Division of Enterprise Technology Strategy and Services

ETSS Policy 100.6

Contingency Planning Policy (CP)

Publish Date: 23 June 2026
Effective Date: 23 June 2026
Last Review: 22 June 2026

doa.entsec@doit.ri.gov

1. Purpose

This policy establishes the requirements for contingency planning across State of Rhode Island information systems. Contingency planning enables the restoration and continuity of operations of mission-critical assets and business functions following a disruption, compromise, or failure. This policy defines requirements for contingency plan development, testing, and training, system backup and recovery, and the establishment of alternate storage, processing, and telecommunications capabilities.

This policy supports the State's compliance with NIST SP 800-53 Revision 5 (Contingency Planning family), NIST Cybersecurity Framework 2.0, IRS Publication 1075, and other applicable federal and state regulatory requirements.

2. Applicability

This policy applies to all State of Rhode Island Executive Branch departments, including agencies, boards, and commissions, as well as their employees (permanent, non-permanent, full-time, and part-time), interns, consultants, contractors, vendors, and any entity that has access to State information systems and data, whether operated or maintained by the State or on behalf of the State. For the purposes of this policy, the term "Agency" refers to any department, agency, division, or unit of the Executive Branch.

This policy applies to all information systems that support essential mission and business functions, including enterprise-managed, agency-managed, cloud-hosted, and hybrid environments. For cloud environments, the system owner is responsible for determining which elements of the cloud environment require compliance with each control.

3. Roles and Responsibilities

3.1. Chief Technology Officer (CTO)

Designated as the official responsible for the enterprise Contingency Planning policy and procedures. Oversees infrastructure and operations teams responsible for enterprise backup, recovery, and alternate site operations.

3.2. Chief Information Security Officer (CISO)

Supports reviews and approval of contingency plans. Ensures that contingency planning activities are coordinated with incident response capabilities. Provides security oversight of alternate site controls and backup cryptographic protections.

3.3. Enterprise Platform Architecture / Disaster Recovery Lead

Responsible for establishing and maintaining alternate storage and processing sites, managing disaster recovery infrastructure, coordinating alternate telecommunications services, and leading enterprise-level contingency plan testing and disaster recovery exercises.

3.4. System Owners

Responsible for developing, maintaining, and testing contingency plans for their information systems. Define RTOs, RPOs, and maximum allowable downtimes in coordination with business owners. Identify critical assets and ensure backup procedures meet recovery objectives. For cloud environments, determine which elements require compliance with each control.

3.5. Agency Information Managers (AIMs) / Technical Support Managers (TSMs)

Coordinate contingency planning activities at the agency level. Support contingency plan testing and execution. Receive distribution of contingency plans and updates. Serve as liaison between agency leadership and ETSS for continuity operations.

3.6. Business Process Owners

Define the maximum allowable downtime and recovery requirements for essential mission and business functions. Provide input into contingency plan development, review, and prioritization of restoration activities.

3.7. All Contingency Personnel

Responsible for completing contingency training within required timelines, participating in contingency plan tests and exercises, and executing assigned contingency roles during activation events.

4. Procedures for Compliance

The following requirements establish the contingency planning controls that agencies and ETSS must implement. Security controls are assigned based on the Information Assurance Level (IAL) of the information system, aligned to the NIST SP 800-53 Rev. 5 Moderate baseline.

4.1 Contingency Planning Policy and Procedures (CP-1)

Applies to: All systems (IAL1, IAL2)

Each agency shall develop, document, and disseminate a contingency planning policy and supporting procedures to designated personnel identified in the applicable System Security Plan. The ETSS Chief Technology Officer (CTO) is designated as the official responsible for the enterprise contingency planning policy and procedures. The policy shall be reviewed and updated at least every three (3) years and following significant changes to technologies, regulatory requirements, or the threat environment. Supporting procedures shall be reviewed in alignment with the policy.

4.2 Contingency Plan (CP-2)

Applies to: All systems (IAL1, IAL2)

Each agency shall:

a. Develop a contingency plan for the information system as part of an overall program for achieving continuity of operations that: (1) identifies essential mission and business functions and associated contingency requirements; (2) provides recovery objectives, restoration priorities, and associated metrics including RTO and RPO; (3) indicates contingency roles, responsibilities, and individuals assigned to contingency roles with contact information; (4) addresses maintaining essential mission and business functions despite a disruption, compromise, or failure; (5) addresses full information system restoration without weakening planned or existing safeguards; and (6) is reviewed and approved by the information system owner, data owner, business process owner, and ETSS CTO, CISO, or delegate.

b. Distribute the contingency plan to key contingency personnel identified by name and role, as defined by the system owner.

c. Coordinate contingency planning activities with incident handling activities.

d. Review the contingency plan at least annually.

e. Update the contingency plan to address changes to the agency, information system, operational environment, or issues identified during plan implementation, testing, or execution.

f. Communicate contingency plan changes to key contingency personnel.

g. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into subsequent contingency testing and training.

h. Protect the contingency plan from unauthorized disclosure or modification.

