State of Maryland

STANDARD

CONTINGNENCY PLANNING

Document No.	Last Updated	Prepared By
MD-STD-306-CP-01	02/18/2026	DOIT OSM

Contingency planning, as a vital component of Zero Trust Architecture (ZTA), is crucial for preparing an organization for unexpected disruptions by ensuring an effective response, minimizing damage, and maintaining resilience through continuous monitoring, adaptive security controls, and least-privilege access enforcement.

PURPOSE AND SCOPE

Purpose	This standard provides the technical and operational specifications needed to establish, prepare, respond to, and recover from disruptive events that may impact State operations.
Scope	This standard provides an organizational approach for achieving resilience in the face of unexpected disruptions.
Applicability	This standard applies to all units of State government (as defined in SF&P 3.5-101(g)), hereafter referred to simply as “agencies.”
Related Policy	This standard is part of a broader policy suite. Refer to MD-POL-100 Cybersecurity & Governance Policy, Appendix C for a list of related policies and standards.
Baseline	This standard has been developed using National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5 Moderate Baseline[1] and State-specific organizationally defined parameters. Agencies may be required to deviate from this baseline when State statute, executive orders, or applicable regulations establish a conflicting requirement that precludes compliance.
Distribution	This document is approved for public distribution and may be shared with external stakeholders, partners, and regulatory bodies. It reflects the State’s commitment to transparency, compliance, and operational excellence. Unauthorized modifications or misrepresentation of this document are strictly prohibited.

[1] NIST SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations.

FOREWORD

Agencies that use Department of Information Technology DoIT-managed services automatically receive, or *inherit*, the compliance those services already meet, reducing duplicative work and accelerating their overall compliance efforts. These centrally governed services, such as hosting platforms, identity management, and network infrastructure, are built with robust control frameworks that automatically extend to participating agencies. By leveraging these offerings, agencies not only align with key operational and security standards but also benefit from pre-configured environments, continuous monitoring, and policy enforcement mechanisms maintained by DoIT. Agencies are encouraged to leverage these services to accelerate readiness, gain cost efficiency, simplify compliance efforts, and allow agencies to focus more fully on mission delivery, knowing that foundational requirements are already in place. Agencies should review the scope of each managed service to understand which standards are inherited and where additional agency-specific controls may still be required.

GUIDANCE AND ENFORCEABILITY

Throughout this document, informational call-out boxes are utilized to provide additional context or elaborate on key topics. While these boxes primarily serve an informational purpose, any directives or mandated actions contained within them are authoritative and carry the same enforceability as the core requirements of this document. For the purposes of this document, the term “shall” denotes a mandatory requirement. Terms such as “where feasible”, “encouraged”, or similar phrasing indicate recommended practices that reflect organizational preference but are not enforceable requirements at this time.

CHANGE RECORD

Version	Summary of Changes	Changed By	Date
1.0	Initial Publication	Miheer Khona	02/18/2026

STANDARDS

306 State Strategy

These standards establish a baseline of contingency planning practices that each agency must implement to comply with State cybersecurity and privacy policies. Each agency shall designate specific personnel with IT responsibilities to ensure the effective implementation of these standards.

306-1 Develop Agency-Level Procedures (CP-1)

In alignment with this standard, develop and document agency-level contingency planning procedures. Agencies must disseminate the procedures to agency personnel with information technology (IT) security responsibilities. Agencies must review, and if needed, update the procedures as deemed appropriate by the agency based on changes and risk at least every **3 years**. At a minimum, the procedures must address purpose, scope, roles and responsibilities, and guidelines.

306-2 Develop a Contingency Plan (CP-2)

Develop a contingency plan, in coordination with DoIT OSM, for the system that:

- Identifies essential mission/business functions and contingency requirements;
- Provides recovery objectives, restoration priorities, and metrics;
- Addresses contingency roles, responsibilities, assigned individuals, and contacts;
- Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure;
- Addresses full system restoration without deterioration of the controls originally planned and implemented;
- Addresses the sharing of contingency information; and
- Is reviewed and approved by designated agency Authorizing Official (AO).

