**Business Impact Analysis Policy Template**

### Business Impact Analysis PolicyTEBMPLATE

###

**EFFECTIVE DATE: 07/01/2014**

ggggf

# PURPOSE

The purpose of this policy is to create a prescriptive set of process and procedures, aligned with applicable COV IT security policy and standards, to ensure that “YOUR AGENCY NAME” develops, disseminates, and updates the Business Impact Analysis (BIA) Policy. This policy and procedure establishes the minimum requirements for the Business Impact Analysis Policy.

This policy is intended to meet the requirements outlined in SEC501, Section 3 Business Impact Analysis.

# SCOPE

All “YOUR AGENCY NAME” employees (classified, hourly, or business partners) as well as all “YOUR AGENCY NAME” systems

# ACRONYMS

BIA: Business Impact Analysis

CIO: Chief Information Officer

COV: Commonwealth of Virginia

CSRM: Commonwealth Security and Risk Management

MEF: Mission Essential Function

ISO: Information Security Officer

IT: Information Technology

ITRM: Information Technology Resource Management

PBF: Primary Business Function

RPO: Recovery Point Objectives

RTO: Recovery Time Objective

SEC501: Information Security Standard 501

“YOUR AGENCY NAME”: ““YOUR AGENCY NAME”

# DEFINITIONS

[See COV ITRM Glossary](http://www.vita.virginia.gov/uploadedFiles/Library/PSGs/EA_PSG_update_011510/ITRMGlossary_011510.pdf)

# BACKGROUND

The Business Impact Analysis Policy at “YOUR AGENCY NAME” is intended to facilitate the effective implementation of the processes necessary meet the Business Impact Analysis requirements as stipulated by the COV ITRM Security Standard SEC501 and security best practices. This policy directs that “YOUR AGENCY NAME” meet these requirements for all IT systems.

Preparing for business interruptions is required by the Commonwealth of Virginia for all agencies. Business interruption preparation activities are formalized by executing a well-defined business continuity process, as specified in the “YOUR AGENCY NAME”’s IT Contingency Planning Policy. This process consists of several steps leading to an effective restoration solution for “YOUR AGENCY NAME”’s mission essential and primary business functions and their supporting processes and resources that may be affected by a business interruption.

The BIA addresses the first step in “YOUR AGENCY NAME”’s business continuity process. The BIA identifies each business function executed by the organization, determines the impact of its failure on the organization, in both tangible and non-tangible terms, identifies the resources (e.g., human, facilities, information technology (IT) systems, communications, transportation, etc.) that will be required to restore the business function, and in the case of multiple failures, prioritizes the order by which business functions will be restored.

# ROLES & RESPONSIBILITY

This section will provide summary of the roles and responsibilities as described in the Statement of Policy section. The following Roles and Responsibility Matrix describe 4 activities:

1. Responsible (R) – Person working on activity
2. Accountable (A) – Person with decision authority and one who delegates the work
3. Consulted (C) – Key stakeholder or subject matter expert who should be included in decision or work activity
4. Informed (I) – Person who needs to know of decision or action

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Roles** | Agency Head | Information Security Officer | “YOUR AGENCY NAME” Continuity Coordinator | “YOUR AGENCY NAME” Continuity Team | “YOUR AGENCY NAME” Directors | Data and System Owners |
| **Tasks** |   |   |  |  |  |  |
| Designate a “YOUR AGENCY NAME” continuity coordinator |  | A/R |  |  |  |  |
| Assign members to serve on continuity team |  |  |  |  | A/R |  |
| Coordinate bia and continuity plans |  |  | A | R |  | R |
| Develop a list of all business functions |  |  | I |  | A | R |
| Create mef’s and pbf’s |  |  | I |  | A | R |
| Determine resources for mef’s and pbf’s |  |  | I |  | A | R |
| Document rto and rpo for mef’s and pbf’s |  |  | I |  | A | R |
| Produce bia |  |  | A |  |  | R |
| Review bia on an annual basis |  |  | A | R | C | C |
| Review and approve bia | A/R | C |  |  |  |  |

# STATEMENT OF POLICY

In accordance with SEC501, “YOUR AGENCY NAME” shall identify their business functions, identify business functions that are essential to its mission, and identify the resources that are required to support these business functions by performing a Business Impact Analysis. “YOUR AGENCY NAME” shall create a single BIA that meets the requirements of SEC501 and that can be used to develop their Continuity Plan (previously referred to as Continuity of Operations Plan or COOP, to include an IT Disaster Recovery Plan, if applicable).

BUSINESS IMPACT ANALYSIS

* 1. The Chief Information Officer, Information Security Officer or an agency designee shall designate a “YOUR AGENCY NAME” employee as the “YOUR AGENCY NAME” Continuity Coordinator, who will serve as chairperson of the “YOUR AGENCY NAME” Continuity Team. “YOUR AGENCY NAME” Directors will name a primary and backup to serve as members of the “YOUR AGENCY NAME” Continuity Team. These members will coordinate all BIA and Continuity Plan functions for their directorate and with all “YOUR AGENCY NAME” System and Data Owners. Each “YOUR AGENCY NAME” Directorate will submit BIA reports to the “YOUR AGENCY NAME” Continuity Team to be used to develop the “YOUR AGENCY NAME” BIA and Continuity Plan.
	2. Each “YOUR AGENCY NAME” Directorate shall develop a list of all business functions that it executes on a routine, occasional, or periodic basis. The documentation shall include, at a minimum:
		1. The primary objectives, customers, and interfaces of the business function;
		2. Any sensitive data used in or produced by the business function;
		3. The potential harm that would occur if the business function were not performed.

