Purpose

Virginia State University (VSU) uses information to perform the business services and functions necessary to fulfill its mission. VSU information is contained in many different mediums including paper, electronic records, voice mail, and the spoken word. The University's Information Security (IS) program is built on the concept of trust and the program provides a sustainable consistent approach to information safeguards that can be replicated across paper and electronic files, systems and transactions. The IS program provides the framework and practices for all business functions, departments, faculty, staff, and students to use in securing their information. The IS program is also designed to provide direction and assistance for developing and implementing information security controls that reduce the risk to VSU information regardless of the medium containing the information.

Rapid and continuing technical advances have increased the dependence of VSU on various security measures to protect University electronic information. This policy establishes the VSU IS Program as a comprehensive framework for developing University security programs that protect its information.

Authority, Responsibility, and Duties

These IT Security Program roles and responsibilities are assigned to individuals, and may differ from the actual role title or working title of the individual's position. Individuals may be assigned multiple roles, as long as the multiple role assignments provide adequate separation of duties, provide adequate protection against the possibility of fraud, and do not lead to a conflict of interests. See Exhibit A, "Reporting Relations to Technology Services".

A. Chief Information Officer (CIO) of the Commonwealth of Virginia (COV)

The Code of Virginia §2.2-2009 states that *"the CIO shall direct the development of policies, procedures and standards for assessing security risks, determining the appropriate security measures and pe1jonning security audits of government electronic information."*

B. COV Chief Information Security Officer (CISO)

The COV CISO is responsible for development and coordination of the COV Information Security Program and, as such, performs the following duties:

1. Administers the COV Information Security Program and periodically assesses whether the program is implemented in accordance with COV Information Security Policies and Standards.
2. Reviews requested exceptions to COV Information Security Policies, Standards, and Procedures.
3. Provides solutions, guidance, and expertise in IT security.
4. Maintains awareness of the security status of sensitive IT systems.

5. Facilitates effective implementation of the COV Information Security Program by:
   a. Preparing, disseminating, and maintaining information security, policies, standards, guidelines and procedures as appropriate;
   b. Collecting data relative to the state of IT security in the COV and communicating as needed; and
   c. Providing consultation on balancing an effective information security program with business needs.
6. Provides networking and liaison opportunities to Information Security Officers (ISOs).

C. Virginia State University President

The University President or his designee is responsible for the security of the University's information systems and data. The University President information security responsibilities include the following:

1. Designate an Information Security Officer (ISO) upon the recommendation of the Chief of Staff for the University, no less than biennially.
2. Approve or disapprove the University Business Impact Analyses (BIAs), Risk Assessments (RAs), Continuity of Operations Plan (COOP), and Information Technology (IT) Disaster Recovery Plan.

D. VSU Chief Information Officer CIO)

The CIO manages and oversees the day-to-day efforts of the Technology Services' unit in support of the mission to promote and deliver reliable information technology (IT) solutions and services to support the educational mission of Virginia State University. CIO is also responsible for notifying and fully disclosing to senior management IT security risks and vulnerabilities impacting information technology solutions. The CIO should:

1. Review and approve the University BIAs, RAs, COOP, and IT Disaster Recovery Plan.
2. Approve System Security Plans that provide adequate protections against security risks; or
3. Disapprove System Security Plans that do not provide adequate protections against security risks, and require that the System Owner implement additional security controls on the information system to provide adequate protections against security risks.
4. Review and approve the IT Security Audit Plan and Corrective Action Plan to address findings of IT Security audits.
5. Maintain liaison with the COV CISO.

E. VSU Deputy CIO

The Deputy CIO is responsible for IT Operations, Web Services, Application Services, Enterprise Architecture, Data Center management and systems maintenance, reviewing the System Security Plans for all University information systems classified as sensitive and is responsible for IT Operations Governance by implementing Information Security policies and procedures within the technology environment, and for ensuring compliance to VITA Information Security Standard. The Deputy CIO should:

1. Review the University BIAs and COOP.
2. Contribute to and approve the RAs and COOP.
3. Prepare IT Disaster Recovery Plan.
4. Prepare System Security Plans for all sensitive systems that provide adequate protections against security risks for other sensitive system and recommend for approval; or
5. Disapprove System Security Plans that do not provide adequate protections against security risks, and recommend that the System Owner implement additional security controls on the information system to provide adequate protections against security risks.

