **Physical and Environmental Security**

Secure areas are necessary to prevent unauthorized physical access, damage, and interference to the organization's premises and information.

### **What the Information Technology organization must do**

- Ensure the physical security of the Data Center, including the following measures:
  - Receptionists who act as gatekeepers to visitors during business hours
  - Controlled access, including use of biometrics at entrances not personally monitored
  - Security presence during non-business hours
  - Monitoring of entrances by a security camera system
  - A fire suppression system that meets or exceeds required fire codes
  - An environmental monitoring system that manages temperature and humidity requirements
- Ensure physical security of other information technology resource locations under the control of the organization

### **What each university organization must do**

- Ensure the physical security of assets under their control, in a manner congruent with the risks to those assets

## **Resources**

A confidential document is maintained by individuals with Information Technology responsible for facility management, and can be made available on request.

Departments can consider contracting with Information Technology to move critical assets into the protected setting of the Data Center.

## Communications and Operations Management

Operational procedures and responsibilities need to be defined to ensure the correct and secure operation of information processing facilities and services. These definitions apply not only to the physical structures but also to areas such as development/maintenance of systems, protection for the integrity of software and information, and backup procedures.

### What the Information Technology organization must do

**Note:** The disaster recovery plans prepared and maintained by Network Infrastructure and Services and CTSSR contain the instructions for timely restoration of operations. These documents contain sensitive information and are only available to authorized personnel.

- Separate production and operations in development and testing work done by Information Technology
- Maintain and update resources for the university community to protect against malicious code, including the website [www.antivirus.vt.edu](http://www.antivirus.vt.edu)
- Maintain and update resources for the university community to protect against threats to email (See E-mail and Calendaring on [www.computing.vt.edu](http://www.computing.vt.edu).)
- Ensure that email is filtered against known viruses using tested and effective mechanisms
- Ensure that production systems managed by Information Technology are backed up on a daily basis and that backups stored off-site

### What each university organization must do

- Maintain disaster recovery plans for locally managed, critical production systems
- Backup locally managed critical production systems
- Employ the proper separation of duties to ensure the integrity of systems and the data they record and maintain
- Use provided antivirus software or equivalent to add extra protection

### Resources

Computing website [www.computing.vt.edu](http://www.computing.vt.edu)

Security web site [www.security.vt.edu](http://www.security.vt.edu)

Converged Technologies for Security, Safety, and Resilience [www.it.vt.edu/organization/ctssr/](http://www.it.vt.edu/organization/ctssr/)

Program Development or Modification Procedure, a document available for development groups within Information Technology

Department Business Management Guide [www.cafm.vt.edu](http://www.cafm.vt.edu)

Information Technology's backup service

[http://computing.vt.edu/security\\_and\\_viruses/network\\_backup/](http://computing.vt.edu/security_and_viruses/network_backup/)

## Access Control

Access to information and business processes must be controlled on the basis of business and security requirements.

*All individuals* must abide by the Acceptable Use Standard, and must manage passwords and/or pass phrases to meet or surpass minimum standards for passwords.

### What the Information Technology organization must do

- Oversee the issuing of enterprise credentials for online access, including the PID or basic identifier, Oracle (Banner) IDs, personal digital certificates under the authority of the Virginia Tech Certificate Authority, Active Directory IDs (Hokies), network access IDs, and email credentials
- Maintains minimum standards for passwords or passphrases for access to university systems

### What each university organization must do

- Use appropriate access controls for systems managed by the organization, with preference to enterprise-level credentials (e.g., PIDs, PDCs, Hokies IDs, Banner IDs)
- Manage any locally issued credentials in ways that either synchronized with centrally managed IDs or that will not be confused with enterprise, centrally managed IDs

## Resources

Acceptable Use Policy <http://www.policies.vt.edu/7000.pdf>

Acceptable Use Standard <http://www.policies.vt.edu/acceptableuse.php>

Account information [http://www.computing.vt.edu/accounts\\_and\\_access/pid/index.html](http://www.computing.vt.edu/accounts_and_access/pid/index.html)

Tutorial for students [http://www.computing.vt.edu/help\\_and\\_tutorials/getting\\_started/students.html](http://www.computing.vt.edu/help_and_tutorials/getting_started/students.html)

Tutorial for faculty/staff: Banner access

[http://www.computing.vt.edu/administrative\\_systems/banner/index.html](http://www.computing.vt.edu/administrative_systems/banner/index.html)

Good passwords [http://www.computing.vt.edu/accounts\\_and\\_access/pickinggoodpasswords.html](http://www.computing.vt.edu/accounts_and_access/pickinggoodpasswords.html)

## **Information Systems Acquisition, Development, and Maintenance**

The security requirements for a system are important to ensure that security is an integral part of information systems, whether purchased or developed within the university. Purchased services using university data must likewise be secure.

