	Contingency Planning Policy		**Document No.** SCIO-SEC-306
Effective Date 01/29/2018	**Review Date** 01/18/2022	**Version** 3	**Page No.** 1 of 9

Scope

The Statewide Information Security Policies are the foundation for information technology security in North Carolina. The policies set out the statewide information security standards required by N.C.G.S. §143B-1376, which directs the State Chief Information Officer (State CIO) to establish a statewide set of standards for information technology security to maximize the functionality, security, and interoperability of the State's distributed information technology assets, including, but not limited to, data classification and management, communications, and encryption technologies. This policy covers all State information and information systems to include those used, managed, or operated by a contractor, an 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 information systems that support the operation and assets of the State. Use by local governments, local education agencies (LEAs), community colleges, constituent institutions of the University of North Carolina (UNC) and other executive branch agencies is encouraged to the extent allowed by law. This security policy is consistent with applicable laws, executive orders, directives, regulations, other policies, standards, and guidelines.

Material Superseded

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

Responsibilities

All covered personnel who utilize State of NC IT resources are responsible for adhering to this policy and with any local Contingency Planning requirements.

Role	Definition
Agency Management	The Agency Head, the Chief Information Officer (CIO), the Chief Information Security Officer (CISO), or other designated organizational officials at the senior leadership level are assigned the responsibility for the continued development, dissemination, implementation, operation and monitoring of the Contingency Planning program.
Business Continuity Plan Administrator & Planner	The person(s) designated as the agency Business Continuity (BC) & Disaster Recovery (DR) Plan Administrator and Planner(s) has the responsibility of overseeing the individual plans and files that constitute the BC/DR Plan and ensuring that they are current, meet these standards and are consistent with the agency's overall plan. At the direction of the State Chief Information Officer, an agency's BC/DR Plan shall be reviewed annually by the Office of the State CIO and recommendations shall be made for improvement, if necessary.
Contingency Planning Team	A team composed of representatives from the agency organizational areas with primary leadership responsibility to identify information technology risks and to determine what impact these risks have on business operations.

Role	Definition
Third Party Service Providers	Third party service providers are those vendors who provide and support contingency plans and capabilities.

CP-1 – Contingency Planning Policy and Procedures

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

All State agencies must develop, adopt, and adhere to a formal, documented contingency planning procedure that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The appropriate level of information technology business continuity management must be in place to sustain the operation of critical information technology services to support the continuity of vital business processes, also known as mission and business essential functions, and the timely delivery of critical automated business services to the State's citizens.

Appropriate planning and testing processes must be in place to ensure that, in the event of a significant business interruption, critical production environments can be recovered and sustained to meet State business requirements. To facilitate the effective recovery of systems and compliance with this policy, coordination is required between the Department of Information Technology (DIT), State, and Agency business units. This policy covers mainframe, distributed environments, and cloud-hosted environments, e.g., Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS).

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. The following subsections in this document outline the Contingency Planning requirements that each agency must implement and maintain in order to be compliant with this policy. This policy and associated procedures shall be reviewed and updated annually, at a minimum. They shall also be updated following agency-defined events that necessitate such change.

This policy and the associated procedures shall be developed, documented, and disseminated by Agency Management, or the Business Continuity Plan Administrator or Planner.

CP-2 – Contingency Plan

The State's information assets must be available to authorized users when needed. Information technology risks must be managed appropriately as required in state and federal laws. A contingency plan/disaster recovery plan must be developed for the recovery of information assets for which the State is named as owner for all known threats to availability, including natural disasters, accidents, malicious destruction, failures, and denial of services. Management shall coordinate contingency plan development with organizational elements responsible for formally documenting the Business Continuity (BC) & Disaster Recovery (DR) Plan that covers all the agency's critical applications and includes procedures or references to procedures to be used for the recovery of systems that perform the agency's essential mission and critical business processes.

Application criticality has the following four categories (Definitions may be found in the Statewide Glossary of Information Technology Terms):

i. Statewide Critical
ii. Department Critical
iii. Program Critical
iv. Noncritical

Agencies with Statewide and Departmental Critical systems must provide disaster recovery capabilities to ensure timely recovery and restoration of service as part of their disaster recovery strategy. Agencies must coordinate contingency plan development and execution with agency divisions and groups responsible for related plans. Plans related to contingency plans for agency information systems include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, Insider Threat Implementation Plan, and Occupant Emergency Plans.

