Purpose

This policy reflects the University's commitment, understanding, and acceptance of its obligation to ensure continuity of operations for mission/business operations with established recovery time objectives (RTOs) and recovery point objectives (RPOs).

Authority, Responsibility, Duties, and Scope

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 interests. This policy applies to contractors, employees, vendors and student interns of Virginia State University (VSU) collectively.

A. System Owner(s)

System and Data Owners are required to participate in the development of the University's Business Impact Analysis (BIA) and establish recovery time objectives (RTOs) and recovery point objectives (RPOs). In coordination with Technology Services Department staff, the System and data owners are responsible for developing a backup and recovery plan to facilitate the proper protection of institutional data. The plan should include, but is not necessarily limited to the following:

1. Identification of all critical data, applications, documentation, personnel, facilities, and other support items that would be necessary to perform essential tasks during a recovery period.

2. The steward responsible for the department of organization's critical data.

3. The specific backup and recovery processes designed to restore the organization's critical data.

    a. The backup scheme used (timeframe for full, incremental, etc.).

    b. Location for off-site storage of critical data. Organizations will document the procedures for maintaining a current copy of the critical data and will determine the frequency of update to this off-site storage.

    c. Documentation of the restoration process including the procedures for the recovery from single-system or application failures, as well as, for a total disaster scenario.

4. Backup and recovery plans must be reviewed and updated regularly to account for new technology, business changes, and migration of applications to alternative platforms.

5. All critical information shall be placed on a networked file server for backup. It is recommended that no critical information, including Protected Health Information as

defined by the Health Information Portability and Accountability Act (HIPAA), be permanently stored on workstations, laptops, or personal devices.

6. Recovery procedures will be tested on a periodic basis however, at a minimum, these procedures will be tested on an annual basis.

B. **Data Owners**

Data Owners must also participate in the development of the University's BIA and establish RTOs and RPOs. Additionally, they must identify the type(s) of data handled by each University IT system, determine whether each type of data is also subject to other regulatory requirements, and determine the potential damages to the University of a compromise of confidentiality, integrity, or availability of each type of data handled by the IT system, and classify the sensitivity of the data accordingly.

C. **Technology Services IT Operations Support Staff**

Technology Services Department support personnel must routinely conduct test restores, document the results of the tests, and implement any corrective actions needed to complete a successful back-up and recovery. The back-up strategy must be tested on an established schedule, not to exceed one year between tests and the results must be documented.

D. **Technology Services Continuity Coordinator**

The Technology Services (TS) Continuity of Operations (COOP) Coordinator is the designated IT employee responsible for collaboration with the university's Continuity Plan (CP) Coordinator as the focal point for IT aspects of Continuity Plan and related Disaster Recovery (DR) planning activities. Using the results of the Business Impact Analysis and Risk Assessment, the TS COOP Coordinator will identify each IT system that is necessary to recover essential business functions or dependent business functions and the RTO and RPO for each such IT system. The TS COOP Coordinator shall develop and maintain a personnel contact information list and incident notification 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

1. VSU Department of Police and Public Safety (DPPS) department is the COOP Coordinator for the University as required in the COOP planning guide by the Virginia Department of Emergency Management (VDEM).
2. It is the policy of the University that the Technology Services department in conjunction with academic and business departments, will develop, document and maintain appropriate policies, standards, and specific written processes and procedures to address

Continuity of Operations Planning, IT Disaster Recovery Planning, and IT Systems and Data Backup and Restoration, specifically as follows:

a. Designate an employee to collaborate with the VSU COOP coordinator as the focal point for IT aspects of COOP and related Disaster Recovery (DR) planning activities and DR training and DR test exercises.

3. Based on results of the Business Impact Analysis (BIA) and Risk Assessments (RA), develop IT disaster recovery components of the University COOP which identifies: :

    a. Each IT system that is necessary to recover business essential functions or dependent business functions and the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for each; and
    b. Personnel contact information and incident notification procedures.
    c. Requirements of an annual exercise (or more often as necessary) of the VSU COOP and IT DR components to assess the adequacy and effectiveness of the plan; and
    d. Requirement of a review and revision of IT DR components following the exercise (and at other times as necessary).

5. The VSU COOP and IT DRP must be approved by the University President. :
6. Periodically review, reassess, test, and revise the VSU COOP and IT DRP to reflect changes in essential business functions, services, IT system hardware and software, and personnel.
7. Establish communication methods to support IT system users' local and remote access to IT systems, as necessary.
8. The Data Backup and Restoration plan must ensure that data and systems can be recovered and information technology services can be resumed following an event causing the loss of data. The University and its business partners will operate within generally accepted best practices for backup and restoration to include, but not be limited to:

    a. Secure off-site storage for backup media.
    b. Store off-site backup media in an off-site location that is geographically separate and distinct from the primary location.
    c. Ensure performance of backups is conducted only by authorized personnel.
    d. Review of backup logs after the completion of each backup job to verify successful completion.
    e. System Owners approve backup schedules of the systems they own.
    f. System Owners approve emergency backup and operations restoration plans of the systems they own.

9. Any backup media that is sent off-site (physically or electronically), or shipped by the United States Postal Service or any commercial carrier, must be protected in accordance within the University's "Data Storage Media Protection Policy".
10. Authorization and logging of deposits and withdrawals of all media that is stored off-site is required.

11. Retention of the data handled by an IT system must be in accordance with the State Library of Virginia records retention policies and procedures.
12. The University's management of electronic information must be performed in such a way that it can be produced in a timely and complete manner when necessary, such as during a legal discovery proceeding.
13. Document and exercise a strategy for testing to ensure that IT systems and data backups and restoration are tested on a periodic basis to ensure backups are functioning as expected and the data can be restored in a usable form.
14. For systems that are sensitive relative to availability, document and exercise a strategy for testing disaster recovery procedures and in accordance with the VSU COOP Plan.
15. Backups procedures established contain an alternate storage site that includes necessary agreements to permit the storage and retrieval of information system backup information; and ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.
16. Contingency Plan will:
    a. Establish an alternate processing site including necessary agreements to permit the transfer and resumption of information system operations for essential missions/business functions within the organization-defined time period consistent with recovery time and recovery point objectives when the primary processing capabilities are unavailable;
    b. Ensure that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and
    c. Ensure that the alternate processing site provides information security safeguards equivalent to that of the primary site.
17. The university will provide contingency training information system users consistent with assigned roles and responsibilities:
    a. Within 10-days of assuming a contingency role or responsibility;
    b. When required by information system changes; and
    c. Annually thereafter.

References

Virginia Information Technology Agency (VITA):

Information Security Standard (SEC501-09.1, 12/08/2016)
IT Contingency Planning Guideline (SEC 508-00, 04/18/07)

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

President