Purpose

The University is committed to maintaining system and information integrity. In an effort to consistently maintain system and information integrity for all its systems, this policy was establish for the university staff, faculty and contractors that support technology activities and users of university systems and data.

Authority, Responsibilities and Duties

This policy applies to all University employees (permanent, temporary, contractual, faculty, administrators and students) who use VSU information technology resources to conduct University business.

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.

A. Chief Information Officer (CIO)

The CIO will give direction to the Technology Services Team to ensure that systems, user access, and data flow processes preserve data and system integrity.

B. Chief Audit Executive (CAE)

The CAE will collaborate with the CIO and ISO to ensure that an audit is performed for all sensitive systems in accordance with ITRM Standard SEC502-02.3.

C. Information Security Officer (ISO)

The ISO is responsible for ensuring that the method chosen to configure systems (architecture), segregate access, transport data, store data, display data, and share data is done according to federal and state laws, regulations, and standards; and university policies and procedures; and maintains data and system integrity.

D. Enterprise Services

The Enterprise Services Team is responsible for implementing or acquiring an infrastructure environment that is configured to ensure appropriate segregation of duties over systems and movement of data and follows all federal and state laws, regulations and standards, as well as, university policies and procedures.

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/library.

Policy Statements

As a commitment to maintain an information technology environment that safeguards its system and data integrity the university will:

1. Configure and safeguard its information technology systems in a systematic and repeatable method in order to preserve the integrity of information technology environment and data based on the information technology platforms and services it provides.
2. Ensure that security audits are performed for all sensitive system hosted or non-hosted by the university on a three year rotation basis as specified by SEC502-02.3.
3. Remediate system flaws by:
   a. Identifying, reporting, and correcting information system flaws;
   b. Testing software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
   c. Installing security-relevant software and firmware updates within 90-days of the release of the updates; and
   d. Incorporating flaw remediation into the organizational configuration management process.
4. Protect System users from malicious code by:
   a. Employing malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;
   b. Updating malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;
   c. Configuring malicious code protection mechanisms to:
      1) Perform periodic scans of the information system at least once a week and real-time scans of files from external sources at network entry/exit points as well as the destination host as the files are downloaded, opened, or executed in accordance with organizational security policy; and
      2) Quarantine malicious code; send alert to administrator in response to malicious code detection.
   d. Addressing the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.
5. Monitor information technology activity by:
   a. Monitoring the information system to detect:
      1) Attacks and indicators of potential attacks; and
      2) Unauthorized local, network, and remote connections;
   b. Identifying unauthorized use of the information system through organization-defined techniques and methods;
   c. Protecting information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion
6. Obtain security alerts, Advisories and Directives by:
   a. Receiving information system security alerts, advisories, and directives from the appropriate external organizations on an ongoing basis;
   b. Generating internal security alerts, advisories, and directives as deemed necessary;
   c. Disseminating security alerts, advisories, and directives to organization-defined list of personnel identified by name and/or by role; and
   d. Implementing security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.
7. Protect users from SPAM by:

a. Employing spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and
b. Updating spam protection mechanisms when new releases are available in accordance with the University's configuration management policy and procedures.

8. Validate information inputs by:
   a. Ensuring that input validation errors are reviewed and resolved within 30-days of discovery.
   b. Determining whether information system behaves in a predictable and documented manner that reflects organizational and system objectives when invalid inputs are received.

References

Virginia Information Technology Agency (VITA):
Information Security Standards (SEC501-09.1) (12/08/2016)

Approval By: _____ **Date:** 9/6/17
President