



OIT 62.203: Business Impact Analysis

Responsible Executive: Information Security Officer
Responsible Office: Office of Information Technology
Related Policy:
Approved-On Date: 2/28/2011
Effective Date: 7/1/2011
Revision Date: 2/1/2011

I. Policy Statement

Business Impact Analysis addresses protecting University information and IT systems commensurate with sensitivity and risk, including system availability needs. This is a central component of the University information security program and allows the University to determine how these factors apply to its IT systems and data.

II. Purpose

The Business Impact Analysis (BIA) policy delineates the steps necessary for the University to identify its business functions, identify those University business functions that are essential to the University's mission, and identify the resources that are required to support these essential University business functions.

Note: The requirements below address only the IT and data aspects of BIA and do not require the University to develop a BIA separate from the BIA that could be used to develop the University's Continuity of Operations Plan (COOP). The University should create a single BIA that meets both the requirements of this Policy and can be used to develop the University COOP. The University should consult the VDEM Continuity of Operations Planning Manual for COOP requirements.

III. Scope

This policy applies to all Commonwealth of Virginia (COV) systems and to the University IT network infrastructure.

IV. Requirements

NSU should:

1. Require the participation of System Owners and Data Owners in the development of the agency's BIA.

2. Identify University business functions.
3. Identify essential business functions.

Note: A business function is essential if disruption or degradation of the function prevents the University from performing its mission, as described in the University mission statement.

4. Identify dependent functions, if any. Determine and document any additional functions on which each essential business function depends. These dependent functions are essential functions as well.
5. For each essential business function and dependent function, assess whether the function depends on an IT system to be recovered. Each IT system that is required to recover an essential function or a dependent function shall be considered sensitive relative to availability. For each such system, the University shall:
 - a. Determine and document the required Recovery Time Objective (RTO), based on University goals and objectives.
 - b. Determine and document the Recovery Point Objectives (RPO).
6. Use the IT information documented in the BIA report as a primary input to IT System and Data Sensitivity Classification (Policy 62.204), Risk Assessment (Policy 62.206), IT Contingency Planning (Policies 62.302, 62.303 and 62.304) and IT System Security Plans (Policy 62.402).
7. Conduct periodic review and revision of the agency BIAs, as needed, but at least once every three years.

V. Violations

Violations of this policy will be addressed in accordance relevant University and Commonwealth of Virginia policies, including University Policy 60.201 and Department of Human Resources Management Policy 1.75. The appropriate level of disciplinary action will be determined on an individual case basis by the appropriate executive or designee, with sanctions up to or including termination or expulsion depending upon the severity of the offense.

VI. Interpretation

The Information Security Officer is responsible for official interpretation of this policy. Questions regarding the application of this policy should be directed to the Office of Information Technology. The Information Security Officer reserves the right to revise or eliminate this policy.