Cyber Resilience and the PACE

Cyber resilience is the ability of IT environments to anticipate, withstand, recover from, and adapt to adverse conditions whether caused by cyberattacks, system failures, or human error. A practical way to embed resilience is through the PACE concept: **Primary, Alternate, Contingency, and Emergency**. This framework ensures that for every critical function, organizations define multiple layers of capability. The Primary system delivers the intended service under normal conditions; the Alternate provides a backup path; the Contingency option offers a different but workable solution; and the Emergency method guarantees continuity when all else fails. By mapping IT services against PACE, teams create structured redundancy, reduce single points of failure, and strengthen operational confidence in the face of disruption[2].

Distribute digital and hard copies of the contingency plan to personnel identified by role in the contingency plan. Coordinate contingency planning activities with incident handling activities. Review the contingency plan for the system at least annually. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing. Communicate contingency plan changes to personnel identified by role in the contingency. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training. Protect the contingency plan from unauthorized disclosure and modification.

CP-2(1): Coordinate contingency plan development with organizational elements (e.g., Incident Response and Emergency Management Teams) responsible for related plans.

Contingency Related Plans

Plan	NIST Description	Focus Area
Continuity of Operations Plan (COOP)	A plan that describes how an organization's mission essential functions will be sustained within **12 hours** and for up to **30 days** as a result of a disaster event before returning to normal operations.	Mision Essential Functions
Business Continuity Plan (BCP)	A subset of COOP that describes how an organization's mission/business processes will be sustained during and after a significant disruption.	Critical Business Processes
Contingency Plan (CP)	A plan to maintain or restore business operations, including computer operations, possibly at an alternate location.	IT Systems
Disaster Recovery Plan (DRP)	A subset of the Contingency Plan focused on restoring IT systems and infrastructure.	IT Systems

[2] CISA Guidance PACE: Leveraging the PACE Plan into the Emergency Communications Ecosystem, Apr. 2023

Plan	NIST Description	Focus Area
Incident Response Plan (IRP)	A plan to detect, respond to, and limit consequences of a malicious cyberattack against an organization's information system(s).	IT Systems

CP-2(3): Plan for the resumption of essential mission and business functions within the time frame specified in the contingency plan after activation of the contingency plan.

CP-2(8): Identify critical system assets supporting all mission and business functions.

306-3 Provide Contingency Training (CP-3)

Provide contingency training to system users consistent with assigned roles and responsibilities:

- Within **90 days** of assuming a contingency role or responsibility;
- When required by system change(s); and
- At least **annually** thereafter.

Training content must include:

- Information regarding when and where to report for duty during contingency operations and if normal duties are affected;
- Role-based training for system administrators who may require additional training on how to set up information systems at alternate processing and storage sites; and
- Role-based training for managers/senior leaders who may require more specific training on how to conduct mission-essential functions in designated off-site locations and how to establish communications with other governmental entities for purposes of coordination on contingency-related activity.

Review and update contingency training content annually and following recovery from an event.

306-4 Perform Contingency Plan Testing (CP-4)

Test the contingency plan for High Valued State System (HVSS) at least **annually**, and periodically for non-HVSS to determine the effectiveness of the plan and the readiness to execute the plan. Review the contingency plan test results and initiate corrective actions, if needed. Real-world contingency plan activation satisfies the testing requirement as long as results are documented.

CP-4(1): Coordinate contingency plan testing with organizational elements responsible for related plans (e.g., COOP, BCP, DRP, IRP, Business Recovery Plan, and Emergency Action Plan (EAP).

306-5 Establish an Alternate Storage Site (CP-6)

Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information; and verify that the alternate storage site provides cybersecurity and privacy controls equivalent to that of the primary site.

CP-6(1): Identify an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats.

CP-6(3): Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.

306-6 Establish an Alternate Processing Site (CP-7)

Establish an alternate processing site, with the necessary agreements in place, to ensure critical system operations can be transferred and resumed within the agency-defined time frame identified in its Business Impact Analysis (BIA) whenever the primary site is unavailable.

Business Impact Analysis

A BIA is a structured process used to identify and evaluate the potential effects of disruptions to critical business operations. It helps agencies understand which functions are essential, how long they can tolerate downtime, and what resources are needed to recover. To perform a BIA agencies shall: a) Identify critical business functions and the systems, personnel, and data they depend on; b) Assess the impact of disruptions (e.g., financial loss, regulatory penalties, reputational damage); c) Determine Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for each function; and d) Prioritize recovery efforts based on operational and mission-criticality. Refer to the NIST Special Publication 800-34 for a BIA template and guidelines.

