GOVERNANCE

This document is governed by the IT Governance policy which provides the following guidance:

a. Roles and Responsibilities
b. Policy Control Application
c. Policy Compliance Requirements
d. Policy Exceptions and Exemptions
e. Policy Reviews and Updates

SCOPE

This policy covers all State information and systems used, managed, or operated by a contractor, agency, or other organization on behalf of the State. This policy applies to all State employees, contractors, and all other users of State information and systems supporting the operation and assets of the State.

All information assets that process, store, receive, transmit or otherwise impact the confidentiality, integrity, and accessibility of State data must meet the required security controls defined in this policy and based on the National Institute of Standards and Technology (NIST) SP 800-53 r5, Security and Privacy Controls.

APPLICABILITY

This document addresses the requirements set forth by the State to implement the family of Contingency Planning security controls at the organization, process and/or system level for all information assets / State data and provides requirements for the identification and authentication process to assure information systems are designed and configured using controls sufficient to safeguard the State's systems and data.

CP-1 POLICY AND PROCEDURES

The State has adopted the Contingency Planning security principles established in NIST SP 800-53, "Contingency Planning" control guidelines as the official policy for this security domain. The "CP" designator identified in each control represents the NIST-specified identifier for the Contingency Planning control family. A designator followed by a number in parenthesis indicates a control enhancement that provides statements of security and privacy capability that augment a base control. Only those control enhancements associated with the moderate level controls are listed. Should an executive-branch agency be required to address other control enhancements for a control item, the organization will be responsible for writing an additional policy to meet that requirement.

The State and executive-branch agencies shall develop, adopt, and adhere to formal, documented contingency planning procedures addressing purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

The State shall implement and maintain appropriate planning and testing processes ensuring critical production environments can be recovered and sustained to meet State business requirements during or after a significant business interruption.

Coordination shall be required between the Office of Information Technology (OIT) and executive-branch agencies.

The following subsections in this document outline the Contingency Planning requirements each agency must implement and maintain to remain compliant with this policy. This policy and associated procedures shall be reviewed and updated at least every three (3) years or following State-defined events requiring review and updates.

CP-2 CONTINGENCY PLAN

A contingency plan shall be developed for the recovery of State information assets from availability threats including, but not limited to, natural disasters, accidents, malicious destruction, equipment failure, and denial of services.

Management shall coordinate contingency plan development with organizational elements responsible for formally documenting the Business Continuity and Disaster Recovery (BC/DR) Plan covering critical applications. This should include procedures or references used for system recovery.

Plans shall:

a. Be developed prior to implementation as part of the development life cycle for technology development or deployment by the State to address all production processing environments and assets;
b. Identify essential mission and business functions and their contingency requirements;
c. Provide recovery time and recovery point objectives, restoration priorities, and estimate the following downtime factors as a result of a disruptive event:
    i. **Maximum Tolerable Downtime (MTD) - The amount of time vital business processes or mission essential functions can be disrupted without causing significant harm to the organization's mission;**
    ii. **Recovery Time Objective (RTO) - The duration of time and a service level within which systems, applications, or functions must be restored after an outage to the predetermined Recovery Point Objective (RPO); and**
    iii. **Recovery Point Objective (RPO) - The RPO represents the point in time, prior to a disruption or system outage, to which business processes or mission essential functions and supporting application data shall be recovered.**
d. Identify roles, responsibilities, and assigned individuals with contact information;
e. Address full information asset restoration without deterioration of original security measures;
f. Address the sharing of contingency information;
g. Be reviewed and approved by agency or department heads;
h. Be distributed to relevant system owners and stakeholders;
i. Coordinate contingency planning activities with incident handling activities;
j. Be revised to address changes to the organization, information asset, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;
k. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into the contingency plan;
l. Protect the contingency plan from unauthorized disclosure and modification;
m. Address the protection of the health and safety of State employees;
n. Address protection of State assets and minimize financial, reputational, legal and/or regulatory exposure;

o. Create crisis teams and response plans for threats and incidents;
p. Require employees to be aware of their roles and responsibilities in the BC/DR Plan and its execution via training and awareness programs;
q. Coordination with Contingency Plan Administrators and the Operations Team must occur for all potential outages that may result in a failover or recovery situation;
r. Be reviewed and submitted to the OIT management at least annually;
s. Support the resumption of vital business processes or mission essential functions within the agency-defined period of contingency plan activation;
t. Define the period for resumption of essential mission/business functions dependent on the severity/extent of disruptions to the information system and its supporting infrastructure; and
u. Define within the contingency plan and Business Impact Analysis (BIA) the period in which the system needs to be operational to support essential mission and business functions.

CP-2 (1) CONTINGENCY PLAN – COORDINATE WITH RELATED PLANS

Plans that are related to contingency plans include Business Continuity Plans, Disaster Recovery Plans, Critical Infrastructure Plans, Continuity of Operations Plans, Crisis Communications Plans, Insider Threat Implementation Plans, Data Breach Response Plans, Cyber Incident Response Plans, Breach Response Plans, and Occupant Emergency Plans.

The State and executive-branch agencies with Statewide and Departmental Critical systems shall provide disaster recovery capabilities to ensure timely recovery and service restoration as part of their disaster recovery strategy.

Agencies shall coordinate contingency plan development and execution with the State and agency divisions and groups responsible for related plans.

CP-2 (3) CONTINGENCY PLAN – RESUME MISSION AND BUSINESS FUNCTIONS

This control may be conducted as part of business continuity planning or as part of business impact analyses. Organizations will prioritize the resumption of business functions, but the period for resuming mission and business functions may be dependent on the severity and extent of the disruptions to the system and its supporting infrastructure.

