Commonwealth of Massachusetts

Massachusetts Office of Information Technology

# Enterprise Business Continuity for IT Management Policy

**Reference #: ITD-POL-SEC-15.1 Issue Date: June 5, 2013
Issue #: 1**

## Table of Contents

[Table of Contents 1](#_Toc438198110)

[Executive Summary 1](#_Toc438198111)

[Whom this Policy Applies To 2](#_Toc438198112)

[Policy Statement 2](#_Toc438198113)

[Roles and Responsibilities 4](#_Toc438198114)

[Related Documents 5](#_Toc438198115)

[Contact 6](#_Toc438198116)

[Appendix A: Terms 7](#_Toc438198117)

[Appendix B: Document History 11](#_Toc438198118)

## Executive Summary

This policy articulates requirements that assist management in defining a framework that outlines business continuity and disaster recovery plans, processes, procedures, testing, and reporting mechanisms that are to be in place and in effect to provide for continuity of agency business operations. This framework provides the necessary structure for building agency operational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, information assets, and Information Technology (IT) Resources, in case of a disruption to or a reduction in the quality of IT services. Agencies are required to have controls in place and in effect that provide reasonable assurance that security objectives are addressed throughout such a disruption.

The Agency Head, or their designee, has the responsibility to exercise due diligence in the adoption of this framework. Agencies are required to achieve compliance with the overall information security goals of the Commonwealth including compliance with laws, regulations, policies and standards to which their technology resources and data, including but not limited to personal information, are subject.

## Whom this Policy Applies To

All agencies and entities governed by the overarching [Enterprise Information Security Policy](http://www.mass.gov/anf/research-and-tech/cyber-security/security-for-state-employees/security-policies-and-standards/information-security-policy.html)[[1]](#footnote-1) are required to adhere to requirements of this supporting policy.

* Executive Department Agencies, [[2]](#footnote-2) as well as any agency or third party that connects to the Commonwealth’s wide area network (MAGNet), are required to comply with this policy.
* Executive Department Agencies are required to ensure compliance by any business partner that accesses Executive Department IT Resources or shared environments, e.g. MAGNet; and
* Executive Department Agencies are required to ensure compliance by third parties in any aspect of the process of providing goods and services to their agency. These include, but are not limited to, electronic data collection, storage, processing, disposal, dissemination and maintenance. Third parties that interact in any way with Executive Department Commonwealth IT Resources, e.g. MAGNet, are required to comply with this policy.

Other Commonwealth entities are encouraged to adopt, at a minimum, security requirements in accordance with this Enterprise Business Continuity Management Policy or a more stringent agency policy that addresses agency specific and business related directives, laws, and regulations.

## Policy Statement

1. Agencies are required to develop, implement, test and maintain a Business Continuity Plan (BCP) for all Information Technology Resources (ITR) that deliver or support core Critical Business Functions on behalf of the Commonwealth of Massachusetts.

For purposes of this policy, the BCP is the overall plan that facilitates sustaining critical operations while recovering from a disruption. BCP’s are required to include, at a minimum:

* + Standard Incident Response Procedures: An information system-focused set of procedures to be used when an event occurs that is not part of the standard operation of a service and may or does cause disruption to or a reduction in the quality of services and Customer productivity.
	+ Disaster Recovery Plan (DRP): An information system-focused plan designed to restore operability of the target system, application, or computer facility infrastructure in the event of large scale disaster and/or other cataclysmic event.
	+ Continuity of Operations Plans (COOP): An information system-focused plan invoked under a DRP when access to the primary facility infrastructure is prevented for an extended period, requiring operations to be restored from an alternate site after an emergency. The COOP may be supported by multiple information system contingency plans to address recovery of impacted individual systems once the alternate facility has been established. The COOP only addresses information system disruptions that require relocation. (From NIST SP 800-34).
1. Agencies are required to conduct risk assessments to identify, estimate, and prioritize risks to organizational operations and conduct business impact analyses to identify all critical functions of the agency, entity or business unit and their supporting information systems. MassIT’s Compliance Assurance Office is available to assist and/or conduct such assessments.
2. Agencies are required to articulate specific information, including the details necessary to effectively respond, manage, and recover from either an Incident or a Catastrophic Event. Further, protecting data and confidential information should be integrated into the above referenced details.
3. Agencies are required to ensure that all BCPs and supporting DRPs and COOPs are in alignment with and in support of any and all legal and regulatory requirements that the agency ITR’s are subject to.
4. Agencies are required, at a minimum, to include the following documentation and procedures in their BCP and its supporting components:
	1. Scope / Objectives
	2. Risk Evaluation and Required Security Controls
	3. Business Impact Analysis
	4. Communications Procedures
	5. BCP Organization Structure
		1. Activation of plans
		2. Succession of Authority Procedures
		3. BCP Team Roles and Responsibilities
			1. Incident/Event Response Teams
			2. Emergency/DR Response Teams
		4. Primary and Alternate Contact Lists
	6. Damage Assessment
	7. Recovery Plans
		1. Critical System Recovery
			1. Prioritization of Recovery
			2. Interdependencies
			3. Resource requirements
			4. Security Controls
			5. COOP
				1. Mobilizing Alternate Locations / Resources
				2. Managing Alternate Locations / Resources
				3. Critical System Support