Ensure the alternate processing site has the equipment and supplies needed to transfer and resume operations or establish contracts to deliver them within the agency-defined time frame. The alternate site shall maintain controls equivalent to those at the primary site.

CP-7(1): Identify an alternate processing site that is sufficiently separated from the primary processing site to reduce susceptibility to the same threats.

CP-7(2): Identify potential accessibility problems to alternate processing sites in the event of an area-wide disruption or disaster and outline explicit mitigation actions. Potential accessibility problems with the alternate processing site and mitigation procedures shall be documented in the contingency plan and any other relevant alternate processing site documentation.

CP-7(3): Develop alternate processing site agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives).

306-7 Establish Alternate Telecommunications Services (CP-8)

Establish alternate telecommunications services, including necessary agreements to permit the resumption of all critical information systems operations within **24 hours,** or as required by the BIA, when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

CP-8(1): Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives), and request telecommunications service priority for all telecommunications services used for national security emergency preparedness if the primary or alternate telecommunications services are provided by a common carrier.

CP-8(2): Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

306-8 Conduct System Backup (CP-9)

Conduct backups at least **weekly** of user-level information, system-level information, and system documentation, including security and privacy related documentation. Protect the confidentiality, integrity, and availability of backup information using access controls.

CP-9(1): Test backup information as part of contingency plan testing to verify media reliability and information integrity.

CP-9(8): To prevent unauthorized disclosure and modification of backup information, implement encryption of back up data following the minimum encryption standards defined in MD-STD-318-SC System and Communication Protection Standard, Section 318-6.

Encryption of IT Backups

Encryption in backup environments safeguards non-public data throughout its lifecycle, from creation and storage to replication and restoration. To further strengthen resilience against modern threats such as ransomware, agencies must also implement immutable backups. Immutable backups are copies of data that cannot be altered or deleted within a defined retention period. Immutable backups ensure that even if primary systems are compromised, recovery can be facilitated from a clean, untampered source. Together with immutability, each of the following encryption layers plays a distinct role in safeguarding data against unauthorized access, tampering, or exfiltration: a) Hardware-level encryption for backup media; b) Backup storage and file system encryption; c) Database backup encryption; d) Network and transport encryption for backup transfers; e) Backup application-level encryption; and f) Key management for backup encryption.

306-9 Perform System Recovery and Reconstitution (CP-10)

Provide for the recovery and reconstitution of the system to a known state consistent with the recovery time and recovery point objectives established in the contingency plans.

CP-10(2): Implement transaction recovery for systems that are transaction-based.

GUIDELINES

ID	Title	Description	Source
CSF Tools	Cyber Security Framework Tools	This website provides supplemental guidance for each security control listed in this document.	*csf.tools (LINK)*
NIST SP 800-34	Contingency Planning Guide for Federal Information Systems	This document provides guidance on developing information system contingency plans, including disaster recovery, incident response, and business continuity strategies.	*csrc.nist.gov (LINK)*

DEFINITIONS

Each unique term used in this standard is defined in the **State of Maryland Cybersecurity & Privacy Glossary**.

COMPLIANCE CHECKLIST

ID	Standard	Compliance
306-1	**Develop Agency-Level Procedures (CP-1)**	☐ Yes ☐ No
306-2	**Develop a Contingency Plan (CP-2)**	☐ Yes ☐ No
306-3	**Provide Contingency Training (CP-3)**	☐ Yes ☐ No
306-4	**Perform Contingency Plan Testing (CP-4)**	☐ Yes ☐ No
306-5	**Establish an Alternate Storage Site (CP-6)**	☐ Yes ☐ No
306-6	**Establish an Alternate Processing Site (CP-7)**	☐ Yes ☐ No
306-7	**Establish Alternate Telecommunications Services (CP-8)**	☐ Yes ☐ No
306-8	**Conduct System Backup (CP-9)**	☐ Yes ☐ No
306-9	**Perform System Recovery and Reconstitution (CP-10)**	☐ Yes ☐ No

Note: When assessing the implementation and effectiveness of the security and privacy controls outlined in this standard, DoIT recommends the use of NIST SP 800-53A Rev. 5, to perform evaluations in a manner that is evidence-based, repeatable, and aligned with the system's documented security posture.