CP-2 (8) CONTINGENCY PLAN – IDENTIFY CRITICAL ASSETS

The State and executive-branch agencies will identify critical system assets supporting essential mission and business functions.

Critical system assets include technical and operational aspects. Technical aspects include system components, information technology services, information technology products, and mechanisms. Operational aspects include procedures (i.e., manually executed operations) and personnel (i.e., individuals operating technical controls and/or executing manual procedures).

Application criticality is categorized as:

a. Statewide Critical;
b. Department Critical;
c. Program Critical; or
d. Noncritical.

CP-3 CONTINGENCY TRAINING

Training and awareness programs shall ensure the organization understands the roles of each individual when responding to a disaster and/or adverse situation. Contingency training content shall be reviewed and updated at least annually or after defined events necessitating change.

Contingency training shall be provided to information system users prior to assuming their contingency role/responsibilities, when required by system changes, and at least annually thereafter.

CP-4 CONTINGENCY PLAN TESTING

Contingency plan testing shall be coordinated with the State along with agency divisions and groups responsible for related plans. The State shall:

a. Develop test objectives and success criteria for Disaster Recovery and/or Restoration procedures;
b. Test and/or exercise the contingency plan for critical information assets at least annually to determine its effectiveness and organizational readiness to execute the plan;
c. Develop a contingency plan exercise After-Action Report; and
d. Initiate corrective actions to ensure the procedures are adequate to restore/recover critical application processes. Document corrective actions in an After-Action Report (AAR).

CP-6 ALTERNATE STORAGE SITE

Alternate storage shall be established for critical systems including necessary agreements to permit the storage and recovery of information asset backup information.

The following must be done:

a. Ensure the alternate storage site provides information security safeguards that meet the comparable protection standards of the primary site;
b. Establish a site location separate from the primary facility to ensure that risk disruption (e.g., natural disasters, structural failures, cyber-attacks) affecting both the primary and alternate site is low or otherwise is at an acceptable level, based on a risk assessment; and
c. Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions. Area-wide disruptions refer to those types of disruptions that are broad in geographic scope (e.g., hurricane, regional power outage, etc.) with such determinations made by the State based on agency assessments of risk.

CP-7 ALTERNATE PROCESSING SITE

The following must be done for alternate processing:

a. Establish an alternate processing site including necessary agreements to permit the resumption of information asset operations for mission essential functions or processes within defined RTOs/RPOs when primary processing capabilities are unavailable;
b. Alternate processing sites shall provide a Service Level Agreement (SLA) containing priority-of-service provisions in accordance with the information system's requirements in the event of a disruption or disaster;
c. Ensure equipment and supplies required to resume operations are available at the alternate site or contracts are in place to support site delivery in time to support the agency-defined period for transfer/resumption;

d. Ensure the alternate storage site provides information security safeguards comparable to the primary site;
e. The alternate processing site must be physically and logically separated from the primary processing site to reduce susceptibility to the same threats;
f. Identify potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster;
g. Outline and document explicit mitigation actions within the contingency plan; and
h. Develop alternate processing site agreements containing priority-of-service provisions.

CP-8 TELECOMMUNICATIONS SERVICES

The State shall:

a. Establish alternate telecommunications services with providers of communications transmission services to maintain readiness to respond and manage any event or crisis;
b. Ensure secondary communication transmission services have agreements for the resumption of information asset operations with defined recovery time and recovery points when primary telecommunications fail;
c. Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with agency availability requirements;
d. Request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier;
e. Consider the potential process/function impact in situations where telecommunications service providers are servicing other organizations with similar priority-of-service provisions; and
f. Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

CP-9 SYSTEM BACKUP

The following shall be done for system backups:

a. Backups of system documentation shall be performed with a frequency consistent with the defined Recovery Time Objective (RTO), and Recovery Point Objective (RPO); and
b. The confidentiality and integrity of backup information shall be protected at the highest level based on the highest classification of data contained in the system.

CP-9 (1) SYSTEM BACKUP – TESTING FOR RELIABILITY AND INTEGRITY

Backup information shall be tested quarterly to verify media or cloud storage reliability and data integrity.

CP-9 (8) SYSTEM BACKUP – CRYPTOGRAPHIC PROTECTION

Cryptographic mechanisms shall be implemented to prevent the unauthorized disclosure and modification of State backup information.

CP-10 SYSTEM RECOVERY AND RECONSTITUTION

The State shall:

a. Provide for the recovery and reconstitution of mission essential functions to a known state after a disruption, compromise, or failure within defined RTO and RPO objectives.
b. Applications categorized as Statewide and/or Agency Critical should have viable disaster recovery support, approval, budget, and be exercised per policy.
c. Ensure plan activations are documented and recorded, and post-activation reviews are conducted for plan effectiveness.
d. Update the plan(s) where necessary and provide a formal report to the State Secretary of Information Technology within 30 days of post-activation review.

POLICY OWNER

Secretary of Office of Information Technology (OIT)

MATERIAL SUPERSEDED

This current policy supersedes all previous versions. All State agencies and contractors/vendors of the State are expected to comply with the current implemented version.

REVISION HISTORY

Revision Date	Summary of Change
12/31/2024	Policy Update

REMAINDER OF PAGE LEFT INTENTIONALLY BLANK

APPROVED BY

Signature	Daniel Urquhart
Approved by	Daniel Urquhart
Title	Secretary of Office of Information Technology (OIT)
Date Approved	01/15/2025

REMAINDER OF PAGE LEFT INTENTIONALLY BLANK