



State of Maine
Department of Administrative & Financial Services
Office of Information Technology

Contingency Planning Policy and Procedures (CP-1)

Table of Contents

Table of Contents..... 2

1.0 Document Purpose:..... 3

2.0 Scope: 3

3.0 Policy Conflict: 3

4.0 Roles and Responsibilities: 3

5.0 Management Commitment: 4

6.0 Coordination Among Agency Entities:..... 4

7.0 Compliance: 4

8.0 Procedures: 4

9.0 Document History and Distribution:..... 10

10.0 Document Review: 11

11.0 Records Management: 11

12.0 Public Records Exceptions: 11

13.0 Definitions: 11

1.0 Document Purpose:

The purpose of this document is to outline the Office of Information Technology (OIT) policy and procedures for contingency planning. This policy is designed to protect the services of the State from corruption or loss of access, due to the disruption of *information assets*.

2.0 Scope:

2.1 This policy applies to all State of Maine employees and contractors (collectively referred to as personnel in this document) with access to:

2.1.1 Executive Branch Agency *information assets*, irrespective of location; and

2.1.2 Information assets from other State government branches that utilize the State network.

3.0 Policy Conflict:

If this policy conflicts with any law or union contract in effect, the terms of the existing law or contract prevail.

4.0 Roles and Responsibilities:

4.1 Agencies are responsible for:

4.1.1 Ensuring that any contract for vendor hosted/managed agency *information assets* adhere to any pertinent federal regulations, state regulations and Office of Information Technology (OIT) policies, procedures, and *standards*.

4.1.2 Ensuring agency personnel are aware of all applicable penalties for non-compliance.

4.1.3 Developing and implementing agency-level policy and procedures, to meet any additional, pertinent contingency planning statutory requirements.

4.2 The Office of Information Technology (OIT) is responsible for:

4.2.1 Assigning an owner for each information asset supported by the Office of Information Technology (OIT).

4.3 Chief Information Officer (CIO) is responsible for:

4.3.1 Owning, executing, and enforcing this policy.

4.4 Chief Information Security Officer (CISO) is responsible for:

Contingency Planning Policy and Procedures (CP-1)

4.4.1 *Disaster recovery* (DR) of State of Maine information assets.

4.5 OIT Information Asset Owners are responsible for:

4.5.1 Ensuring that standard operating procedures (SOPs) are developed and/or employees trained to support the recovery of systems as specified in the Information System Contingency Plan (ISCP).

4.5.2 Ensuring the appropriate techniques are followed for the information assets they are responsible for, to recover infrastructure quickly and effectively following a service disruption.

5.0 Management Commitment:

The State of Maine is committed to following this policy and the procedures that support it.

6.0 Coordination Among Agency Entities:

The Office of Information Technology (OIT) provides information system contingency planning at the enterprise-level for infrastructure consumed by agency information assets. Agencies coordinate with their Office of Information Technology (OIT) Account Managers, and/or the Application Managers, to address any additional agency-specific contingency plan requirements. Application development managers serve as the owners for the agency information assets that their teams support.

7.0 Compliance:

7.1 For State of Maine employees, failure to comply with the procedures identified in this policy may result in progressive discipline up to and including dismissal.

7.2 For State of Maine contractors and non-State of Maine personnel, failure to comply may result in removal of the individual's ability to access and use State of Maine data and systems. Employers of non-State of Maine personnel will be notified of any violations.

7.3 Personnel are also subject to any applicable penalties for statutory requirements compliance violations. Depending on the requirement and the nature of the violation, penalties could include fines and/or criminal charges.

8.0 Procedures:

8.1 The following standards apply to the State of Maine's contingency planning capabilities. They represent the base set of procedural requirements that are implemented for contingency planning.

8.2 Contingency Plan (CP-2 including CE-1, CE-2, CE-3, CE-8):

Contingency Planning Policy and Procedures (CP-1)

- 8.2.1 The Office of Information Technology will recover OIT-hosted information assets, following a disruption, as outlined in the Information Systems Contingency Plan (coming soon).
- 8.2.2 Agencies must ensure that, where required, Information System Contingency Plans (ISCPs) are established for I.T. services and assets procured by the agency. Best practice is to require an ISCP as part of the vendor contract.
- 8.2.3 Agencies must develop contingency plans to meet statutory requirements or the needs of the agency. A good guide for the contingency plan is outlined in [NIST SP 800-34](#).¹

8.3 Contingency Training (CP-3):

- 8.3.1 Agencies must provide contingency training to information asset users, consistent with assigned roles and responsibilities, to ensure that the training includes the appropriate content and level of detail.
 - 8.3.1.1 Office of Information Technology contingency plan training is outlined in Contingency Plan Training, Testing and Exercise Procedures (IR-2, CP-3, IR-3, and CP-4) (coming soon).

