Purpose

The University's infrastructure security is a direct reflection of the ability to develop an information system architectural structure that appropriately protects the interfaces that either input or export data from the University's information technology environment. This policy will assist at setting the appropriate controls to safeguard the university in the movement of its data internally and with hosted vendors.

Authority, Responsibility, and Duties

The 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 interest.

A. Enterprise Manager

The Enterprise Manager is responsible for ensuring that the University's Information Technology infrastructure protects the movement of data within the university and between its vendor partnership.

B. Network Manager

The Network Manager is responsible for ensuring that the network topology is sound to ensure that communication connections internal to the University and with its partners are designed in a manner that safeguards the University's data and systems connected to the network.

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.

General Requirements

The University will consider the following requirements when implementing its information technology environment:

1. **Application Partitioning** - The information system separates user functionality (including user interface services) from information system management functionality
2. **Security Function Isolation** - The information system isolates security functions from non-security functions;
3. **Information Shared Resources** - The information system prevents unauthorized and unintended information transfer via shared system resources.
4. **Denial of Service Protection** -The information system protects against or limits the effects of denial of service attacks by employing security safeguards.

5. **Resource Priority** - The information system protects the availability of resources by allocating organization-defined resources by priority.

6. **Boundary Protection** – The University will:

   a. Monitor and control communications at the external boundary of the system and at key internal boundaries within the system;

   b. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal organizational networks; and

   c. Connect to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

7. **Transmission Integrity** - The information system protects the integrity of transmitted information.

   a. Require the use of encryption or digital signatures for the transmission of email and attached data that is sensitive relative to integrity.

   b. Require encryption for the transmission of email and attached data that is sensitive relative to confidentiality. The ISO should consider and plan for the issue of agency email being intercepted, incorrectly addressed, or infected with a virus

8. **Network Disconnect** - The information system terminates the network connection associated with a communications session at the end of the session or after 15-minutes of inactivity.

9. **Cryptographic Key Establishment and Management** -The University establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with the organization-defined requirements for key generation, distribution, storage, access, and destruction.

   The University will:

   a. Define the process for the creation and storage of any cryptographic keying material used to protect organization-defined information rated sensitive for confidential or integrity Agency practices for selecting and deploying encryption technologies and for the encryption of data.

   b. Document the procedure for the creation and storage of any cryptographic keying material used to protect organization-defined information rated sensitive for confidential or integrity

   c. Ensure that the cryptographic keying material remain under the exclusive control of the commonwealth.

10. **Use Cryptography -** The information system implements cryptography in accordance with applicable Commonwealth laws, Executive Orders, directives, policies, regulations, and standards.

    The University will:

    a. Define and document Agency practices for selecting and deploying encryption technologies and for the encryption of data.

    b. Document appropriate processes before implementing encryption. These processes must include the following components:

1) Instructions in the IT Security Agency's Incident Response Plan on how to respond when encryption keys are compromised;

2) A secure key management system for the administration and distribution of encryption keys; and

3) Requirements to generate all encryption keys through an approved encryption package and securely store the keys in the event of key loss due to unexpected circumstances.

c. Require encryption for the transmission of data that is sensitive relative to confidentiality or integrity over non-Commonwealth networks or any publicly accessible networks, or any transmission outside of the data's broadcast domain. Digital signatures may be utilized for data that is sensitive solely relative to integrity

11. **Collaborative Computing Devices** – The University will:

a. Prohibit remote activation of collaborative computing devices; and

b. Provide an explicit indication of use to users physically present at the devices.

12. **Public Key Infrastructure Certificates** -The University will issue public key certificates under an approved organization-defined certificate policy or obtains public key certificates from an approved service provider.

13. **Mobile Code** – The University will:

a. Define acceptable and unacceptable mobile code and mobile code technologies;

b. Establish usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and

c. Authorize, monitor, and control the use of mobile code within the information system.

14. **Voice Over Internet Protocol** – The University will:

a. Establish usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and

b. Authorize, monitor, and control the use of VoIP within the information system.

15. **Secure Name/Address Resolution Service (Authoritative Source)** -The University will:

a. Provide additional data origin and integrity artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and

b. Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace

16. **Secure Name/Address Resolution Service (Recursive or Coaching Resolver)** The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

17. **Architecture and Provisioning for Name/Address Resolution Service** -The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.
18. **Session Authenticity** - The information system protects the authenticity of communications sessions.
19. **Protection of Information at Rest** - The information system protects the confidentiality and integrity of information at rest.
20. **Out-of-Band Channels** - The organization employs organization-defined out-of-band channels for the physical delivery or electronic transmission of organization-defined information, information system components, or devices to organization-defined individuals or information systems.
21. **Process Isolation** - The information system maintains a separate execution domain for each executing process.
22. **Port and I/O Device Access -** The organization physically disables or removes organization-defined connection ports or input/output devices on organization-defined information systems or information system components.
23. **Sensor Capability and Data** – The University will:
    a. Prohibit the remote activation of environmental sensing capabilities with the following exceptions: agency head approved policy, indicating business functions that cannot be accomplished without the use of the capability; and
    b. Provide an explicit indication of sensor use to the user of the device.
24. **Usage Restrictions** – The University will:
    a. Establish usage restrictions and implementation guidance for organization-defined information system components based on the potential to cause damage to the information system if used maliciously; and
    b. Authorize, monitor, and control the use of such components within the information system.
    c. Permit the remote activation of environmental sensing capabilities if required as part of an authorized incident response activity; and
    d. Only provide an explicit indication of the sensor use if authorized by the incident response team.

References

Virginia Information Technology Agency (VITA):
Information Security Standards (SEC501-09) (05/01/2015)
IT Systems Security Guideline (SEC515-00) (07/17/2008)

Library of Virginia Records Retention and Disposition Schedule for Administrative Records GS-101 located at: http://www.lva.virginia.gov/agencies/records/sched_state/GS-101.pdf

Library of Virginia Records Retention and Disposition Schedule for State Agencies: College and University located at: http://www.lva.virginia.gov/agencies/records/sched_state/GS-111.pdf

Approval By: _____ **Date:** 10/4/17
President