Short term

Long term

Local

Regional

Pandemic

1. Agencies are required to verify that critical third party vendors are contractually obligated to meet agency business continuity requirements. Alternate third party vendors are required to be identified where appropriate.
2. Agencies are required to securely store copies of plans and supporting materials in a remote location (a) at a sufficient distance to escape any damage from a disaster at the agency’s main information processing facilities and (b) in such a manner that they are available (via remote connection, external e-mail location, etc.).
3. Agencies are required to document, implement and annually test plans including the testing of all appropriate security provisions to minimize impact to systems or processes from the effects of major failures of IT Resources or disasters.
4. Agencies are required to identify appropriate mechanisms to ensure that plans remain current and updated between annual tests and reviews accounting for:
	1. Change management implications
	2. New/Major upgrades of system implementations
	3. New policy adoption
	4. New contract implementations
	5. New threat/risk identification
	6. Staff/resource/responsibility changes
5. Agencies are required to publish plans and sufficiently train any and all individuals that are required or responsible for supporting the BCP.

## Roles and Responsibilities

All agencies and entities governed by the overarching [Enterprise Information Security Policy](http://www.mass.gov/anf/research-and-tech/cyber-security/security-for-state-employees/security-policies-and-standards/information-security-policy.html)[[3]](#footnote-3) are subject to the referenced roles and responsibilities in addition to those specifically stated within this supporting policy. The roles and responsibilities associated with implementation and compliance with this policy are detailed below:

### Assistant Secretary for Information Technology

* Develop mandatory standards and procedures for agencies to follow prior to entering into contracts that will provide third parties access to electronic highly sensitive information, including but not limited to, personal information or IT systems containing such information.
* Approval and adoption of the Enterprise Business Continuity Management Policy, supporting standards and their revisions.

### Secretariat Chief Information Officer (SCIO) and Agency Head

* Provide communication, training, implementation and enforcement of this policy.
* Provide proper third party oversight as applicable for any outsourced Business Continuity and Disaster Recovery services including IT Resources and alternate IT facilities.
* Review and approve Business Continuity and Disaster Recovery programs and plans submitted by the Secretariat or Agency.
* Continuous testing and monitoring of the plans including execution and simulation of outage or catastrophic event, and recovery at alternate site(s).

### Enterprise Security Board (ESB)

* Recommend revisions and updates to this policy and related standards.

### Massachusetts Office of Information Technology (MassIT)

* Maintain this policy and related standards including review of related recommendations of the Enterprise Security Board, issue policy revisions and updates. Provide assistance and direction when requested, or as necessary.

### Third parties

* Required to comply with agency implementation of this policy at a minimum or a more stringent agency specific policy including:
	+ Conformance to agency Business Continuity Plan and supporting Disaster Recovery Plan and Continuity of Operations Plan.

## Related Documents

Primary references that were used in development of this policy include:

* ISO 27001
* Executive Order 504
* [FEMA *Ready* Business](http://www.ready.gov/business/implementation)[[4]](#footnote-4)

Additional information referenced includes:

* M.G.L., Ch 93H
* M.G.L., Ch 93I
* M.G.L., Ch 66A
* ISO 27002
* CobiT
* ITIL
* HIPAA Security Rule
* NIST 800-34

## Contact

Standards@state.ma.us

## Appendix A: Terms

Key terms used in this policy have been provided below for your convenience. For a full list of terms please refer to the glossary of [Commonwealth Specific Terms](http://www.mass.gov/anf/research-and-tech/policies-legal-and-technical-guidance/glossary-of-commonwealth.html)[[5]](#footnote-5) on the Massachusetts Office of Information Technology’s website.

**Alternate Site:** An alternate operating location to be used by business functions when the primary facilities are inaccessible. 1) Another location, computer center or work area designated for recovery. 2) Location, other than the main facility, that can be used to conduct business functions. 3) A location, other than the normal facility, used to process data and/or conduct critical business functions in the event of a disaster.