8.4 Contingency Plan Testing (CP-4 including CE-1):

- 8.4.1 Agencies must ensure that agency Information System Contingency Plans are tested annually. This requires active coordination with OIT.
- 8.4.2 Agencies must coordinate contingency plan testing with organizational elements responsible for related plans (e.g., business continuity plans, occupant emergency plans, continuity of operations plans, etc.)
 - 8.4.2.1 Office of Information Technology contingency plan testing and exercises are outlined in Contingency Plan Training, Testing and Exercise Procedures (IR-2, CP-3, IR-3, and CP-4) (coming soon).

8.5 Alternative Storage Site (CP-6 including CE-1, CE-3):

- 8.5.1 Agencies must determine which agency information assets require alternative site storage.
 - 8.5.1.1 Agencies consult with OIT to establish alternative storage sites, to meet identified business and/or regulatory requirements, for agency information assets. The actual action-items will differ between OIT-hosting and remote-hosting.

¹ <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf>

Contingency Planning Policy and Procedures (CP-1)

- 8.5.1.2 The Office of Information Technology manages two data centers, with equivalent security safeguards, that are available for agencies to utilize as primary and alternative storage sites, for OIT-hosted information assets.
 - 8.5.1.2.1 The two data centers consolidate State of Maine storage onto the EMC series of arrays network attached storage (NAS) and storage area networks (SAN), allowing full storage integration to be achieved.
 - 8.5.1.2.2 OIT has implemented a solution of tiered storage, data management and de-duplication at the NAS level, which includes user shares and application shares.
 - 8.5.1.2.3 Data center replication is available for NAS based storage, to provide agencies with an alternative storage site, where required.
- 8.5.1.3 The State of Maine offsite storage location is contracted out to a professional offsite service company (Iron Mountain).
 - 8.5.1.3.1 As required by statute, agencies conduct inspections of the vendor site to ensure that appropriate security safeguards are implemented.
- 8.5.2 Agencies must ensure that any required alternative site is geographically separated from the primary site, to reduce susceptibility to threats (e.g., natural disasters or structural failures).
 - 8.5.2.1 The two OIT data centers are geographically separated.
 - 8.5.2.2 For OIT-hosted information assets, offsite storage and/or disaster recovery tapes are maintained and stored at an Iron Mountain facility, also geographically separated from the two OIT data centers.
- 8.5.3 Agencies, in collaboration with OIT, must identify potential access issues to any required alternate site in the event of a wide-area disruption (e.g., hurricane or regional power outage) or disaster and outline explicit mitigation actions.
 - 8.5.3.1 Access requirements of the OIT data centers in the event of a wide-area disruption are part of relevant OIT plans (e.g., contingency plan, incident response plan).

Contingency Planning Policy and Procedures (CP-1)

8.5.3.2 Access requirements of the offsite storage site in the event of a wide-area disruption are documented as part of the contractual agreement with the vendor (Iron Mountain).

8.5.3.2.1 The current vendor was chosen after reviewing the vendor's ability to meet safeguarding requirements.

8.5.3.2.2 The access requirements are determined and reviewed during contract renewals or requests for proposals.

8.5.3.2.3 OIT has the right to negotiate contract terms and conditions with the information technology rider of the contract.

8.5.3.2.4 Audits of the offsite location are done by the State of Maine to ensure the necessary safeguards are maintained at the required level.

8.6 Alternative Processing Site (CP-7 including CE-1, CE-2, CE-3):

8.6.1 Agencies must determine which agency information assets require an alternative processing site.

8.6.1.1 Agencies consult with OIT to establish alternative processing sites, to meet identified business and/or regulatory requirements, for agency information assets. The actual action-items will differ between OIT-hosting and remote-hosting.

8.6.1.2 The Office of Information Technology manages two data centers, with equivalent security safeguards, that are available for agencies to utilize as primary and alternative processing sites, for OIT-hosted information assets.

8.6.1.2.1 Agencies collaborate with OIT to establish necessary agreements to permit the transfer and resumption of information asset operations for essential missions/business functions within the time period specified when the primary processing capabilities are unavailable; and

8.6.1.2.2 Ensure that equipment and supplies required to transfer and resume operations are available at the alternative processing site or contracts are in place to support delivery to the site within the organizationally defined time period for transfer/resumption.

