Policy Title: Business Impact Analysis

Policy Type: Administrative

Policy Number: ADMINISTRATIVE POLICY # 32 – 8 – 3 (2014) Business Impact Analysis

Approval Date: 05/28/2014 Revised

Responsible Office: Office of Information Technology

Responsible Executive: CIO

Applies to: Office of Information Technology

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.

TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>TABLE OF CONTENTS</th>
<th>PAGE NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contacts</td>
<td>1</td>
</tr>
<tr>
<td>Stakeholder(s)</td>
<td>1</td>
</tr>
<tr>
<td>Purpose</td>
<td>2</td>
</tr>
<tr>
<td>Requirements</td>
<td>2</td>
</tr>
<tr>
<td>Violations</td>
<td>3</td>
</tr>
<tr>
<td>Interpretation</td>
<td>3</td>
</tr>
<tr>
<td>Publication</td>
<td>3</td>
</tr>
<tr>
<td>Review Schedule</td>
<td>3</td>
</tr>
<tr>
<td>Related Documents</td>
<td>3</td>
</tr>
</tbody>
</table>

CONTACT(S)

Office of Information Technology – (757)823-2869

STAKEHOLDER(S)

University Faculty & Staff
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 a BIA and do not require the University to develop a BIA separate from the BIA that could be used to develop an agency’s Continuity Plan (previously referred to as Continuity of Operations Plan). The University should create a single BIA that meets both the requirements of this Policy and can be used to develop the University Continuity Plan (previously referred to as Continuity of Operations Plan).

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 mission essential functions (MEFs).

   Note: MEFs are functions that cannot be deferred during an emergency or disaster.

4. Identify dependent and supporting functions, known as primary business functions (PBFs), previously referred to as primary functions, on which each mission essential function (MEF) depends.

5. For each MEF and PBF, assess whether the function depends on an IT system to be recovered. Each IT system that is required to recover a MEF or PBF shall be considered sensitive relative to availability. For each such system, the University shall:

   a. Document the required Recovery Time Objective (RTO), based on University and COV goals, objectives, and MEFs, as outlined in the University Continuity Plan.

   b. Document the Recovery Point Objectives (RPO) as outlined in the University Continuity Plan.

6. Use the IT information documented in the BIA report as a primary input to IT System and Data Sensitivity Classification (Section 62.3), Risk Assessment (Section 62.6), Contingency Plan (Section 62.8.6) and System Security Plan (Section 62.8.12).
7. Conduct periodic review and revision of the University BIAs, as needed, but at least once every three years.

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.

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.

PUBLICATION

This policy shall be widely published and distributed to the University community. To ensure timely publication and distribution thereof, the Responsible Office will make every effort to:

1. Communicate the policy in writing, electronic or otherwise, to the University community within 14 days of approval;

2. Submit the policy for inclusion in the online Policy Library within 14 days of approval;

3. Post the policy on the appropriate SharePoint Site and/or Website; and

4. Educate and train all stakeholders and appropriate audiences on the policy’s content, as necessary. Failure to meet the publication requirements does not invalidate this policy.

REVIEW SCHEDULE

- Next Scheduled Review: 05/28/2015
- Approval by, date: Office of Information Technology and 05/28/2014
- Revision History:
  - Supersedes (previous policy): OIT 62.8.3 Business Impact Analysis

RELATED DOCUMENTS