Information Security

Policy Type: Administrative
Responsible Office: Office of Technology Services, Office of the Vice President of Administration
Initial Policy Approved: 09/30/2009
Current Revision Approved: 09/27/2018

Policy Statement and Purpose

Information technology enables more accurate, reliable, and faster information processing with information more readily available to administration, faculty, staff, and students. However, information technology has also brought new administrative concerns, challenges, and responsibilities. Information assets must be protected from natural, technological and human hazards. Policies and practices must be established to ensure that hazards are reduced or their effects minimized.

The focus of information security is ensuring reasonable and proportionate protection of information and continuation of program operations. Providing efficient accessibility to necessary information is the impetus for establishing and maintaining information systems.

This policy sets forth the elements of VCU's Information Security Program, including its associated information classification and protection requirements, and the procedure for reporting, investigating and resolving suspected violations. This policy is part of VCU's Information Technology Policy Framework referenced in the Related Documents section. The information technology standards and baselines associated with this policy that are included in the Information Technology Policy Framework must be followed in conjunction with this policy. Information technology guidelines are also included in the framework as recommendations and best practices.

Noncompliance with this policy may result in disciplinary action up to and including termination. VCU supports an environment free from retaliation. Retaliation against any employee who brings forth a good faith concern, asks a clarifying question, or participates in an investigation is prohibited.

Table of Contents

Who Should Know This Policy

All employees, contractors, students and affiliates who generates, processes, transmits, stores or accesses VCU information are responsible for knowing this policy and familiarizing themselves with its contents and provisions.

Definitions

Information Technology Baseline
An information technology baseline is a set of technical requirements that define the minimum required standard practices. Information technology baselines are used in conjunction with information technology standards and policies.

Information Technology Guideline
An information technology guideline is a recommended practice that allows some discretion or leeway in its interpretation, implementation, or use.

Information Technology Standard
An information technology standard is a formal document for an established norm of methods, criteria, and processes for technology subjects.

Organizational Unit
Within the context of this document, an organizational unit is a school, a department, or division that reports directly to a vice president. Examples of organizational units include School of Engineering, College of Humanities and Sciences, School of Medicine, Office of Technology Services, Enrollment Services, and Facilities Management.

Payment Card Industry Data Security Standard (PCI-DSS)
Payment Card Industry Data Security Standard is a set of comprehensive requirements for enhancing payment card data security. Compliance with the PCI-DSS helps to alleviate vulnerabilities that put cardholder data at risk.

Server
Within the context of this document a server refers to a computer system or a collection of computer systems designed to provide services that process, store, or transmit data and information for one or multiple clients; where the client maybe other computer systems or programs that are used by individual

users. A server may be hosted by VCU inside of its networks, or hosted by a third party on the Internet or other external networks. Examples include file, print, Web, application and database servers.

Unit Head
A unit head is the administrative employee responsible for the operations of an organizational unit. A unit head can be a dean of a school or the director of a department or division.

VCU Information
Information in paper, electronic or oral form that is collected, generated, transmitted, processed or stored by a VCU employee, consultant, contractor or other affiliate in the course of their work and is used to support the academic, research, patient care or administrative operations in VCU.

Contacts

VCU Office of Technology Services officially interprets this policy. VCU Office of Technology Services is responsible for obtaining approval for any revisions as required by the policy *Creating and Maintaining Policies and Procedures* through the appropriate governance structures. Please direct policy questions to the Office of Technology Services, Information Security Office at infosec@vcu.edu.

Policy Specifics and Procedures

Information Security Program
Based on sensitivity and risk, the VCU Information Security Program is established to protect VCU information and information assets, which includes, but is not limited to:

- Physical protection of information processing facilities and equipment.
- Maintenance of application and data integrity.
- Assurance that information systems perform their critical functions correctly, in a timely manner, and under adequate controls.
- Protection against unauthorized access to information, information systems and protection against unauthorized disclosure of information.
- Assurance of the continued availability of reliable and critical information.

The VCU Information Security Program addresses information security from three distinct perspectives:

1. **Information Confidentiality**: Certain information that is collected, generated, processed, transmitted or stored by university academic, research, patient care and administrative operations is protected by various industry and legal regulations, such as FERPA, HIPAA, Code of VA, and PCI-DSS among others**.** Information protected under such regulations must be kept confidential and protected from unauthorized disclosure and access. Failure to protect this information can result in legal, financial and reputational damage to the university and our own selves.

2. **Information Integrity**: Information entered, processed, stored, generated, or disseminated by information systems must be protected from internal data or programming errors and from misuse by individuals inside or outside of VCU. Specifically, the information must be protected from unauthorized or accidental modification, destruction, or disclosure. Otherwise, the university risks compromising the integrity of VCU programs, violating individual rights to privacy, violating copyrights, triggering financial and reputational damage to the university, or facing criminal or civil penalties.