F. VSU Information Security Officer (ISO)

The ISO is responsible for developing and managing the University's information security program. The ISO's duties are as follows:

1. Develop and manage a University information security program that meets or exceeds the requirements of VSU information security policies and standards in a manner commensurate with risk.
2. Verify and validate that all University systems and data are classified for sensitivity.
3. Develop and maintain an information security awareness and training program for University staff, including contractors and IT service providers. Require that all information system users complete required information security awareness and training activities prior to, or as soon as practicable after, receiving access to any system, and no less than annually, thereafter. Escalate to management any University staff member who has not successfully completed the information security awareness training courses(s).
4. Implement and maintain the appropriate balance of preventative, detective and corrective controls for University systems commensurate with data sensitivity, risk and systems criticality.
5. Mitigate and report all information security incidents in accordance with §2.2-603 of the Code of Virginia and VITA requirements and take appropriate actions to prevent recurrence.
6. Ensure compliance is maintained with the current version of the VITA *IT Security Audit Standard* (COV ITRM Standard SEC502). This compliance must include, but is not limited to:
    a. Requiring development and implementation of an university plan for IT security audits, and submitting this plan to the Chief of Staff and CIO for review and approval;
    b. Requiring that the planned IT security audits are conducted;
    c. Receiving reports of the results of IT security audits;
    d. Requiring development of Corrective Action Plans to address findings of IT security audits; and
    e. Reporting to the Chief of Staff all IT security audit findings and progress in implementing corrective actions in response to IT security audit findings.
7. Prepare and draft the annual VITA IT Security Audit plan to the Chief of Staff, Deputy CIO and CIO for review and approval.
8. Ensure that designee prevents conflict of interests and adhere to the security concept of separation of duties by assigning roles so that:

a. The ISO is not a System Owner or a Data Owner except in case of compliance systems for information security;
b. The System Owner and the Data Owner are not system Administrators for information systems or data they own; and
c. The ISO, Systems Owners, and Data Owners are VSU employees.

9. Review, and approve System Security Plans that provide adequate protections against security risks; or
10. Disapprove System Security Plans that do not provide adequate protections against security risks, and recommend that the System Owner implement additional security controls on the information system to provide adequate protections against security risks.
II. Maintain liaison with the COV CISO.

G. Privacy Officer

The University Human Resources, Student Health Services, the University Registrar, and other departments will manage and ensure the privacy of information in their respective areas. They will coordinate their efforts with the VSU ISO who, in accordance with the current VITA Information Security Standard, has responsibility to provide guidance on:

I. The requirements of state and federal Privacy laws.
2. Disclosure of and access to sensitive data.
3. Security and protection requirements in conjunction with information systems when there is some overlap among sensitivity, disclosure, privacy, and security issues.

H. System Owner

The System Owner is the University business manager responsible for having an information system operated and maintained, in support of the (essential) business functions for which the business manager is accountable. With respect to information security, the System Owner's responsibilities include the following:

I. Require that the information system users complete any system unique security training prior to, or as soon as practicable after, receiving access to the system, and no less than annually, thereafter.
2. Manage system risk and developing any additional information security policies and procedures required to protect the system in a manner commensurate with risk.
3. Maintain compliance with VSU Information Security policies and standards in all information system activities.
4. Maintain compliance with requirements specified by Data Owners for the handling of data processed by the system.
5. In collaboration with the Deputy CIO or Data Center Manager designate a System Administrator for the system.

I. Data Owner

The Data Owner is the University manager responsible for the policy and practice decisions regarding data, and is responsible for the following:

I. Evaluate and classify sensitivity of the data.
2. Define protection requirements for the data based on the sensitivity of the data, any legal or regulatory requirements, and business needs.
3. Communicate data protection requirements to the System Owner.
4. Define requirements for access to the data.

J. System Administrator

The System Administrator is an analyst, engineer, or consultant who implements, manages, and/or operates a system or systems at the direction of the System Owner, Data Owner, and/or Data Custodian. The System Administrator assists University management in the day-to-day administration of University information systems, and implements security controls and other requirements of the University information security program on information systems for which the System Administrator has been assigned responsibility.

K. Data Custodian

Data Custodians are individuals or organizations in physical or logical possession of data for Data Owners. Data Custodians are responsible for the following:

I. Protecting the data in their possession from unauthorized access, alteration, destruction, **or usage.**
2. Establishing, monitoring, and operating information systems in a manner consistent with VSU Information Security policies and standards.
3. Providing Data Owners with reports, when necessary and applicable.

L. IT System Users

All IT system users of VSU information systems, including all University employees (permanent, temporary, contractual, faculty, administrators and students) are responsible for the following:

I. Reading and complying with University information security program requirements, policies, and procedures.
2. Reporting data breaches of information security, actual or suspected, to their University management, Technology Services Help Desk, and/or the VSU ISO.
3. Taking reasonable and prudent steps to protect the security of information systems and data to which they have access.
4. Completing the annual IT Security Awareness training courses.
5. Reading and complying with the University's Acceptable User policy and Acceptable Use User agreement in the University's IT Security Awareness training portal.
6. Report all lost or stolen IT assets to the ISO, IT Help Desk, Department of Police and Public Safety (DPPS) and the Director of IT Services.

Definitions

The IT security definitions and terms can be found in the Commonwealth of Virginia (COV) Information Technology Resource Management (ITRM) Glossary. It is referenced on the ITRM Policies, Standards, and Guidelines web page on www.vita.virginia.gov/librarv.

Policy Statement

This policy applies to all University employees (permanent, temporary, contractual, faculty, administrators, and students) who are responsible for the development, coordination, and execution of the University's Information Security program.

