Purpose

The University is committed to providing a safe information technology environment that ensures the integrity of each system; therefore, all sensitive systems will be audited on a three year cycle as required by the Commonwealth Security Standard SEC501-09.1.

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 Audit Executive (CAE)

The CAE will be responsible for ensuring that IT Security Audits are performed according to the Commonwealth Security Standards (specifically SEC501-09.1 and SEC525-02). The CAE will work with the Chief Information Officer to schedule the sensitive systems and track audit findings for the university.

B. Chief Information Officer (CIO)

The CIO will determine which IT sensitive system require auditing according to the security audit plan. The CIO will work with the Internal Audit Department to determine whether audits will be contacted internally or externally.

C. IT Governance and Risk Management Director

The IT Governance and Risk Management Director is responsible for ensuring that the auditors have the information needed and assists with scheduling interviews for auditors.

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

The University will:

1. Determine whether the information system is capable of auditing the following events: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes;

2. Coordinate the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events; and
3. Provide a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents
4. Provide audit tracking capabilities within University systems that will considering the following:
    a. **Content of Records** -The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.
    b. **Audit Storage Capacity** - The information system off-loads audit records at least once every 30-days onto a different system or media than the system being audited.
    c. **Response to Audit Processing Failures** - Alerts designated organizational officials in the event of an audit processing failure;
    d. **Audit Review, Analysis, and Reporting**
        1. Reviews and analyzes information system audit records at least once a week for indications of inappropriate or unusual activity; and
        2. Reports findings to designated organizational officials
    e. **Time Stamps**
        1. Use internal system clocks to generate time stamps for audit records; and
        2. Record time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets the organization-defined granularity of time measurement based on the sensitivity of the system.
    f. **Protection of Audit Information -**The information system protects audit information and audit tools from unauthorized access, modification, and deletion.
    g. **Audit Records Retention** - The University retains audit records for consistent with the University's records retention policy to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.
    h. **Audit Generation**
        1. Provides audit record generation capability for the auditable events defined in SEC 501-09.1 section AU-2 at the operating system, services, applications, and network components;
        2. Allows authorized organization personnel to select which auditable events are to be audited by specific components of the information system; and
        3. Generates audit records for the events and content defined in SEC 501-09.1 Section AU-3.
    i. **Monitoring for Information Disclosure** -The University monitors organization-defined open source information and/or information sites at the appropriate

organization-defined frequency for evidence of unauthorized disclosure of organizational information.

References

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

10/4/17

Approval By: _____ **Date:** _____
President