Purpose

The purpose of this policy is to ensure that the University will conduct, develop, and maintain a viable business impact analysis that will identify their business functions, those business functions that are essential to the University's mission, and identify the IT resources that are required to support these essential functions.

Authority, Responsibilities and Duties

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. Refer to Information Security Policy 6110 for roles and responsibilities.

A. System Owners

Systems Owners are required to participate in the development of the University's Business Impact Analysis (BIA). Additionally, for each mission essential function (MEF) and primary business function (PBF), these individuals will assess whether the function depends upon an IT system for recovery. Each system that is required to recover an MEF or PBF shall be considered sensitive relative to availability. For each system classified as "Sensitive", System Owners are required to establish recovery time objectives (RTO) and recovery point objectives (RPO). The resources required to support each MEF and PBF must be identified as well. Lastly, the System Owners reviews and approves the BIA.

B. Data Owners

Data Owners must also participate in the development of the University's Business Impact Analysis (BIA) to establish recovery time objectives (RTO) and recovery point objectives (RPO). Additionally, these individuals must identify the type(s) of data handled by each University IT system for which they are the data owner, determine whether each type of data is also subject to other regulatory requirements, and determine the potential damages to the University due to 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. University Executives and Senior Management

University Executives and Senior Management in Academic and Business units of the University are responsible for and must participate in the development of the University's Business Impact Analysis (BIA) to ensure that recovery time objectives (RTO) and recovery point objectives (RPO) are established for the systems and data handled by all the University IT systems within their purview. These individuals are also responsible for establishing overall priorities for

recovery of systems and data and periodic review (at least annually) of the BIA to adjust RTO/RPO and priorities. University Executives shall approve the final BIA prioritization list.

Roles and Responsibilities

1. Business Impact Analysis (BIA) delineates the steps necessary for VSU to identify the business functions, identify those business functions (e.g. Primary Business Functions - PBFs) that are essential to the University's mission (Mission Essential Functions – MEFs), and identify the resources that are required to support its essential business functions.
2. 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).
3. 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 Plan, IT Disaster Recovery Planning,* and *IT Systems and Data Backup and Restoration.*
4. 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.
5. 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. Require 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. Require 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) are picked up by Iron Mountain or any commercial cannier, 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 VSU COOP Plan.

Policy Statement

This Business Impact Analysis policy applies to all University employees (permanent, temporary, contractual, faculty, administrators and students) who use VSU information technology resources to conduct University business.

I. It is the policy of the University that it will develop and periodically update, the business impact analysis to ensure that the recovery time objectives (RTO) and recovery point objectives (RPO) for essential business functions and dependent functions that rely upon IT resources, are identified and documented. The information will be used as input to the IT Systems and Data Sensitivity Classification, Risk Assessments, IT Contingency Planning, and IT System Security Plans.

2. Exceptions to this Policy

Exceptions to this policy will require a documented request that details the business case for the exception, specifically what requirement the exception is for, and what mitigating controls will be implemented to protect the University. Refer to Information Security Policy 6110 for the requirements and process to file an exception.

3. Violations of Policy

Violation of this policy may result in disciplinary action under the Virginia Department of Human Resources Policy 1.60, Standards of Conduct (4116/08, 611111).

References

Virginia Information Technology Agency (VITA):
- Information Security Standard (SEC 501-09) (02/20/2015)
- IT Contingency Planning Guideline (SEC 508-00) (04118/07)
- IT Security Audit Standard (SEC502-02.2) (01/06/2013)

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