Note: A Business Function Information Template to document this information will be provided by the Commonwealth Security and Risk Management Directorate.

* 1. The “YOUR AGENCY NAME” Continuity Coordinator will compile the information from the Business Function Information Templates to create a prioritized list of business functions.
	2. Identified business functions shall be classified as:
		1. Mission essential functions; or
			1. MEFs are functions that cannot be deferred during an emergency or disaster.
		2. Dependent and supporting functions, known as primary business functions, on which each mission essential function depends.
	3. For each MEF and PBF, the “YOUR AGENCY NAME” directorates will:
		1. Determine the resources required by the function. Examples for resources may include offices and furniture, data center facilities, utilities, phone and fax services, IT systems (hardware and software), data communications services, transportation and fueling services, personnel, periodic maintenance services, etc.
		2. Assess whether the function depends on an IT system. If the business function is dependent on IT resources, the “YOUR AGENCY NAME” Continuity Team will determine, in consultation with the “YOUR AGENCY NAME” Directorate, the extent to which the business function depends on IT resources. Each IT system that is required to recover a MEF or PBF shall be considered sensitive relative to availability. For each such system, the “YOUR AGENCY NAME” Continuity team shall:
			1. Document the Recovery Time Objective.
			2. Document the Recovery Point Objectives.
	4. The “YOUR AGENCY NAME” Continuity Coordinator will use this information to identify the minimum number of types and quantities of resources that must be restored at an alternate site to provide an acceptable level of service during a business interruption.
		1. Some resources may be shared by several business processes and may have different priority levels depending on their criticality. In such cases, the resource priority designation for restoration purposes shall be the highest priority assigned.
	5. The “YOUR AGENCY NAME” Continuity Coordinator, with the participation of System Owners and Data Owners, will produce a BIA report that:
		1. Documents the dependence of the “YOUR AGENCY NAME”’s mission essential and primary business functions on business processes and resources, including specific IT systems and/or data; and
		2. Specifies the required recovery time for each process and resource, including IT systems and/or data, on which mission essential and primary business functions depends, based on:
			1. Agency and COV goals and objectives; and
			2. The extent to which mission essential and primary business functions depend upon the specific resource, including IT systems and/or data.
	6. The “YOUR AGENCY NAME” Continuity Coordinator will provide the BIA report to the “YOUR AGENCY NAME” Information Security Officer, System Owners, and Data Owners, for use in IT system and data sensitivity classification and risk assessment, and will use the BIA report in IT contingency planning.
	7. The “YOUR AGENCY NAME” Continuity Coordinator and “YOUR AGENCY NAME” Continuity team conduct an annual review of the BIA to determine its currency, and will facilitate updating the BIA, as necessary, and no less than once every three years.
	8. The “YOUR AGENCY NAME” Agency Head will review and approve the BIA after initial completion and following subsequent updates.

**ASSOCIATED**

**PROCEDURE** “YOUR AGENCY NAME” Information Security Program Policy

**AUTHORITY**

**REFERENCE** [*Code of Virginia, §2.2-2005 et seq.*](https://law.lis.virginia.gov/vacode/title2.2/chapter20.1/section2.2-2005/#:~:text=%C2%A7%202.2%2D2005.-,Creation%20of%20Agency%3B%20appointment%20of%20Chief%20Information%20Officer,A.&text=The%20CIO%20shall%20exercise%20the,and%20the%20Secretary%20of%20Administration.)

(Powers and duties of the Chief Information Officer “CIO” ““YOUR AGENCY NAME” Name”; ““YOUR AGENCY NAME””)

**OTHER**

**REFERENCE** [ITRM Information Security Policy (SEC519)](http://www.vita.virginia.gov/uploadedFiles/Library/PSGs/Security_Policy_519_00_Final_0709.pdf)

 [ITRM Information Security Standard (SEC501)](http://www.vita.virginia.gov/uploadedfiles/VITA_Main_Public/Library/PSGs/Information_Security_Standard_SEC501_06_07012011.pdf)

| Version History |
| --- |
| Version | Date | Change Summary  |
| 1 | 01/13/2004 | Original publication of the *Business Impact Analysis and Risk Assessment Procedure* |
| 2 | 09/28/2007 | Supersedes the *Business Impact Analysis and Risk Assessment Procedure* and includes changes thataddress the roles and responsibilities of the Information Security Officers (ISO) and the Continuity of Operation Plan coordinator.  |
| 3 | 2/01/2013 | Administrative Change |
| 4 | 7/01/2014 | Name changed and updated to conform to Information Security Standard SEC501 revision 8. Role matrix added |
| 5 | 11/09/2021 | Formatting Changes |