



## **Business Continuity and Disaster Recovery Standard**

Document Name: Business Continuity and Disaster  
Recovery  
Document ID: IS.005

Effective Date: October 15<sup>th</sup>, 2018

Last Revised Date: November 16, 2023

### Table of contents

1. Purpose .....	2
2. AUTHORITY .....	2
3. Scope .....	2
4. Responsibility.....	2
5. Compliance.....	2
6. Standard Statements .....	3
6.1 Business Continuity Management.....	3
6.2 Disaster Recovery Management .....	4
7. Control Mapping .....	6
8. Related Documents .....	6
9. Document Change Control .....	6

## 1. PURPOSE

Business Continuity and Disaster Recovery – The purpose of this **standard** is to establish **procedures** for the continuation of critical business processes in the event of any organizational or **information** technology (“IT”) infrastructure failure and define the related **controls** and acceptable practices.

## 2. AUTHORITY

M.G.L. Ch. 7d provides that “Notwithstanding any general or special law, rule, regulation, executive order, policy or procedure to the contrary, all executive department agencies shall, and other state agencies may, adhere to the policies, procedures and objectives established by the executive office of technology services and security with respect to activities concerning information technology.”

## 3. SCOPE

This document applies to the use of **information, information systems**, electronic and computing devices, **applications**, and network resources used to conduct business on behalf of the Commonwealth. The document applies to the Executive Branch including all executive offices, and all boards, commissions, agencies, departments, divisions, councils, and bureaus, hereinafter referred to as Commonwealth Agencies and Offices. Other Commonwealth entities that voluntarily use or participate in services provided by the Executive Office of Technology Services and Security, (EOTSS), such as mass.gov, must agree to comply with this document as a condition of use. Executive Branch Agencies and Offices are required to implement **procedures** that ensure their **personnel** comply with the requirements herein to safeguard **information**.

## 4. RESPONSIBILITY

- 4.1. The Enterprise Risk Management Office is responsible for the development and ongoing maintenance of this **standard**.
- 4.2. The Enterprise Risk Management Office is responsible for compliance with this **standard** and may enlist other departments in the maintaining and monitoring of compliance with this **standard**.
- 4.3. Any inquiries or comments regarding this **standard** must be submitted to the Enterprise Risk Management Office by sending an email to [ERM@mass.gov](mailto:ERM@mass.gov).
- 4.4. Additional information regarding this **standard** and its related **standards** may be found at <https://www.mass.gov/cybersecurity/policies>.

## 5. COMPLIANCE

- 5.1. Compliance with this document is mandatory for the Executive Branch including all Commonwealth Agencies and Offices. Violations are subject to disciplinary action in accordance with applicable employment and collective bargaining agreements, up to and including the termination of their employment and/or assignment with the Commonwealth.

**Exceptions** to any part of this document must be requested online through ServiceNow, <https://www.mass.gov.service-now.com> ). An **exception** may be granted only if the benefits of the **exception** outweigh the increased **risks**, as determined by the **Commonwealth CISO**, or his or her designee. Any and all **exceptions** will be for a specified time and will be narrow in scope. .

## 6. STANDARD STATEMENTS

### 6.1 Business Continuity Management

Commonwealth Agencies and Offices must establish a Business Continuity Program.

#### 6.1.1 Commonwealth Agencies and Offices must develop and maintain **processes** for business continuity, as follows:

