1. Purpose

Establish policy for effective contingency planning that enables the restoration and continuity of operations of mission-critical assets and business functions.

2. Applicability

This policy is applicable to all State of Rhode Island Executive Branch Departments¹ (including agencies, boards and commissions), and their employees (including permanent, non-permanent, full-time, and part-time) and interns, consultants, contractors, vendors, contracted individuals, and any entity having access to state information systems and data, whether operated or maintained by the state or on behalf of the state. For this policy, the term "agency" is used to refer to any department, agency, division, or unit of the Executive branch of the State of Rhode Island.

3. Definitions

Alternate Processing Site
A processing site that reflects the continuity of operation requirements of essential mission and business functions identified in the contingency plan to ensure that essential mission and business functions are reconstituted after a disruption, compromise, or failure.

Alternate Storage Site
A storage site that is geographically distinct from the primary storage site that maintains duplicate copies of information and data.

Contingency Plan
A planned course of action designed to effectively respond to information system disruptions, compromises, or failures and restore continuity of operation of essential mission and business functions. Contingency planning is related to other risk management activities, including business continuity, disaster recovery, continuity of operations, critical infrastructure, incident response, occupant emergency planning.

¹ State of Rhode Island Executive Branch Departments does not include the University of Rhode Island, the State Colleges, the General Treasurer, the Attorney General, or the Secretary of State.
4. Procedures for Compliance

Security controls in this policy will be implemented in accordance with the security categorization of the information system. The security categorization is based on the Information Assurance Level (IAL) requirements of the information system.

Low Risk Systems (IAL1)
Information systems that only contain data that is public by law or directly available to the public via mechanisms such as the internet. In addition, desktops, laptops, and supporting systems used by agencies are Low Risk unless they store, process, transfer, or communicate private or sensitive data.

Moderate Risk Systems (IAL2)
Information systems that store, process, transfer, or communicate private or sensitive data or have a direct dependency on a Moderate system. At a minimum, any information system that stores, processes, transfers, or communicates PII or other sensitive data types is classified as a Moderate system.

4.1. [IAL1, IAL2] Contingency Planning Policy and Procedures (CP-1). The agency will develop, document, disseminate, review, and annually update a contingency planning policy and procedures.

4.2. [IAL1, IAL2] Contingency Plan (CP-2). The agency will (i) develop a contingency plan for the information system as part of an overall program for achieving continuity of operations of its mission and business functions, (ii) review and update, as required, the contingency plan on an annual basis and after a change to the agency, information system, operational environment, or due to issues that arise from contingency planning testing or execution, (iii) distribute the contingency plan to key contingency personnel (individuals assigned contingency roles and responsibilities) initially and after an update, (iv) coordinate contingency planning activities with incident handling activities, and (v) protect the contingency plan from unauthorized disclosure or modification. Contingency plans should:

- Identify essential mission and business functions and associated contingency requirements.
- Provide recovery objectives, restoration priorities, and associated metrics.
- Indicate contingency roles, responsibilities, and individuals assigned to contingency roles, including contact information.
- Address maintaining essential mission and business functions despite an information system disruption, compromise, or failure.
- Address full information system restoration without weakening planned or existing safeguards.
- Be reviewed and approved by appropriate personnel, including the information system owner, data owner, business process owner, and ETSS CISO.
4.2.1. [IAL2] Coordinate with Related Plans (CP-2.1). The agency will coordinate contingency plan testing with personnel responsible for plans related to other agency or enterprise risk management planning.

4.2.2. [IAL2] Resume Essential Mission and Business Functions (CP-2.3). The agency will plan for the resumption of essential mission and business functions within two (2) hours of contingency plan activation.

4.2.3. [IAL2] Identify Critical Assets (CP-2.8). The agency will identify critical information system technical and operational assets (e.g. services, system components, mechanisms, procedures, personnel) supporting essential mission and business functions.

4.3. [IAL1, IAL2] Contingency Training (CP-3). The agency will 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. Contingency training should reflect the continuity requirements identified in the contingency plan.

4.4. [IAL1, IAL2] Contingency Plan Testing (CP-4). The agency will (i) test the contingency plan annually based on the continuity requirements of the plan to determine its effectiveness and agency readiness to execute the plan, (ii) review the results of contingency plan tests, and (iii) initiate corrective actions, as required. The following provides a sample (not all-inclusive) list of contingency tests and exercises:

   **Checklist**
   A document that identifies activities relevant to contingency planning. Checklists are useful for system owners, executive management, and project managers to verify whether a checklist activity was performed (“yes” or “no”). Checklists are best suited only to ensure that relevant contingency planning activities were performed and are not an appropriate substitute for more thorough contingency plan tests and exercises.

   **Walk-Through**
   A verbal review of the contingency plan to ensure its completeness and identity gaps within roles, responsibilities, and high-level controls of the plan. Walk-throughs are best suited for every-other-year reviews of IAL1 and low risk IAL2 information systems where the contingency plan has not changed.