4.2.1 Coordinate with Related Plans (CP-2(1))

Applies to: Moderate and above (IAL2)

Each agency shall coordinate contingency plan development and testing with personnel responsible for related plans, including disaster recovery planning, continuity of operations planning, and incident response planning.

4.2.2 Resume Mission and Business Functions (CP-2(3))

Applies to: Moderate and above (IAL2)

Each agency shall plan for the resumption of essential mission and business functions within the maximum allowable downtime, as determined by the business owner, of contingency plan activation.

4.2.3 Identify Critical Assets (CP-2(8))

Applies to: Moderate and above (IAL2)

Each agency shall identify critical information system technical and operational assets (including services, system components, mechanisms, procedures, and personnel) supporting essential mission and business functions.

4.3 Contingency Training (CP-3)

Applies to: All systems (IAL1, IAL2)

Each agency shall:

a. Provide contingency training to all personnel assigned contingency roles and responsibilities within three (3) months of being assigned a contingency role, annually thereafter as refresher training, and whenever the information system undergoes a significant change.

b. Review and update contingency training content every three (3) years and following significant information system changes. Training content shall reflect the continuity requirements identified in the contingency plan.

4.4 Contingency Plan Testing (CP-4)

Applies to: All systems (IAL1, IAL2)

Each agency shall:

a. Test the contingency plan at least annually based on the continuity requirements of the plan to determine its effectiveness and agency readiness to execute the plan. Contingency tests and exercises may include checklists, walk-throughs, tabletop exercises, simulations, and comprehensive tests (including disaster recovery testing). The type and rigor of testing shall be commensurate with the criticality and IAL of the information system.

b. Review the results of contingency plan tests and document an after-action report to identify improvements to existing processes, procedures, and policies.

c. Initiate corrective actions as required based on test results.

4.4.1 Coordinate with Related Plans (CP-4(1))

Applies to: Moderate and above (IAL2)

Each agency shall coordinate contingency plan testing with personnel responsible for related plans, including disaster recovery, continuity of operations, and incident response planning.

4.5 Alternate Storage Site (CP-6)

Applies to: Moderate and above (IAL2)

Each agency shall:

a. Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information. Alternate storage site agreements shall specify access rules, physical and environmental conditions and protection requirements, and coordination of delivery and retrieval of backup media. ETSS maintains an enterprise-managed warm-site alternate storage and processing facility located out of state on the east coast to support recovery of essential mission and business functions.

b. Ensure that information security safeguards at the alternate storage site are equivalent to those at the primary storage site. All assets at the alternate site fall under the same controls defined in the enterprise System Security Plan and ETSS security program.

4.5.1 Separation from Primary Site (CP-6(1))

Applies to: Moderate and above (IAL2)

Each agency shall identify an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats. The enterprise alternate recovery site is in Pennsylvania, sufficiently distanced to mitigate shared disaster or outage risk with the ETSS Rhode Island-located data centers.

4.5.2 Accessibility (CP-6(3))

Applies to: Moderate and above (IAL2)

Each agency shall identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption (such as a hurricane or regional power outage) and outline explicit mitigation actions that will allow for the retrieval of backup information. Accessibility is validated as part of annual disaster recovery testing.

4.6 Alternate Processing Site (CP-7)

Applies to: Moderate and above (IAL2)

Each agency shall:

a. Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of all ETSS-managed information system operations within timeframes consistent with defined RTOs and RPOs when primary processing capabilities are unavailable. The agency is responsible for identifying information systems critical to continuity of operations. Alternate processing site agreements shall identify physical and environmental protection requirements, access rules, and coordination of delivery and retrieval of backup media.

b. Ensure equipment and supplies required to transfer and resume operations are available at the alternate processing site, or that contracts are in place to support delivery to the site within the defined recovery timeframes.

c. Ensure that information security safeguards at the alternate processing site are equivalent to those at the primary processing site.

4.6.1 Separation from Primary Site (CP-7(1))

Applies to: Moderate and above (IAL2)

Each agency shall identify an alternate processing site that is physically separate from the primary site to reduce the risk from the same threats.