- 6.1.1.1 Identify a Business Continuity Lead that will have primary responsibilities for the Business Continuity Program, including plan development, plan testing and program sustainment.
- 6.1.1.2 Perform a **risk** assessment of critical **information assets**: Establish **controls** to identify, contain and mitigate the **risks** associated with the loss or disruption of critical business processes and **information assets** (see *IS.010 Information Security Risk Management Standard* for additional detail on **risk** assessments).
- 6.1.1.3 Conduct **business impact analysis** (BIA): Commonwealth Agencies and Offices must leverage *IS.004 Asset Management Policy* when applicable, to perform a BIA to identify critical business processes, **information assets**, customers, **third parties**, technical and non-technical dependencies, and recovery timelines and to assess the impact a disruption would have on the organizational processes, systems, and operations.
  - 6.1.1.3.1 The BIA must be updated whenever a major organizational change occurs or at least annually, whichever comes first.
- 6.1.1.4 Develop business continuity plans (BCP): Commonwealth Agencies and Offices will develop BCPs for critical business processes based on prioritization of likely disruptive events in light of their probability, severity and consequences for **information** security identified through the BIA and **risk** assessment processes.
  - 6.1.1.4.1 BCPs will address both manual and automated processes used by the agency and document minimum operating requirements to resume critical functions/**applications** in an appropriate period of time.
  - 6.1.1.4.2 The primary responsibility for developing, maintaining, and testing organizational and functional BCPs will reside with the Business Continuity Lead.
    - 6.1.1.4.2.1 Roles and responsibilities of BCP **stakeholders** will be clearly defined and communicated.
    - 6.1.1.4.2.2 Point(s) of contact should be identified from the customer side for any **incident** or crisis communication via call, messaging and/or email. The contact details of the point(s) of contact should be validated and updated at least annually.

6.1.1.4.3 BCPs must be updated whenever a major organizational change occurs or at least annually, whichever comes first.

6.1.1.4.4 BCPs will be developed as follows:

6.1.1.4.4.1 Identify essential mission and business functions and a plan for maintaining these functions in the event of system or environment compromise, disruption, or failure.

6.1.1.4.4.2 Create and implement adequate business recovery and **risk** mitigation strategies, including the definition of acceptable recovery time frames.

6.1.1.4.4.3 Clearly state the conditions required for activating BCPs to minimize the cost associated with unnecessary use.

6.1.1.4.4.4 Define fallback and resumption emergency **procedures** to allow for temporary measures and full resumption as required. Ensure that **confidential information** is protected while operating in emergency mode.

6.1.1.4.4.5 Assess BCP impact to external organizational dependencies and contracts.

6.1.1.4.4.6 Develop public relations strategy to ensure effective and timely communication to relevant **stakeholders**.

6.1.1.4.5 Business Continuity Lead will schedule and conduct annual BCP test for BCP **users** consistent with assigned responsibilities.

6.1.1.4.6 Business Continuity Lead will schedule and evaluate BCP testing **procedures** to ensure that they are practical and realistic.

6.1.1.4.6.1 Perform annual tests of the BCPs to identify incorrect assumptions, oversights, and account for updates to equipment or **personnel** changes. Test results will be reported to senior management, **the Commonwealth CISO**, or his or her designee, and the Security Office.

6.1.1.4.6.2 All relevant **stakeholders** associated with BCP procedures will participate in annual testing. A debrief session to evaluate test results and to discuss lessons learned should be conducted following the test.

6.1.1.4.6.3 If significant changes are implemented to BCPs, testing cadence must be reevaluated and executed.

6.1.2 **Information Owner** will develop backup standard operating procedures that are in alignment with *IS.012 Operations Management Standard* and specifically *Data Backup and Restoration in IS.012 Operations Management Standard* to ensure that copies of critical **data** are retrievable.

## 6.2 Disaster Recovery Management

Commonwealth Agencies and Offices must ensure that Disaster Recovery (DR) **procedures** will be initiated when the appropriate **personnel** have determined that the ability to recover critical **information assets** will likely exceed the established recovery time and/or recovery point objectives. Adequate

backup facilities should be provided such that all essential **information assets** can be recovered following a disaster.