A. Exceptions to Security Requirements

If System Owner (the requesting party) determines that compliance with the provisions of this policy or any related information security policy would adversely impact a business process of the agency, the System Owner may request approval to deviate from a specific requirement by submitting an exception request to the VSU ISO. For each exception, the requesting System Owner shall fully document:

1. The business need,
2. The scope and extent,
3. Mitigating safeguards,
4. Residual risks, and
5. The specific duration.

Each request shall be in writing to the VSU ISO and approved by the VSU CIO indicating the acceptance of the defined residual risks. Included in each request shall be a statement detailing the reasons for the exception as well as mitigating controls and all residual risks. The requesting System Owner will be informed of the action taken. An exception will not be accepted for processing unless all residual risks have been documented. Denied exceptions may be appealed to the CIO of VSU. The form to document exceptions requests is included in Exhibit B of this document.

Once the exception request is approved by the VSU CIO, the request is then submitted to the President of VSU for signature and submitted to VITA Commonwealth Security and Risk Management for final approval by the COV CISO.

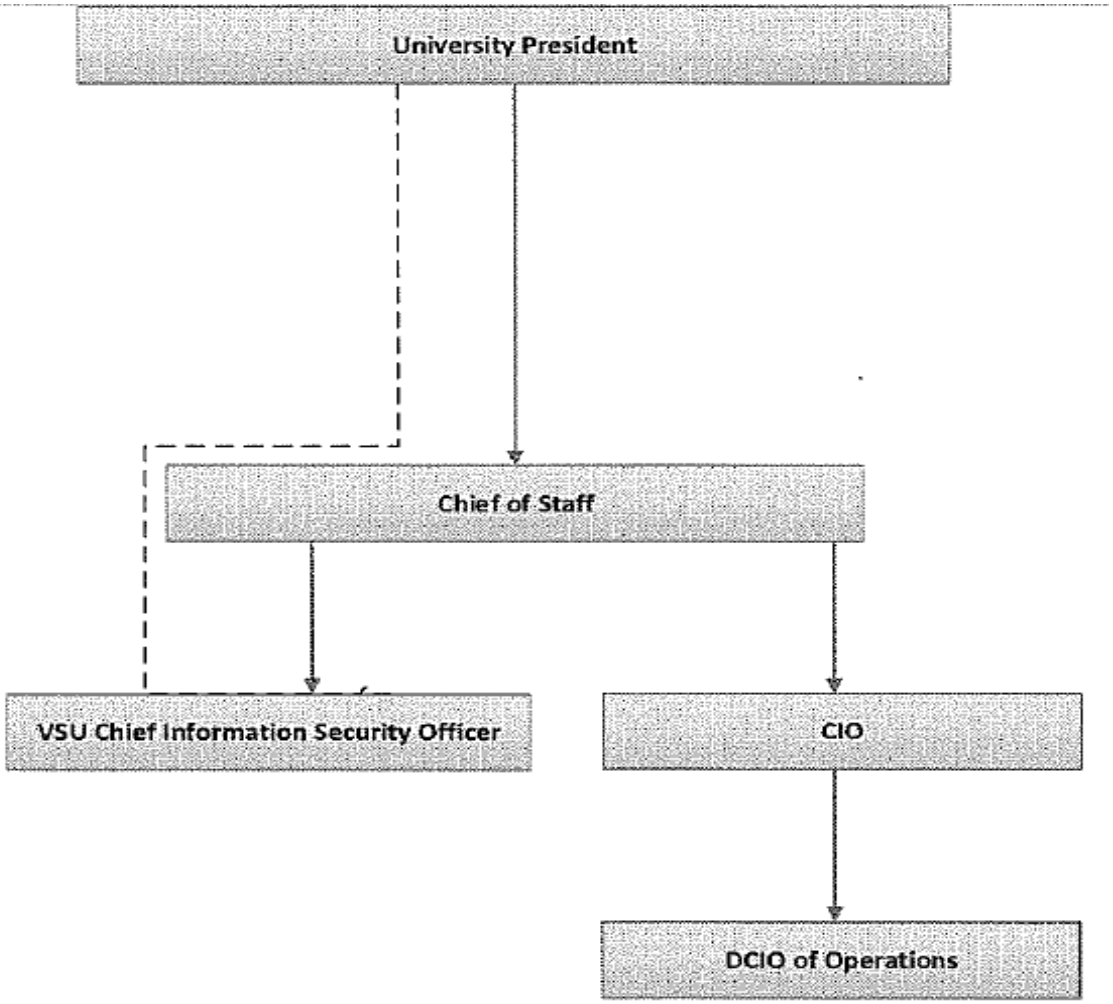
References

Virginia Information Technology Agency (VITA):
Information Security Standard (SEC 501-09) (02/20/2015)

Virginia Information Technology Agency (VITA):
IT Security Audit Standard (SEC 502-02.2) (01106/2013)

Exhibit A

Reporting Relationships of Technology Services



Note: VSU CISO directly reports to the Chief of Staff, but he or she has direct access to the University President if needed to discuss IT Security risks and vulnerabilities.