### **What the Information Technology organization must do**

- Process requisitions for computer equipment, software, maintenance, and service (Office of Computer Purchasing)
- When developing or enhancing software, meet security standards and undertake security testing

### **What each university organization must do**

- Follow published procurement procedures and standards
- When developing or enhancing software that uses university data or connects to the university network, meet security standards and arrange for security testing by the IT Security Office

### **Resources**

Computer Purchasing [www.ita.vt.edu/purchasing.html](http://www.ita.vt.edu/purchasing.html)

University Purchasing Office [www.purch.vt.edu/](http://www.purch.vt.edu/)

Standard for the Procurement of Information Technology Applications

[www.it.vt.edu/publications/pdf/Procurement\\_STANDARD\\_signed\\_1-19-11.pdf](http://www.it.vt.edu/publications/pdf/Procurement_STANDARD_signed_1-19-11.pdf)

## Information Security Incident Management

Evaluating and reporting security incidents is important to ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

*All individuals* who suspect an exposure of university data should call 540-231-HELP immediately.

### What the Information Technology organization must do

- Maintain an incident response procedure document
- Maintain the Computer Incident Response Team to carry out these procedures

**Note:** The document contains confidential information and is available to authorized personnel only.

- Arrange for intake of reports of suspected exposure of university data and other suspect incidents; specifically, through phoning 540-231-HELP, using the Web form [www.4help.vt.edu](http://www.4help.vt.edu), or emailing [abuse@vt.edu](mailto:abuse@vt.edu)

### What each university organization must do

- Handle incidents that are small and confined to local systems in a timely manner
- Promptly report larger or more complex incidents to 4help

### Resources

Security website <http://security.vt.edu>

Computing Support Center [http://www.computing.vt.edu/help\\_and\\_tutorials/4help/index.html](http://www.computing.vt.edu/help_and_tutorials/4help/index.html)

IT Security Lab [http://www.security.vt.edu/IT%20Security/security\\_lab.html](http://www.security.vt.edu/IT%20Security/security_lab.html)

## **Business Continuity Planning**

Business continuity plans help departments to counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

### **What the Information Technology organization must do**

- Periodically review and maintain plans to ensure operations can be recovered and operational within a stated time

### **What each university organization must do**

- Work with Emergency Management and other relevant university units to ensure that emergency plans are appropriate and up-to-date

## **Resources**

Emergency Management [www.emergency.vt.edu/](http://www.emergency.vt.edu/)

Security website--Play It Safe [http://www.security.vt.edu/Reading\\_gateway.html](http://www.security.vt.edu/Reading_gateway.html)

## Compliance

Legal requirements necessitate Virginia Tech to ascertain compliances to avoid breaches of law, statutory, regulatory, or contractual obligations, and of security requirements.

### What the Information Technology organization must do

- Provide training and awareness resources, including presentations offered upon request
- Provide security reviews upon request, and as scheduled based upon risk
- Conduct vulnerability assessments and penetration testing

### What each university organization must do

- Ensure that unit personnel who access university data have periodic training on the security requirements for the data they handle, whether in computing systems or in paper files

## Resources

Security website ([http://security.vt.edu/resources\\_and\\_information/index.html](http://security.vt.edu/resources_and_information/index.html)), where references to several sites provide more details on compliance issues:

- FERPA— individuals access to their academic record, as well as third party access and the appropriate security of the education record
- HIPAA— privacy protection for health records
- G-L-B— the security and confidentiality of customer nonpublic financial information records
- PCI— Payment Card Industry (PCI) Data Security Standard for credit card usage
- SOX— Sarbanes-Oxley Act dealing with financial applications
- Patriot Act— gives the federal government the ability to investigate threats to the national security
- Copyright laws—legal right to exclusive publication, production, sale, or distribution of literary, musical or artistic work
- Additional Federal and State regulations—dealing with day-to-day activities from purchasing items to personnel issues to reporting structures to what's legal to access

**Revision July 2012**

Moved risk assessment from the Information Technology Security Office to Converged Technology for Security, Safety, and Resilience; additional editorial updates

Approved by Earving L. Blythe, Vice President for Information Technology and Chief Information Officer

(Signed) \_\_\_\_\_