**Asset:** An item of property and/or component of a business activity/process owned by an organization. There are three types of assets: physical assets (e.g. buildings and equipment); financial assets (e.g. currency, bank deposits and shares) and non-tangible assets (e.g. goodwill, reputation).

**Business Continuity:** The ability of an organization to provide service and support for its customers and to maintain its viability before, during, and after a business continuity event.

**Business Continuity Plan (BCP):**  Process of developing and documenting arrangements and procedures that enable an organization to respond to an event that lasts for an unacceptable period of time and return to performing its critical functions after an interruption.

**Business Impact Analysis:** A process designed to prioritize business functions by assessing the potential quantitative (financial) and qualitative (non-financial) impact that might result if an organization was to experience a business continuity event.

**Contact List:** A list of team members and/or key personnel to be contacted including their backups. The list will include the necessary contact information (i.e. home phone, pager, cell, etc.) and in many cases it is considered confidential.

**Contingency Plan:** A plan used by an organization or business unit to respond to a specific systems failure or disruption of operations.

**Contingency Planning:** Process of developing advanced arrangements and procedures that enable an organization to respond to an undesired event that negatively impacts the organization.

**Continuity Of Operations Plan (COOP):** Provides procedures and guidance to sustain an organization’s mission essential functions at an alternate site for up to 30 days. Information systems are addressed based only on their support of the mission essential functions.

**Critical Business Functions:** The critical operational and/or business support functions that could not be interrupted or unavailable for more than a mandated or predetermined timeframe without significantly jeopardizing the organization. An example of a business function is a logical grouping of processes/activities that produce a product and/or service such as Accounting, Staffing, Customer Service, etc.

**Damage Assessment:** The process of assessing damage to computer hardware, vital records, office facilities, etc., and determining what can be salvaged or restored and what must be replaced following a disaster.

**Dependency:** The reliance or interaction of one activity or process upon another.

**Disaster:** A sudden, unplanned catastrophic event causing unacceptable damage or loss. 1) An event that compromises an organization's ability to provide critical functions, processes, or services for some unacceptable period of time 2) An event where an organization's management invokes their recovery plans.

**Disaster Recovery:** The ability of an organization to respond to a disaster or an interruption in services by implementing a disaster recovery plan to stabilize and restore the organization's critical functions.

**Disaster Recovery Plan:** The management approved document that defines the resources, actions, tasks and data required to manage the technology recovery effort. Usually refers to the technology recovery effort. This is a component of the Business Continuity Management Program.

**Escalation:** The process by which event related information is communicated upwards through an organization's established Chain of Command.

**Event:** Any occurrence that may lead to a business continuity incident.

**Exercise:** A people focused activity designed to execute business continuity plans and evaluate the individual and/or organization performance against approved standards or objectives. Exercises can be announced or unannounced, and are performed for the purpose of training and conditioning team members, and validating the business continuity plan. Exercise results identify plan gaps and limitations and are used to improve and revise the Business Continuity Plans. Types of exercises include: Table Top Exercise, Simulation Exercise, Operational Exercise, Mock Disaster, Desktop Exercise, Full Rehearsal.

**Hot site:** An alternate facility that already has in place the computer, telecommunications, and environmental infrastructure required to recover critical business functions or information systems.

**Impact:** The effect, acceptable or unacceptable, of an event on an organization. The types of business impact are usually described as financial and non-financial and are further divided into specific types of impact.

**Incident:** An event which is not part of a standard operating business which may impact or interrupt services and, in some cases, may lead to disaster.

**Incident Response:** The response of an organization to a disaster or other significant event that may significantly impact the organization, its people, or its ability to function productively. An incident response may include evacuation of a facility, initiating a disaster recovery plan, performing damage assessment, and any other measures necessary to bring an organization to a more stable status.

**Information Security:** The securing or safeguarding of all sensitive information, electronic or otherwise, which is owned by an organization.

**Infrastructure:** The underlying foundation, basic framework, or interconnecting structural elements that support an organization.

**Internal Hot site:** A fully equipped alternate processing site owned and operated by the organization.

**ITSEC:** The objective of the IT Commonwealth Service Excellence Committee (ITSEC) is to better align IT with the business for the purpose of delivering the highest quality IT services at the most efficient cost. It fosters inter-agency communication and effective service delivery through the collaboration, sharing and adoption of best practices to achieve the collective goal of best serving the agencies and citizens of the Commonwealth.

**Loss:** Unrecoverable resources that are redirected or removed as a result of a Business Continuity event. Such losses may be loss of life, revenue, market share, competitive stature, public image, facilities, or operational capability.