Contingency Planning Policy and Procedures (CP-1)

8.6.2 Agencies must, in collaboration with OIT, ensure that the alternative processing site is geographically separated from the primary site, to reduce susceptibility to threats (e.g., natural disasters or structural failures).

8.6.2.1 The OIT data centers are geographically separated.

8.6.3 Agencies, in collaboration with OIT, must identify potential access issues to the alternate processing site in the event of a wide-area disruption (e.g., hurricane or regional power outage) or disaster and outline explicit mitigation actions.

8.6.3.1 OIT is responsible for disaster recovery of the OIT data centers. Information asset restoration order priority (based on criteria established by the Governor's Office) in the event of a disaster is as follows:

8.6.3.1.1 Essential communications

8.6.3.1.2 Citizen health and safety

8.6.3.1.3 Direct citizen services

8.6.3.1.4 State revenue

8.6.3.1.5 Economic development

8.6.3.1.6 Routine government services

8.6.3.2 Agencies collaborate with OIT to develop any required alternative processing site agreements that contain priority-of-service provisions in accordance with the organizational availability requirements (including recovery time objectives).

8.7 Telecommunications Services (CP-8 including CE-2):

8.7.1 The Office of Information Technology (OIT) works with agencies and vendors to implement required agency-identified telecommunications services to:

8.7.1.1 Ensure an alternative telecommunications service level agreement (SLA) is in place to permit resumption of agency system recovery time objective (RTO) and business function maximum tolerable downtime (MTD) (as part of a formal agency business impact analysis (BIA)).

8.7.1.1.1 The agency system owner defines a resumption time period consistent with the RTOs and business impact analysis. The time period is approved by the agency business owner.

Contingency Planning Policy and Procedures (CP-1)

8.7.2 The Office of Information Technology obtains alternative telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

8.7.2.1 The Office of Information Technology Network Services maintains two (2) physically and logically diverse paths to the servicing internet service provider (ISP), and local and long-distance telephone providers.

8.8 Information System Backup (CP-9 including CE-1):

8.8.1 For OIT-hosted information assets, the Office of Information Technology (OIT), in conjunction with agencies:

8.8.1.1 Conducts Commvault backups of user-level information contained in the information asset, where requested, in accordance with the agency-defined required frequency for agency information assets. Defaults are specified below:

8.8.1.1.1 Performs full backups weekly to separate media.

8.8.1.1.2 Performs incremental or differential backups daily to separate media.

8.8.1.1.3 Ensures backups include user-level and system-level information (including system state information).

8.8.1.1.4 Stores three generations of backups (full as well as related incremental or differential backups) offsite.

8.8.1.1.5 Logs off-site and on-site backups with the name, date, time, and action.

8.8.1.2 Conducts Commvault backups of system-level information contained in the information asset in accordance with the agency-defined required frequency for agency information assets. Defaults are specified above.

8.8.1.3 Conducts Commvault backups of information asset documentation, including security-related documentation, consistent with agency-defined *recovery time objectives* and *recovery point objectives*.

8.8.1.4 Protects the confidentiality, integrity, and availability of backup information at OIT storage locations.

Contingency Planning Policy and Procedures (CP-1)

8.8.1.4.1 OIT stores backup tapes at a secure location within OIT data centers.

8.8.1.5 The Office of Information Technology tests backup information following each backup to verify media reliability and information integrity, minimally on an annual basis.

8.9 Information System Recovery and Reconstitution (CP-10 including CE-2):

8.9.1 For OIT-hosted information assets, the Office of Information Technology (OIT), in collaboration with agencies, implements the agency-defined system recovery and reconstitution requirements for agency information assets:

8.9.1.1 Provides for the recovery and reconstitution of the information asset to a known state after a disruption, compromise, or failure, consistent with agency-defined requirements.

8.9.1.1.1 OIT Information Asset Owners implement transaction recovery for transaction-based systems (e.g., employing transaction rollback and transaction journaling mechanisms) to meet agency-defined requirements for the information assets that they manage.

8.9.1.1.2 OIT Information Asset Owners implement application-level exception handling to rollback transactions that are flagged as identified exceptions to meet agency defined requirements for the applications that OIT manages. Exceptions may result from a technical problem or a business rule data conflict.