3. **Information Availability**: Many academic, research, patient care and administrative operations within the university are fully dependent upon the availability of information technology services to perform and support their daily functions. The interruptions, disruption, or loss of information technology services may adversely affect VCU's ability to administer programs and provide services. The effects of such risks must be minimized.

Information Classification and Protection

In order to successfully implement the Information Security Program, VCU must classify its information based on sensitivity and risk. VCU must then apply reasonable and proportionate security protection to safeguard the confidentiality, integrity and availability of this information.

- **Each organizational unit** in VCU is responsible for the classification of the VCU information managed by the unit according to sensitivity and risk. Classification of information must follow the requirements delineated in the VCU *Data Classification Standard*.

- **The unit head of each organizational unit** is responsible for the confidentiality and integrity of VCU information managed by the unit.

- **All individuals** who handle or store VCU information are required to:

  - Follow all applicable laws, regulations, policies, including but not limited to the VCU Information Technology Standards and any associated procedures and baselines when generating, accessing, processing, transmitting, storing and deleting VCU information.

  - Follow reasonable and proportionate care to safeguard such information from any misuse, loss or theft, including but not limited to unauthorized access, modification and deletion.

  - Exercise reasonable and proportionate care to ensure the accuracy, completeness, and integrity of such information.

  - Report any observed misuse, loss or theft of such information or assets containing such information to the VCU Information Security Office in a prompt manner and without unreasonable delay.

Reporting, investigation and resolution of violations
Anyone who suspects a violation of this policy is expected to report the suspected violation to the office or department where the suspected violation occurs; to the VCU [Compliance] Helpline; or to the Chief Information Officer in accordance with the VCU *Duty to Report* and the *Computer and Network Resources Use* policies.

All violations of this *Information Security* policy are subject to the same investigation and resolution procedures documented in the *Computer and Network Resources Use* policy.

Request for Exception
All requests for exception(s) to this policy are evaluated by the Information Security Office on a case-by-case basis. Exception requests should be made using the Information Security Exception Request Form. The completed exception request form is automatically emailed the unit head listed in the request. After the unit head approves the request, the Information Security Office will provide the secondary review and approval as appropriate. Evaluation criteria for exception include the requirement to which an exception is requested, the sensitivity of the information affected, compensating controls in place to mitigate additional risks, and business processes affected by the exception. The Information Security Office will send the exception request review decision and any additional correspondence to the requestor's and the unit head's email addresses.

Forms

1. Information Security Exception Request Form

Related Documents

The VCU Information Technology Policy Framework contains VCU Information Technology policies, standards and baseline requirements, all of which must be followed in conjunction with this policy. The framework also includes information technology guidelines as recommendations and best practices. The standards, policies and other documents specifically discussed in this policy are listed below.

1. VCU Information Technology Policy Framework
2. VCU Data Classification Standard
3. VCU Data Classification Tool
4. VCU Data Management System
5. VCU Information Security Office Homepage
6. VCU Information Technology Standards
7. Family Educational Rights and Privacy Act (FERPA) https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

8. Health Insurance Portability and Accountability Act (HIPAA) https://www.hhs.gov/hipaa/index.html
9. Code of Virginia https://law.lis.virginia.gov/vacode
10. VCU Policy: *Duty to Report and Protection from Retaliation*
11. VCU Policy: *Computer and Network Resources Use*

Revision History

This policy supersedes the following archived policies:

Approval/Revision Date	*Title*
9/30/2009	*Information Security Policy*
8/10/2015	*Information Security Policy*
1/19/2017	*Information Security* (minor revision to note that VCU's Information Technology Policy Framework encompasses this policy)

FAQ

1. I am not an employee of VCU, does this policy still apply to me?

The VCU Information Security Policy and associated information technology standards apply to VCU information. Therefore, any personnel who handle VCU information must read, understand and abide by the information security policies and standards.

2. In addition to VCU's Data Classification Standard, are there any other resources available to help me classify information and understand the expectations for handling each type of sensitive information?

Yes. VCU provides an interactive Data Classification Tool that can be used by individuals to understand the sensitivity of specific datasets. Additionally, VCU's Data Management System is designed to provide VCU personnel with guidance on the handling, transmission and storage of information, including specific requirements related to the handling of various types of information, IT resources and services offered by the university that can assist in handling of such information, and specific precautions one should take in handling various types of information. Links to both tools are provided in the "Related Documents" section above, and they can both be found within the VCU Information Security Office website at https://go.vcu.edu/infosec.

3. How do I report a suspected security incident or a violation of this policy?

For possible security incidents such as an email scam, possible hacking, or a lost / stolen device containing sensitive data, you may report the incident directly through the links on the home page of the VCU Information Security Office website (https://go.vcu.edu/infosec). For potential policy violation, aside from the aforementioned reporting links on the VCU Information Security Office homepage, you may report to the VCU Helpline.