Maryland

DEPARTMENT OF INFORMATION TECHNOLOGY

Office of Security Management

Continuity of Operations Policy

Distribution Statement: 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.

State of Maryland

CONTINUITY OF OPERATIONS POLICY

MD-POL-210-01 | **Last Updated: 02/18/2026**

TABLE OF CONTENTS

CHANGE RECORD

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

State of Maryland

CONTINUITY OF OPERATIONS POLICY

MD-POL-210-01	Last Updated: 02/18/2026

100 INTRODUCTION

Purpose:	This policy establishes the requirements for building and maintaining restoration capabilities that support recovery to normal State operations after an incident or disruption.
Scope:	This policy addresses the identification, protection, and recovery of State systems and services in the event of a cybersecurity incident, disruption, or degradation of normal operations.
Authorization:	This policy is authorized by State Finance & Procurement Article (SF&P) § 3.5-303 and § 3.5-2A-04.
Applicability:	This policy applies to all "units of State government" (as that term is defined in SF&P 3.5-101(g)), hereafter referred to as “agencies.”
Superseded Policy:	The full policy suite outlined in MD-POL-100 Cybersecurity & Governance Policy, Appendix C supersedes the State of Maryland Information Technology Security Manual Version 1.2, June 28, 2019.
Waivers:	Refer to the MD-POL-100 Cybersecurity Governance Policy guidance on exception requests and waivers related to this policy.
Stakeholder Roles:	**Department of IT (DoIT) -** The Department responsible for developing, maintaining, revising, and enforcing information technology policies, procedures, and standards.
	State Chief Information Security Officer (SCISO) - The appointed individual responsible for overseeing the State's cybersecurity strategy and ensuring the protection of its information systems.
	State Chief Privacy Officer (SCPO) - The individual responsible for supporting agencies in the development and implementation of effective privacy programs, developing privacy policies, and promoting compliance with data protection best practices.

	Executive Branch Secretaries, Executive Directors, and Administrators (or equivalent) – The individuals who oversee specific departments and agencies responsible for ensuring the implementation of this policy and any related standards for their respective agencies.
	IT Managers – Any staff with the responsibility of procuring or operating IT systems and equipment within an agency.
	Information Security Officers (ISO) - The individuals assigned to provide agencies with security expertise, guidance, and resources to assist agencies in meeting State and Federal cybersecurity compliance requirements.
	Information User (hereafter referred to simply as "user") - Any person who interacts with a State computer system, software application, or network service to include State employees, contractors, vendors, third-party providers.
Stakeholder Responsibilities:	Following the policy statements in each area, a RACI matrix is provided to clearly address responsibility for each policy statement as follows:
	[R] Responsible: The person or people within each agency who are tasked with completing the work.
	[A] Accountable: The person or people within each agency who authorize and assign the work and validate that the work is completed.
	[C] Consulted: The person or people within each agency whose input is sought during the completion of the task.
	[I] Informed: The person or people within each agency who need to be kept up to date on the progress or completion of the task.

All requirements in this policy remain in effect unless an applicable State Statute or Executive Order establishes a conflicting requirement that precludes compliance.

200 POLICY

The following sections detail the actions required to reduce the impact of, withstand, and recover from business disruptions, and enhance resiliency.

200.1 CONTINUITY PLANNING

200.1.1 Continuity of Operations Plan: Agencies shall develop a plan to recover from disruptions in a manner that aligns with the standards and guidance provided by the Maryland Department of Emergency Management (MDEM) and the DoIT Office of Security Management (OSM). The plan shall include at a minimum:

- Mission Essential Functions (MEF);
- Recovery Time Objectives (RTO);
- Recovery Point Objectives (RPO);
- Order of Succession;
- Alternate Facilities;
- Continuity Communications;
- Vital Records Management;
- Devolution of Control; and
- Reconstitution.

Refer to the MD-STD-306-CP, Contingency Planning Standard, for more information on continuity planning and how other related plans (e.g., continuity of operations plans, business continuity plans, contingency plans, disaster recovery plans, and incident response plans) support this function.

Table 1 RACI Matrix – Continuity Planning

	DOIT	SCISO	Secretaries/ Directors	IT Managers	ISOs
Continuity of Operations Plan	C	I	A	R	C

[R] Responsible, [A] Accountable, [C] Consulted, [I] Informed

200.2 RECOVERY ACTIVITIES

200.2.1 Recovery: Recovery activities shall be performed in a prioritized manner in accordance with the continuity of operations plan (COOP) or related plans, and shall include at a minimum:

- Integrity verification of backups before use, including malware and intrusion detection scanning;
- Integrity verification of recovered assets for normal operating status; and
- A review of mission essential functions and cybersecurity risk during post-disruption analysis.

200.2.2 Reporting & Communication: All recovery activities shall be tracked and status validated until the end of recovery is declared. Recovery activities shall be coordinated with DoIT OSM (and MDEM if an emergency is declared) prior to any communication with external stakeholders.

Table 2 RACI Matrix – Recovery Activities

	DOIT	SCISO	Secretaries/ Directors	IT Managers	ISOs
Restoration	C	I	A	R	C
Reporting & Communication	C	I	A	R	C

[R] Responsible, [A] Accountable, [C] Consulted, [I] Informed

300 APPROVAL

Katie Savage
Secretary & State Chief Information Officer
Maryland Department of Information Technology

James Saunders

James Saunders
State Chief Information Security Officer
Maryland Department of Information Technology

APPENDIX A: POLICY MAPPING MATRIX

This matrix provides a mapping of NIST CSF[1] Best Practices to the sections in this policy for reference.

NIST CSF Category	NIST CSF Sub-Categories	Maryland Policy Mapping
Recover	RC.RP: Incident Recovery Plan Execution	Section 200.1, 200.2
Recover	RC.CO: Incident Recovery Communication	Section 200.1, 200.2

[1] NIST Cyber Security Framework 2.0

APPENDIX B: DEFINITIONS

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