Plans must include the following:

a. Be developed prior to implementation as part of the development life cycle for technology development or deployment by agency to address all production processing environments and assets.

b. Identify essential missions and business functions and associated contingency requirements.

c. Provide recovery time and recovery point objectives, restoration priorities; and estimate the following three downtime factors for consideration 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), for example, one business day (8 hours) or one day (24 hours).

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 (given the most recent backup copy of the data) after an outage, e.g., the last completed transaction or the point immediately before the last backup commences.

d. Identify contingency roles, responsibilities, assigned individuals with contact information.

e. Address eventual, full information asset restoration without deterioration of the security measures originally planned and implemented.

f. Address the sharing of contingency information.

g. Be reviewed and approved by designated officials within the agency.

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 the employees of the State of North Carolina.

n. Address the protection of assets of the State and minimize financial, reputational, legal and/or regulatory exposure.

o. Create crisis teams and response plans for threats and incidents.

p. Require that employees are made aware of their roles and responsibilities in the BC/DR Plan and in plan execution through 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 State CIO on an annual basis, and as otherwise requested by the State CIO.

s. Support the resumption of e vital business processes or mission essential functions within the agency-defined time period of contingency plan activation.

t. Define the time period for resumption of essential mission/business functions dependent on the severity/extent of disruptions to the information system and its supporting infrastructure.

u. Define within the contingency plan and Business Impact Analysis (BIA) the time period in which the system needs to be operational to support essential mission and business functions.

CP-3 – Contingency Training

Personnel must be trained in their contingency roles and responsibilities with respect to the information assets. Training and awareness programs shall ensure that the organization understands the roles each individual within the organization in a disaster/or adverse situation. The contingency training content shall be reviewed and updated on an annual basis and following any defined events that necessitate change.

Contingency training shall be provided to information system users for the following conditions:

i. Prior to assuming a contingency role or responsibility,

ii. When required by information system changes,

iii. Annually thereafter.

CP-4 – Contingency Plan Testing

Contingency plan testing must be coordinated with divisions and groups responsible for related plans. The following must be done:

a. Develop test objectives and success criteria to enable an adequate assessment of the Disaster Recovery and/or Restoration procedures.

b. Test and/or exercise the contingency plan for the critical information assets annually, at a minimum, in order to determine the plan’s effectiveness and the organization’s readiness to execute the plan.

c. Develop a contingency plan exercise after action report.

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).

Table 1 – Test Types

Test Type	Description
Walk-Through	A participatory session featuring an oral walk-through of the technology recovery plan and of the specific tasks documented within the plan. This exercise should confirm the plan’s design and identify role and responsibility gaps or other weaknesses in the plan. This type of exercise can be used on alternating years between more complete testing for lower criticality systems.
Table-Top	A participatory session using example interruptions led by a facilitator to test the integrity of the disaster recovery plan as well as the readiness of the participating staff to respond to an adverse event.

Stand-Alone	Tests one or more specific components of a technology recovery plan in isolation from other components. Focuses on data restoration with network connectivity and is usually limited to a single platform or system. It may or may not include testing application interdependencies.
Partial Integration	Tests one or more specific components of a technology recovery plan. Includes testing data restoration with network connectivity and testing some interdependencies with applications and/or platforms.
Full End-to-End	Tests the technology recovery plan in a technology recovery testing environment without risk to the production environment, tests all components of the technology recovery plan and all functionality of an application. Includes testing transactions and testing all interdependencies with other applications and/or platforms. Tests shall be conducted at alternate sites or other recovery arrangements of the testing organization, personnel, equipment, facilities, and processes.

CP-5 – Contingency Plan Update

Withdrawn: Incorporated into CP-2.