8.9.2 For remote-hosted information assets, the agencies, in collaboration with the OIT Vendor Management Office, implements the agency-defined system recovery and reconstitution requirements for agency information assets.

9.0 Document History and Distribution:

Version	Revision Log	Date
<i>Version 1.0</i>	<i>Initial Publication</i>	<i>August 23, 2019</i>

Approved by: Chief Information Officer, OIT.

Contingency Planning Policy and Procedures (CP-1)

Legal Citation: [Title 5, Chapter 163: Office of Information Technology](#)².

Waiver Process: [See the Waiver Policy](#)³.

Distribution:

This document will be distributed to all appropriate State of Maine personnel and will be posted on the OIT website (<https://www.maine.gov/oit/policies>).

10.0 Document Review:

This document is to be reviewed annually and when substantive changes are made to policies, procedures or other authoritative regulations affecting this document.

11.0 Records Management:

Office of Information Technology security policies, plans, and procedures fall under the *Routine Administrative Policies and Procedures and Internal Control Policies and Directives* records management categories. They will be retained for three (3) years and then destroyed in accordance with guidance provided by Maine State Archives. Retention of these documents will be subject to any future State Archives General Schedule revisions that cover these categories.

12.0 Public Records Exceptions:

Under the Maine Freedom of Access Act, certain public records exceptions may limit disclosure of agency records related to information technology infrastructure and systems, as well as security plans, procedures or risk assessments. Information contained in these records may be disclosed to the Legislature or, in the case of a political or administrative subdivision, to municipal officials or board members under conditions that protect the information from further disclosure. Any aggrieved person seeking relief for an alleged violation of the FOAA may bring suit in any Superior Court in the state.

13.0 Definitions:

13.1 **Business Impact Analysis (BIA):** A process that identifies and evaluates the potential effects (financial, life/safety, regulatory, legal/contractual, reputation and so forth) of natural and man-made events on business operations.

13.2 **Business Continuity Plan (BCP):** A broad disaster recovery approach whereby enterprises plan for recovery of the entire business process. This includes a plan for workspaces, telephones, workstations, servers,

² <http://legislature.maine.gov/statutes/5/title5ch163sec0.html>

³ <http://www.maine.gov/oit/policies/waiver.pdf>

Contingency Planning Policy and Procedures (CP-1)

applications, network connections and any other resources required in the business process.

- 13.3 **Continuity of Operations (COO):** Ongoing process to ensure that necessary steps are taken to identify the impact of potential losses and maintain viable recovery strategies, recovery plans, and continuity of services.
- 13.4 **Contingency Plan (CP):** Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disasters. Contingency planning is a component of continuity of operations, disaster recovery, and *risk management*.
- 13.5 **Disaster Recovery (DR):** The technical aspect of business continuity. The collection of resources and activities to re-establish Information Technology services (including components such as infrastructure, telecommunications, systems, applications and data) at an alternate site following a disruption. Disaster recovery includes subsequent resumption and restoration of operations at a more permanent site. Note: DR does *not* have to occur at an alternate site if the current location is still suitable for DR procedures, but this is not typical.
- 13.6 **Information Asset:** Used interchangeably with **Information System**. A discrete, identifiable piece of information technology, including hardware, software, and firmware. Information assets include, for example, mainframes, workstations, servers (e.g., database, electronic mail, authentication, web, proxy, file, domain name), input/output devices (e.g., scanners, copiers, printers), network components (e.g., firewalls, routers, gateways, voice and data switches, process controllers, wireless access points, network appliances, sensors), operating systems, virtual machines, middleware, business applications, system software, development tools, and miscellaneous related utilities.
- 13.7 **Maximum Tolerable Downtime (MTD):** Represents the total amount of time the system owner/authorizing official is willing to accept for a mission/business process outage or disruption and includes all impact considerations. Determining MTD is important because it could leave contingency planners with imprecise direction on (1) selection of an appropriate recovery method, and (2) the depth of detail which will be required when developing recovery procedures, including their scope and content.
- 13.8 **Recovery Point Objective (RPO):** The point in time to which data must be recovered after an outage.

Contingency Planning Policy and Procedures (CP-1)

- 13.9 **Recovery Time Objective (RTO):** The overall length of time an information system's components can be in the recovery phase before negatively impacting the organization's mission or mission/business processes.
- 13.10 **Risk Management (RM):** The identification, evaluation, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability or impact of unfortunate events or to maximize the realization of opportunities.
- 13.11 **Standard:** A collection of specific (technical and/or procedural) requirements that must be adhered to.