4.6.2 Accessibility (CP-7(2))

Applies to: Moderate and above (IAL2)

Each agency shall identify potential accessibility problems with the alternate processing site in the event of an area-wide disruption and outline mitigation procedures that will allow for access to the site.

4.6.3 Priority of Service (CP-7(3))

Applies to: Moderate and above (IAL2)

Each agency shall develop alternate processing site agreements that prioritize services in accordance with availability requirements, RTOs, RPOs, and the criticality of the system. SLAs and contracting for the alternate site shall consider ETSS required controls to replicate the primary environment.

4.7 Telecommunications Services (CP-8)

Applies to: Moderate and above (IAL2)

Each agency shall establish alternate telecommunications services (including voice and data) and associated agreements to permit the resumption of information system operations for essential agency mission and business functions, including constituent services call center operations, within defined RTOs and RPOs when primary telecommunications capabilities are unavailable. The system owner shall define a resumption time consistent with recovery time objectives and business impact analysis.

4.7.1 Priority of Service Provisions (CP-8(1))

Applies to: Moderate and above (IAL2)

Each agency shall:

a. Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with availability requirements and recovery time objectives.

b. Request Telecommunications Service Priority for all telecommunications service users for security emergency preparedness if primary or alternate telecommunications services are provided by a common carrier.

4.7.2 Single Points of Failure (CP-8(2))

Applies to: Moderate and above (IAL2)

Each agency shall obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

4.8 System Backup (CP-9)

Applies to: All systems (IAL1, IAL2)

Each agency shall:

a. Perform backups of user-level information maintained on the information system in a manner consistent with contingency plan RTO and RPO, but no less than weekly.

b. Perform backups of system-level information maintained on the information system in a manner consistent with contingency plan RTO and RPO, but no less than weekly.

c. Perform backups of information system documentation, including security and privacy-related documentation, within the frequency defined in the applicable System Security Plan in a manner consistent with contingency plan RTO and RPO.

d. Protect the confidentiality, integrity, and availability of backup information.

4.8.1 Testing for Reliability and Integrity (CP-9(1))

Applies to: Moderate and above (IAL2)

Each agency shall periodically test backups to ensure reliability of the media and integrity of the information. Data deemed to be critical to maintain agency mission and business functions, for both on-premises and cloud environments, shall be tested no less than quarterly. Remaining backup information shall be tested at least annually.

4.8.2 Cryptographic Protection (CP-9(8))

Applies to: Moderate and above (IAL2)

Each agency shall implement FIPS 140-2 or FIPS 140-3 validated cryptographic mechanisms to prevent unauthorized disclosure and modification of classified and sensitive data, including PII and FTI, within backup information.

4.9 System Recovery and Reconstitution (CP-10)

Applies to: All systems (IAL1, IAL2)

Each agency shall provide for the recovery of essential mission and business functions

and reconstitution of the information system to a known state within the RTO and RPO identified in the system contingency plan after a disruption, compromise, or failure. Recovery and reconstitution activities include resetting system parameters, reinstalling patches, reestablishing configuration settings, reinstalling application and system software, and fully testing the information system.

4.9.1 Transaction Recovery (CP-10(2))

Applies to: Moderate and above (IAL2)

For systems that are transaction-based (such as database management systems and transaction processing systems), the information system shall implement transaction recovery mechanisms, including transaction rollback and transaction journaling.

5. Repercussions for Non-Compliance

Failure to comply with this policy may result in corrective action proportional to the severity of the violation. Consequences may include, but are not limited to:

a. Mandatory remediation of contingency plan deficiencies within defined timelines.

b. Formal counseling or written reprimand for failure to maintain or test contingency plans.

c. Referral to agency management for disciplinary proceedings.

d. Denial of system authorization (Authority to Operate) for systems that do not have a current, tested contingency plan.

e. Escalation to ETSS leadership and the CDO for systemic non-compliance affecting enterprise continuity posture.

Non-compliance findings shall be documented and tracked through ETSS governance processes and may be recorded as findings in the agency Plan of Action and Milestones (POAM).

6. Approval / Review Signatures

Sanjay Gupta
Digitally signed by Sanjay Gupta
Date: 2026.06.22 16:35:47 -04'00'

Chief Technology Officer (CTO)
Division of Enterprise Technology Strategy and Services (ETSS)

Brian Tardiff
Digitally signed by Brian Tardiff
Date: 2026.06.23 08:35:06 -04'00'

Chief Digital Officer (CDO)
Division of Enterprise Technology Strategy and Services (ETSS)