CP-6 – Alternate Storage Site

An alternate storage site must be established for systems that are defined as critical 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 in a location that is separate from the primary facility to ensure that the risk of a disruption (e.g., natural disasters, structural failures, hostile cyber attacks) affecting both the primary and alternate site is low or otherwise is at an acceptable level, based on an assessment of risk.

c. Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions. Area-wide disruptions refer to those types of disruptions that are broad in geographic scope (e.g., hurricane, regional power outage) with such determinations made by agencies based on agency assessments of risk. Explicit mitigation actions include, for example:

   i. Duplicating backup information at other alternate storage sites if access problems occur at originally designated alternate sites;

   ii. Planning for physical access to retrieve backup information if electronic accessibility to the alternate site is disrupted.

d. This control is optional for LOW risk information systems.

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 vital business processes or mission essential functions within defined recovery times and recovery points when the primary processing capabilities are unavailable. Alternate processing sites shall provide a Service Level Agreement (SLA) that contains priority-of-service provisions in accordance with the information system's requirements in the event of a disruption or disaster. This may be in the form of a priority-of-service provision or through a provider with a sufficient network of facilities to ensure available capacity.

b. Ensure that equipment and supplies required to resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the agency-defined time period for transfer/resumption.

c. Ensure that the alternate storage site provides information security safeguards that meet the comparable protection standards of the primary site.

d. Identify an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.

e. Determine what is considered a sufficient degree of separation between primary and alternate processing sites based on the types of threats that are of concern.

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.

h. Develop alternate processing site agreements that contain priority-of-service provisions in accordance with agency availability requirements (including recovery time objectives). Priority-of-service agreements refer to negotiated agreements with service providers that ensure that agencies receive priority treatment consistent with their availability requirements including defined RTO and RPO objectives as defined in the business impact analysis (BIA) and contingency plan.

i. This control is optional for LOW risk information systems.

CP-8 – Telecommunications Services

The following must be done for telecommunication services:

a. Establish alternate telecommunications services with telecommunication service providers that provide communications transmission services to maintain a state of readiness or to respond to and manage any event or crisis.

b. Communications transmission services must include necessary agreements to permit the resumption of information asset operations for essential missions and business functions within defined recovery time and recovery points when the primary telecommunications capabilities are unavailable.

c. Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with agency availability requirements (including recovery time objectives).

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.

f. Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

g. This control is optional for LOW risk information systems.

CP-9 – System Backup

a. Backups must be conducted of system documentation, such as operating system files and application software from organization managed laptops, workstations, servers, as well as security-and privacy-related documentation, and user level information, such as user level files stored on a shared network drive, at a frequency that is consistent with agency defined Recovery Time Objective (RTO), and Recovery Point Objective (RPO).

b. The confidentiality and integrity of backup information must be protected.

CP-9 (1) – Information System Backup | Testing for Reliability/Integrity

Backup information must be tested quarterly to verify media or cloud storage reliability, and information (data) integrity.

CP-9 (8) – System Backup | Cryptographic Protection

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

CP-10 – System Recovery and Reconstitution

The following must be done for system recovery and reconstitution:

a. Provide for the recovery and reconstitution of vital business processes/mission essential function(s), including transaction-based information systems, to a known state after a disruption, compromise, or failure within agency defined RTO and RPO objectives.

b. Applications categorized as Statewide and or Agency critical are recommended to have viable disaster recovery support, approval, budget in place, and be exercised according to policy.

c. Ensure plan activations are documented and recorded, and post-activation reviews are conducted to evaluate the effectiveness of the plan(s).

d. Update the plan(s) where necessary and provide a formal report to the State CIO within 30 days of post-activation review.

CP-11 – Alternate Communication Protocols (Optional)

This control is optional for LOW and MODERATE risk information systems.

CP-12 – Safe Mode (Optional)

This control is optional for LOW and MODERATE risk information systems.

CP-13 – Alternative Security Mechanisms (Optional)

This control is optional for LOW and MODERATE risk information systems.

Enforcement

Violations of this policy or failure to implement provisions of this policy may result in disciplinary action up to and including termination, civil litigation, and/or criminal prosecution.

DocuSigned by:
Approved: James Weaver 1/19/2022 | 11:34 AM EST
372C8D237E5547A...

Secretary of Department of Information Technology (DIT)