Purpose

The 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.

VSU'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 VSU IS program provides the framework and practices for all business functions, departments, faculty, staff and students to use in securing their information. The VSU IS program is 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.

Guiding Principles

The following principles guide the development and implementation of the VSU Information Security Program.

a. The VSU Information Security program is and shall continue to be designed to:
   1. Ensure the confidentiality, integrity and availability of VSU information;
   2. Protect against any anticipated threats or hazards to the security or integrity of the information; and
   3. Protect against unauthorized access to or use of the information that could result in substantial harm or inconvenience to anyone.

b. VSU sensitive information is:
   1. A critical asset that shall be protected; and
   2. Restricted data permitted for use to authorized personnel for official purposes.

c. VSU recognizes that Information Security is:
   1. A cornerstone of maintaining public trust;
   2. Managed to address both business and technology requirements;
   3. Risk-based and cost-effective;
   4. Aligned with VSU priorities, industry best practices, and government requirements;
   5. Directed by policy but implemented by business owners;
   6. Applied holistically, regardless of medium.

Scope of Policy

This IT Security Monitoring and Logging policy applies to all University employees (permanent, temporary, contractual, faculty, administrators and students) who develop and use VSU information technology resources to conduct University business and to transmit sensitive data or Personally Identifiable Information (PII) in the performance of their jobs, and all VSU information systems that store or process PII or other sensitive data.

Policy Statement

It is the policy of the VSU that Security Monitoring and Logging for all University information systems will be consistent with then-current best practices for Security Monitoring and Logging as prescribed by Commonwealth Security and Risk Management:

1. Establishing, monitoring, and operating IT systems in a manner consistent with COV Information Security policies and standards.
2. Monitors the use of information system accounts for unauthorized usage
3. Monitors privileged role assignments for any unauthorized usage
4. Monitors information system accounts for atypical or suspicious usage use; and reports atypical usage of information system accounts to the agency Information Security Officer ("ISO"), agency head, or Information Security Officer ("ISO").
5. Displays to users organization-defined system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable Commonwealth laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that;
    a. Users are accessing a Commonwealth information system;
    b. Information system usage may be monitored, recorded, and subject to audit;
    c. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and
    d. Use of the information system indicates consent to monitoring and recording;
6. For publicly accessible systems:
    a. Displays system use information before granting further access;
    b. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
    c. Includes a description of the authorized uses of the system.
7. Require acknowledgement that monitoring of IT systems and data may include, but is not limited to, network traffic; application and data access; keystrokes (only when required for security investigations and approved in writing by the Agency Head); and user commands; email and Internet usage; and message and data content.
8. The information system monitors and controls remote access methods.
9. All WLAN Hotspot access and traffic must be monitored for malicious activity, and log files stored on a centralized storage device;
10. Automated monitoring and control of remote access sessions allows organizations to detect cyber-attacks and also ensure ongoing compliance with remote access policies by auditing connection activities of remote users on a variety of information system components (e.g., servers, workstations, notebook computers, smart phones, and tablets)
11. All COV WLAN access and traffic must be monitored for malicious activity, and associated event log files stored on a centralized storage device;

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 Information Officer 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 Attachment 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.

Exemptions from Applicability

Systems under development and/or experimental systems that do not create additional risk to production systems and surplus and retired systems are explicitly exempt from complying with the requirements defined in this document.

Authority

Commonwealth of Virginia Information Technology Resource Management (ITRM) Information Security Standard SEC501-09 (February 20, 2015).

Responsibilities and Duties

These 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.

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

escalate problems, requirements, and matters related to information security to the highest level necessary for resolution.

2. Approve or disapprove the University Business Impact Analyses (BIAs), Risk Assessments (RAs), Continuity of Operations (COOP), and Information Technology (IT) Disaster Recovery Plan.

VSU Associate Vice President (AVP) and Information Officer (CIO)

The AVP and 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. AVP and CIO is also responsible for notifying and fully disclosing to senior management IT security risks and vulnerabilities impacting information technology solutions. The AVP and CIO should:

1. Review and approve the University Business Impact Analyses (BIAs), Risk Assessments (RAs), Continuity of Operations (COOP), and Information Technology (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.

VSU Deputy CIO for IT Administration

The Deputy CIO for Administration is responsible for IT Governance of enterprise wide projects and the Information Security Program to include, University information technology assets, policy, information security awareness, applications and web development services, risk management and continuity planning. The Deputy CIO for Administration

1. Reviews and approves the University Business Impact Analyses (BIAs), Risk Assessments (RAs),

   Continuity of Operations Plan (COOP), and Information Technology (IT) Disaster Recovery Plan.

   a. Approve System Security Plans that provide adequate protections against security risks; or
   b. 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.
2. Ensure compliance is maintained with the current version of the VITA *IT Security Audit Standard* (COV ITRM Standard SEC502).
3. Maintain liaison with the COV CISO.

VSU Deputy CIO for IT Operations

The Deputy CIO for IT Operations is responsible for IT Operations, 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 of IT Operations should:

1. Review the University Business Impact Analyses (BIAs) and Continuity of Operations Plan (COOP).
2. Contribute to and approve the Risk Assessments (RAs), Continuity of Operations Plan (COOP).
3. Prepare Information Technology (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.

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* (COY 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 Deputy CIO of IT Administration and AVP 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 Deputy CIO of IT Administration and AVP and CIO 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 Deputy CIO of IT Administration and AVP and CIO for review and approval.
8. Ensure that designee prevents conflicts 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.

11. Maintain liaison with the COV CISO.

Privacy Officer

At VSU, the 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:

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

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:

1. 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 DCO IT Operations, designate a System Administrator for the system.

Data Owner

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

1. 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.

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.

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:

1. 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.

***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:

1. 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.
6. Sign the University's Acceptable Use User agreement and return to IT Security Office.

Report all lost or stolen IT assets to the Department of Police and Public Safety (DPPS) and the University's IT Asset Manager.

Policy Review

At a minimum, this policy will be reviewed and updated every two years or earlier if necessary.

Violations of Policy

Violation of this policy may result in:

- Disciplinary action under the Virginia Department of Human Resources Policy 1.60, Standards of Conduct (4116/08, 6/1/11)

Prosecution under "Virginia Computer Crimes Act." § 18.2-152.1.

Definitions

Refer to Policy 6110 for definitions and full Glossary of Terms

Control - Any protective action, device, procedure, technique or other measure that reduces exposures. Types of controls include preventative, detective, corrective, etc.

Countermeasure- An action, device, procedure, technique, or other measure that reduces vulnerability or the impact of a threat to an information system.

Data Breach - The unauthorized access and acquisition of unreacted computerized data that compromises the security or confidentiality of personal information. Good faith acquisition of personal information by an employee or agent of an individual or entity for the purposes of the individual or

Entity that is authorized to view the data is not a breach of the security of the system, provided that the personal information is not used for a purpose other than a lawful purpose of the individual or entity or subject to further unauthorized disclosure.

Data Security - Data Security refers to those practices, technologies, and/or services used to apply security appropriately to data.

References

Virginia Department of Human Resources Management:
Policy 1.60 Standards of Conduct (4116/08, 6/1111)

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

Approval By: _____ Date: 5/10/16
President