**NIST:** The National Institute of Standards and Technology was founded in 1901 and is now part of the U.S. Department of Commerce. Today, NIST measurements support the smallest of technologies—nanoscale devices so tiny that tens of thousands can fit on the end of a single human hair—to the largest and most complex of human-made creations, from earthquake-resistant skyscrapers to wide-body jetliners to global communication networks.

**Outage:** The interruption of automated processing systems, infrastructure, support services, or essential business operations, which may result, in the organizations inability to provide services for some period of time.

**Prioritization:** The ordering of critical activities and their dependencies are established during the BIA and Strategic-planning phase. The business continuity plans will be implemented in the order necessary at the time of the event.

**Quantitative Assessment:** The process for placing value on a business function for risk purposes. It is a systematic method that evaluates possible financial impact for losing the ability to perform a business function. It uses numeric values to allow for prioritizations. This is normally done during the BIA phase of planning.

**Recovery:** Implementing the prioritized actions required to return the processes and support functions to operational stability following an interruption or disaster.

**Recovery Management Team:** See: Business Continuity Management (BCM) Team.

**Recovery Teams:** A structured group of teams ready to take control of the recovery operations if a disaster should occur.

**Recovery Time Objective (RTO):** The period of time within which systems, applications, or functions must be recovered after an outage (e.g. one business day). RTO's are often used as the basis for the development of recovery strategies, and as a determinant as to whether or not to implement the recovery strategies during a disaster situation.

**Response:** The reaction to an incident or emergency to assess the damage or impact and to ascertain the level of containment and control activity required. In addition to addressing matters of life safety and evacuation, Response also addresses the policies, procedures and actions to be followed in the event of an emergency.

**Restoration:** Process of planning for and/or implementing procedures for the repair of hardware, relocation of the primary site and its contents, and returning to normal operations at the permanent operational location.

**Risk:** Potential for exposure to loss which can be determined by using either qualitative or quantitative measures.

**Risk Assessment / Analysis:** Process of identifying the risks to an organization, assessing the critical functions necessary for an organization to continue business operations, defining the controls in place to reduce organization exposure and evaluating the cost for such controls. Risk analysis often involves an evaluation of the probabilities of a particular event.

**Simulation Exercise:** One method of exercising teams in which participants perform some or all of the actions they would take in the event of plan activation. Simulation exercises, which may involve one or more teams, are performed under conditions that at least partially simulate 'disaster mode'. They may or may not be performed at the designated alternate location, and typically use only a partial recovery configuration.

**System:** Set of related technology components that work together to support a business process or provide a service.

**System Recovery:** The procedures for rebuilding a computer system and network to the condition where it is ready to accept data and applications, and facilitate network communications.

**Test:** A pass/fail evaluation of infrastructure (example-computers, cabling, devices, hardware) and\or physical plant infrastructure (example-building systems, generators, utilities) to demonstrate the anticipated operation of the components and system. Tests are often performed as part of normal operations and maintenance. Tests are often included within exercises. (See Exercise).

**Threat:** A combination of the risk, the consequence of that risk, and the likelihood that the negative event will take place.

**Uninterruptible Power Supply (UPS):** A backup electrical power supply that provides continuous power to critical equipment in the event that commercial power is lost. The UPS (usually a bank of batteries) offers short-term protection against power surges and outages. The UPS usually only allows enough time for vital systems to be correctly powered down.

## Appendix B: Document History

| Date | Action | Effective Date | Next Review Date |
| --- | --- | --- | --- |
| 6/5/13 | Publish Enterprise Business Continuity Management Policy  | 6/5/2013 | 1/30/2014 |
| 2/1/14 | Reviewed | 2/1/14 | 2/2/15 |
| 2/20/15 | Reviewed | 2/20/15 | 2/21/16 |
| 12/15/2015 | Accessibility remediation – no content changes | 2/22/16 | 1/1/17 |

1. http://www.mass.gov/anf/research-and-tech/cyber-security/security-for-state-employees/security-policies-and-standards/information-security-policy.html [↑](#footnote-ref-1)
2. The Executive Department is comprised of the Executive Branch minus the Constitutional Offices, i.e., the State Auditor, State Treasurer, the Attorney General, and the Secretary of the Commonwealth. [↑](#footnote-ref-2)
3. http://www.mass.gov/anf/research-and-tech/cyber-security/security-for-state-employees/security-policies-and-standards/information-security-policy.html [↑](#footnote-ref-3)
4. http://www.ready.gov/business/implementation [↑](#footnote-ref-4)
5. http://www.mass.gov/anf/research-and-tech/policies-legal-and-technical-guidance/glossary-of-commonwealth.html [↑](#footnote-ref-5)