Title: Information Technology (IT) Contingency Planning Policy Policy: 6135

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, 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 interests. Refer to Information Security Policy 6110 for roles and responsibilities. This policy applies to contractors, employees, vendors and student interns of Virginia State University ("VSU") collectively.

A. System Owner(s)

System Owners are required to:

1. Develop, document and disseminate to the appropriate personnel or roles, a contingency policy that identifies essential missions and business functions and the associated contingency requirements. The requirements will address scope, purpose, roles, responsibilities, management commitment, and coordination among organizational entities for the mission essential business functions.

2. Develop procedures that facilitate the implementation of the contingency planning policies and controls

3. Create a schedule to review the Contingency planning policy on an annual basis. Provisions should be made for more frequent reviews in event of changes within the organization or the University overall.

4. Coordinate the contingency plan with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.

5. Designate an employee as a point of contact to collaborate with Technology Services, telecommunications and environmental support to ensure that all Continuity and Disaster Recovery Planning efforts are in line with the University as a whole.

6. Protect the contingency plan from unauthorized disclosure or updates/modifications.

7. Will ensure that at least an annual contingency exercise (more if deemed necessary) is conducted to ensure accuracy, adequacy and effectiveness of the plan. A review of the plan is required, with revisions/updates being added as deemed necessary.

8. Where external parties/service providers are involved, coordinate with those entities to ensure all contingency requirements are met.

9. Once the Contingency Plan is completed, create an IT Disaster Recovery Plan (DRP). This plan will ensure that mission essential functions and their dependencies are restored within the required recovery time objective (RTO).

10. Likewise, the DRP will be reviewed, tested, reassessed and revised, at least on an annual basis (but more often, if deemed necessary due to changes within the organization).

11. Provide contingency training to all users that is consistent with their applicable roles and responsibilities.

    a. This training will occur within the first 30 days of hire within the contingency role or responsibility

    b. Training is also required when changes occur within the system that result in a revision to the contingency procedures/policies.

    c. Annual training is required on an on-going basis to ensure that all personnel involved in the contingency program is kept up-to-date with the operation.

12. For mission essential systems, establish an alternate processing site in the event of disruption of service.

    a. The alternate site includes all required documentation, agreements required for resumption of service within the required recovery time objective (RTO)

    b. The alternate site will be equipped with the necessary equipment, supplies and telecommunication services to support the mission essential functions until normal operations resume.

    c. The alternate site will provide security that is at least equivalent to that of the primary site.

    d. The alternate site shall have telecommunications agreements that contain provisions for priority-of-service that are consistent with the RTO.

13. 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.

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

15. 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.

16. 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**

Using the results of the Business Impact Analysis and Risk Assessment, the Technology Services (TS) Continuity Plan 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 Continuity Plan 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 Continuity Plan Coordinator for the University as required in the Continuity 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 Continuity Plan coordinator as the focal point for IT aspects of Continuity Planning 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 Continuity Plan 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. Require an annual exercise (or more often as necessary) of the VSU Continuity Plan and IT DR components to assess the adequacy and effectiveness of the plan; and
    d. Require review and revision of IT DR components following the exercise (and at other times as necessary).
5. The VSU Continuity Plan and IT Disaster Recovery Plan (DRP) must be approved by the University President.
6. Periodically review, reassess, test, and revise the VSU Continuity Plan 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 IT security requirements.

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. IT system and data backups and restoration must be 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, recovery of the system and data will be tested based on disaster recovery procedures and in accordance with the VSU Continuity Plan.

References

Virginia Information Technology Agency (VITA):

Information Security Standard (SEC501-09, 02/20/2015)
IT Security Audit Standard (SEC502-02.2, 01/06/2013)
IT Contingency Planning Guideline (SEC 508-00, 04/18/07)

NIST Special Publications

Contingency Planning Guide for Information Technology Systems SP 800-34 Rev.1, 05/2010
Recommend Security Controls for Federal Information Systems and Organizations SP 800-53 A Rev.4
Computer Security Incident Handling Guide SP 800-61 Rev.2 08/2012
Information Security Handbook: A Guide for Managers SP 800-100.

Approval By: _____ Date: 5/10/16
President