   **Table Top Exercise**
   A classroom-based discussion where a test facilitator presents a scenario (e.g. emergency, disaster) to contingency plan individuals assigned contingency roles and responsibilities for the purpose of discussing coordination, recovery, and decision-making activities. Table top exercises assess readiness and response capabilities of contingency plan teams responsible for IAL1 or IAL2 information systems.
Simulation
Similar to a table top exercise, except that the scenario (e.g. disaster, emergency) is simulated on an information system to test various aspects of contingency recovery objectives and restoration priorities (e.g. information system restoration, data reconstruction, network connectivity) associated with the scenario. Simulations may be used to test the contingency response for any information system, although costs associated with simulations likely relegate them to high risk IAL2 information systems.

Comprehensive Test
Test end-to-end functionality or recovery aspects of transactions, applications, network connectivity, system interdependencies, or other components of the information system in accordance with contingency plan requirements. Disaster recovery testing is one type of comprehensive test. Comprehensive tests should be performed at primary and alternate sites with individuals assigned contingency roles and responsibilities. Comprehensive tests should be periodically conducted for all high risk IAL2 information systems.

4.4.1. [IAL2] Coordinate with Related Plans (CP-4.1). The agency will coordinate contingency plan testing with personnel responsible for plans related to other agency or enterprise risk management planning.

4.5. [IAL2] Alternate Storage Site (CP-6). The agency will establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information, and ensure that information security safeguards at the alternate storage site are equivalent to those at the primary storage site. Alternate storage site agreements should specify access rules, physical and environmental conditions and protection requirements, and coordination of delivery/retrieval of backup media.

4.5.1. [IAL2] Separation from Primate Site (CP-6.1). The agency will identify an alternate storage site that is physically separate from the primary storage site to reduce the risk from the same threats.

4.5.2. [IAL2] Accessibility (CP-6.3). The agency will identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption (e.g. hurricane, regional power outage) and outlines mitigation procedures that will allow for the retrieval of backup information at the alternate storage site.

4.6. [IAL2] Alternate Processing Site (CP-7). The agency will establish an alternate processing site, including necessary agreements to permit the transfer and resumption of information system operations, and ensure that equipment and supplies required to transfer and resume operations are available at the alternate processing site (or contracts are in place to support delivery to the site) within 12 hours for transfer/resumption. The agency will ensure that information security safeguards at the alternate process site are equivalent to those at the primary processing site. Alternate processing site agreements should identify physical and environmental protection requirements, access rules, and coordination of delivery and retrieval of backup media.
4.6.1. [IAL2] Separation from Primate Site (CP-7.1). The agency will identify an alternate processing site that is physically separate from the primary storage site to reduce the risk from the same threats.

4.6.2. [IAL2] Accessibility (CP-7.2). The agency will identify potential accessibility problems to the alternate processing site in the event of an area-side disruption (e.g. hurricane, regional power outage) and outlines mitigation procedures that will allow for access to the alternate processing site.

4.6.3. [IAL2] Priority of Service (CP-7.3). The agency will develop alternate processing site agreements that prioritize services in accordance with availability requirements and recovery time objectives.

4.7. [IAL2] Telecommunications Services (CP-8). The agency will establish alternate telecommunications services (voice and data) and associated agreements to permit for the resumption of information system operations for essential agency mission and business functions within two (2) days when primary telecommunications capabilities are unavailable at either the primary or alternate storage or processing sites.

4.7.1. [IAL2] Priority of Service Provisions (CP-8.1). The agency will develop primary and alternate telecommunications service agreements that contain priority-of-service provisions.

4.7.2. [IAL2] Single Points of Failure (CP-8.2). The agency will obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

4.8. [IAL1, IAL2] Information System Backup (CP-9). The agency will perform backups of user-level and system-level information, as well as information system and security-related documentation, in a manner consistent with contingency plan recovery time and recovery point objectives, but no less than weekly. The agency will protect the confidentiality, integrity, and availability of backup information at storage locations.

4.8.1. [IAL2] Testing for Reliability/Testing (CP-9.1). The agency will periodically test backups to ensure reliability of the media and integrity of the information. Data deemed critical to maintaining agency mission and business functions will be tested no less than quarterly.

4.9. [IAL1, IAL2] Information System Recovery and Reconstitution (CP-10). The agency will provide for the recovery of essential mission and business functions and reconstitution of the information system to a known state after a disruption, compromise, or failure.

4.9.1. [IAL2] Transaction Recovery (CP-10.2). For systems that are transaction-based (e.g. database management systems, transaction processing systems), the
information system will implement traction recovery (e.g. transaction rollback, transaction journaling).

5. Approval / Review Signature:

Brian Tardiff  
Digitally signed by Brian Tardiff  
Date: 2020.09.14 08:40:48 -04'00'

Chief Information Security Officer