Maryland

DEPARTMENT OF
INFORMATION TECHNOLOGY

Office of Security Management

Cybersecurity Policy

Emergency and Binding Operational Directives

Table of Contents

Introduction 1
Policy Statement 1
Applicable Law and Policy 2
Scope and Responsibilities 2
Key Terms 2

Revision History

Version	Date	Description of Changes
1.0	October 1, 2022	Initial Version

Approval

Charles I Stewart IV __

__10/1/2022__

Charles “Chip” Stewart
State Chief Information Security Officer

Date

Introduction

Emergency and binding operational directives are compulsory directions to Units within the Executive Branch for purposes of safeguarding information and information systems. This policy establishes the mandate to follow the directives and the mechanism by which the State Chief Information Security Officer (SCISO) issues and communicates these mandates.

Policy Statement

The State Chief Information Security Officer is responsible for developing and overseeing the issuance of binding operational directives.

The State Chief Information Security Officer, in consultation with the Secretary, may issue binding operational directives, including:

- requirements for reporting security incidents
- requirements for the mitigation of exigent risks to information systems; and
- other operational requirements the State Chief Information Security Officer may determine necessary;

Additionally, in response to a known or reasonably suspected information security threat, vulnerability, or incident that represents a substantial threat to the information security of a unit, the State Chief Information Security Officer, in consultation with the Secretary, may issue emergency directives requiring units to take any lawful action with respect to the operation of an information system, including such systems used or operated by another entity on behalf of an agency, that collects, processes, stores, transmits, disseminates, or otherwise maintains State information, for the purpose of protecting the information system from, or mitigating, an information security threat.

Binding Operational Directives and Emergency Directives may be updated periodically and will be posted on the Department of Information Technology's website and sent electronically to the heads of each unit and the designated technical contact within each unit. The Secretary of Information Technology may repeal or revise, at their discretion, directives that are inconsistent with State law, policy, or strategy.

Applicable Law and Policy

Maryland State Finance and Procurement Code Ann. Title 3.5

Scope and Responsibilities

All Units of the Executive Branch of the State Government are required to comply with this Policy. Agency executives and applicable staff covered by this policy shall ensure adherence. No exceptions to this policy are permitted without the written consent of the State CISO.

Key Terms

Binding Operational Directive: Compulsory **strategic** direction to a unit that is for purposes of safeguarding information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk.
Department of Information Technology (DoIT): An executive branch unit of Maryland state government, organized according to Maryland Code, State Finance and Procurement Article, § 3A.
Emergency Directive: Compulsory **tactical** direction to a unit that is for purposes of safeguarding information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk.
Incident: means an occurrence that:

- actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or
- constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

Information security: means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide:

- integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;
- confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
- availability, which means ensuring timely and reliable access to and use of information.

State Chief Information Security Officer: The State-Level executive responsible for the direction, coordination, and implementation of cybersecurity strategy and, policy for all units of the executive branch.
Units: All executive branch units of state government.