Purpose

Establishing and maintaining a healthy infrastructure and system environment starts with maintenance practices and schedules that are consistent and repeatable. This System Maintenance Policy was created to ensure that maintenance procedure are in place, understood by all university faculty, staff; and implemented and practiced by operational staff and system users.

Authority, Responsibility, Duties and Scope

System maintenance is a collective responsibility of University employees, contractor, etc. 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. System maintenance oversight responsibility must be considered when hosting systems outside of the university's direct care and the expectation of care over those system will must be governed by this policy and understood and agreed upon by outsourced vendors.

A. Enterprise Manager

The Enterprise Manager is responsible for ensuring that infrastructure and system maintenance is appropriately scheduled and implemented to protect the university's systems and data. The Enterprise Manager is required to collaborate with the Information Security Office and Systems Owner to ensure that patches to systems and infrastructure are timely updated and version upgrades are consistent with Commonwealth Security Requirements; therefore, prior to implementation of maintenance, the Enterprise Manager should understand the impact of maintenance on the data center's system resources.

B. Information Security Officer (ISO)

The ISO is responsible for partnering with the Enterprise Manager and Systems Owner to ensure that maintenance procedures are implemented in a manner the safeguards the university's systems and data and these routine maintenance procedures are performed in accordance with Commonwealth Security and Risk Management Standards.

C. Systems Owner

The Systems Owner is responsible for informing the Enterprise Manager of any impacts that may occur as a result of scheduling of maintenance on the business and application specifically. The Enterprise Manager, ISO and the Systems Owner will coordinate system maintenance schedules to minimize impact to students and network activity. The Systems Owner is also responsible for coordinating communication of hosting vendor's maintenance activities to the ISO and Enterprise Manager.

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 Policy Statements

1. Maintenance Procedures should include the following:
   a. Scheduling, performing, documenting, and reviewing records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.
   b. Approval and monitoring of all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;
   c. Requirements that a designated organization official explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;
   d. Sanitizing equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;
   e. Checking all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions;
   f. Including the appropriate maintenance-related information in organizational maintenance records.
   g. Requiring that non-escorted personnel performing maintenance on the information system have required access authorizations; and
   h. Designating organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

References

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

9/6/17

Approval By: _____ **Date**_____
President