- 6.2.1 Commonwealth Agencies and Offices must develop and maintain **processes** for disaster recovery plans at both onsite primary Commonwealth locations and at alternate offsite locations. DR plans must include step-by-step emergency procedures, including:
  - 6.2.1.1 Identify relevant **stakeholders** (primary and secondary) and establish a call tree.
  - 6.2.1.2 Conduct a damage assessment of the impacted IT infrastructure and **applications**.
  - 6.2.1.3 Establish **procedures** that allow facility access (e.g., recovery/secondary site) in support of the restoration of lost **data** in the event of an emergency.
  - 6.2.1.4 Recover critical agency services and **information assets** based on recovery priorities as established during the BIA.
  - 6.2.1.5 Provide interim means for performing critical business processes at or above the minimum service level defined in the BCP and within the tolerable length of time.
  - 6.2.1.6 Restore service at the original site of impact and migrate from the alternate locations to the original site without unacceptable interruption or degradation in service.
- 6.2.2 Commonwealth Agencies and Offices must ensure that DR plans will be tested annually. The test may consist of structured walk-through exercises or actual execution of the plan at an appropriate alternate site. The results will be discussed, reported, and documented with senior management, the **Commonwealth CISO**, or his or her designee, and the Security Office.
  - 6.2.2.1 Detailed test plans must be developed with clear test scope, purpose, and objectives, as well as identify the **personnel** involved and the timeframe necessary for the test. Measurement criteria must be included.
  - 6.2.2.2 **Information** security aspects (e.g., **data** protection) of the test plan will be reviewed and approved by the Security Office.
  - 6.2.2.3 All critical processes and **applications**/systems for contingency, recovery, automatic fail-over, manual fail-over and replacement of failed components will be tested:
    - 6.2.2.3.1 Annually under normal operating conditions. The assessment may include announced or unannounced events.
    - 6.2.2.3.2 Whenever significant technological, organizational, or business changes occur.
- 6.2.3 Commonwealth Agencies and Offices must ensure that DR **personnel** will keep a current copy of the DR plan documentation at the designated primary and alternate locations.
- 6.2.4 Commonwealth Agencies and Offices must ensure that approval to distribute the DR plan is the responsibility of the designated DR Lead.
- 6.2.5 Systematic version **control** to manage the DR plan will be implemented to maintain accuracy. Outdated versions of the DR plan will be retired.

## 7. CONTROL MAPPING

Section	NIST SP800-53 R5	CIS 18 v6	NIST CSF
6.1 Business Continuity Management	AU-7	CSC 8	PR.PT-1
	AU-9	CSC 8	PR.PT-1
	IR-4	CSC 17	DE.AE-family
	CP-1	-	ID.GV-1
	CP-2	-	ID.AM-5
	CP-3	-	-
6.2 Disaster Recovery Management	CP-4	CSC 17	PR.IP-4
	CP-1	-	ID.GV-1
	CP-2	-	ID.AM-5
	CP-4	CSC 17	PR.IP-4
	CP-6	CSC 11	PR.IP-4
	CP-7	-	-
	PE-17	-	-
	CP-10	CSC 11	RS.RP-1

## 8. RELATED DOCUMENTS

Document	Effective date

## 9. DOCUMENT CHANGE CONTROL

Version No.	Revised by	Effective date	Description of changes
0.90	Jim Cusson	10/01/2017	Corrections and formatting.
0.92	John Merto	01/02/2018	Corrections, Formatting
0.95	Sean Vinck	5/7/2018	Corrections and Formatting
0.96	Andrew Rudder	5/31/2018	Corrections and Formatting
0.98	Anthony O'Neill	05/31/2018	Corrections and Formatting
1.0	Dennis McDermitt	06/01/2018	Pre-Publication Review
1.0	Andrew Rudder	10/4/2018	Approved for Publication by: John Merto
1.1	Megan Perkins	7/15/2020	Annual Review; Minor corrections and formatting
1.2	Sean M. Hughes	11/04/2021	Annual Review
1.3	Sean M. Hughes	08/29/2022	Updates for NIST 800-53R5 and annual review
1.4	Thomas E. McDermott	11/16/2023	Corrections, formatting, updating and Annual Review
1.5	Anthony O'Neill		Final Review

The owner of this document is the **Commonwealth CISO** (or his or her designee). It is the responsibility of the **document owner** to maintain, update and communicate the content of this document. Questions regarding this document must be submitted to the **document owner** by sending an email to [ERM@mass.gov](mailto:ERM@mass.gov).

## 9.1 Annual Review

This *Business Continuity and Disaster Recovery Standard* should be reviewed and updated by the **document owner** on an annual basis or when significant **policy** or **procedure** changes necessitate an amendment.