# Enterprise Information Security Governance and Management Policy

**POLICY NUMBER: 17-03-NJOIT**

| Approved By: | | Version: |
|---|---|---|
| Christopher J. Rein, Chief Technology Officer | | 2.0 |
| **Effective Date:** | **Revision Date:** | **Supersedes:** |
| October 18, 2017 | April 12, 2023 | N/A |

## 1 Policy

The Chief Technology Officer (CTO) of New Jersey and the Director, New Jersey Office of Homeland Security and Preparedness (NJOHSP) jointly establish the Information Security Governance Committee and a management structure for information security across the Executive Branch of New Jersey State government (The Policy).

## 2 Authority

The Policy is established under the authority of New Jersey Statute NJSA, Sections C.52:18A-224 through C.52:18A-234, known as *"The Office of Information Technology Reorganization Act."*

New Jersey Executive Order #5 creating the Office of Homeland Security and Preparedness (OHSP) (Corzine, 3/6/2006).

New Jersey Executive Order #178 creating the New Jersey Cybersecurity and Communications Integration Cell ("NJCCIC") (Christie, 5/20/2015).

The Critical Infrastructure Information Act of 2002, 6 U.S.C. §133et seq.

# 3 Scope

All Executive Branch departments and State agencies (Agencies) are directed to cooperate fully with the NJOIT and the CTO to implement the provisions of the Policy, and to ensure effective use of information technology within the Executive Branch of State Government.

# 4 Objective

This Policy defines the information security management authorities, roles and responsibilities of New Jersey Executive Branch officers, departments, and agencies.

# 5 Roles and Responsibilities

## 5.1 Information Security Governance Committee (ISGC)

The ISGC shall be established and co-chaired by the Director of NJOHSP and the Chief Technology Officer. Membership will include the State CISO, State Chief Data Officer, Director of the NJCCIC, as well as representatives from the Governor's Office, the Office of the Attorney General, the Civil Service Commission, the Department of the Treasury's Office of Management and Budget, and other State agencies, as appropriate. The ISGC shall report to the Cabinet and be responsible for:

i. Assisting the State CISO in overseeing and executing New Jersey's information security management program;

ii. Reviewing the Statewide Information Security Policies and Standards– and subsequent amendments–to ensure their alignment with the Executive Branch of State Government business objectives and goals, risk tolerances, and statutory, regulatory, and contractual requirements;

iii. Providing direction and counsel regarding the assessment and management of information security risks and cyber threats to the State of New Jersey;

iv. Reviewing reports on major information security incidents and cases of non-compliance;

v. Overseeing the response to information security incidents;

vi. Reviewing security metrics and trends regarding the overall performance of the information security program;

vii. Staying abreast of cybersecurity threats to the Executive Branch of State Government through briefings and reports.

## 5.2 Director, New Jersey Office of Homeland Security and Preparedness (NJOHSP)

The Director of NJOHSP shall be responsible for administering, coordinating, leading, and supervising New Jersey's counter-terrorism and preparedness efforts. The goal of this Office shall be to coordinate emergency response efforts across all levels of government, law enforcement, emergency management, non-profit organizations, other jurisdictions, and the private sector, to protect the people of New Jersey. In addition, the Director shall be responsible for the strategic development, execution, and management of an effective and efficient information security program to manage cyber risks and ensure the confidentiality, integrity, and availability of the Executive Branch's information assets.

i. Overseeing the response to information security incidents;

ii. Staying abreast of cybersecurity threats to the Executive Branch of State Government and informing the ISGC through regular briefings and reports.

iii. Advise the ISGC through regular briefings and reports.

## 5.3 Chief Technology Officer (CTO), New Jersey Office of Information Technology (NJOIT)

The CTO leads NJOIT, which is responsible for providing and maintaining the information technology infrastructure of the Executive Branch of State

Government, including all ancillary departments and agencies. The CTO provides vision and leadership for NJOIT and is responsible for coordinating and conducting all Executive Branch technology operations. The CTO directs the planning, implementation, and governance of enterprise IT systems in support of the Executive Branch of State Government's business objectives and operations to improve cost-effectiveness, service quality, and mission development.

At the CTO's direction, NJOIT fulfills the following responsibilities in support of the State's Information Security Program:

i. Design, acquisition, and implementation of enterprise IT systems in compliance with the Statewide Information Security Manual's Policies and Standards set by the State CISO;

ii. Operation and support of IT systems in compliance with approved security procedures, including, but not limited to:

    1. *IT asset management;*

    2. *Malware protection;*

    3. *Patch management;*

    4. *Web proxying and Content filtering;*

    5. *Secure file exchange; and*

    6. *Data encryption;*

iii. Management of third parties providing managed information services to the NJOIT and other State Entities;

iv. Identity and access management;

v. Disaster recovery planning and operations;

vi. Providing recommendations on policy and control enhancements to NJOHSP's Division of Cybersecurity;

vii. Monitoring NJOIT's IT environment to identify, contain, or eliminate unauthorized activity;

viii. Assisting in implementing the Information Security Incident Response

Plan;

ix. Providing subject-matter expertise for technical issues regarding information security;

x. Executing the day-to-day security management of enterprise information, systems, and solutions through the application of controls as defined within the Statewide Information Security Manual's Policies and Standards.

## 5.4 State Chief Information Security Officer (CISO)

The State CISO reports to the Director of NJOHSP and serves as head of NJOHSP's Division of Cybersecurity. The State CISO shall establish and manage an information security program to ensure the confidentiality, integrity, and availability of the State of New Jersey Executive Branch's information resources, systems, and services while promoting and protecting privacy. The State CISO has overall responsibility for the development, implementation, and performance of the information security program by:

i. Setting strategic information security planning across the Executive Branch of State Government;

ii. Publishing the Statewide Information Security Manual's Policies and Standards;

iii. Developing, managing, and executing the statewide Information Security Incident Response Plan;

iv. Identifying security requirements to limit the risks associated with identified Executive Branch business objectives as defined by the Governor and the Heads of State agencies;

v. Developing, maintaining, and interpreting the Statewide Information Security Manual's Policies and Standards;

vi. Providing information security subject matter expertise to State agencies;

vii. Drafting and implementing an information security awareness and training program to be used by all State agencies;

viii. Providing security metrics to track the performance of the information security program;

ix. Developing an Information Security Governance, Risk, and Compliance program, including, but not limited to:

1. *Coordinating and conducting compliance and risk assessments of agencies and their information assets;*

2. *Conducting and managing vulnerability assessments of agency networks, applications, databases, and systems;*

3. *Conducting penetration tests of agency networks applications, databases, and systems;*

4. *Conducting information security risk assessments of third parties with access to State of New Jersey information assets.*

## 5.5 Director, New Jersey Cybersecurity and Communications Integration Cell (NJCCIC)

The NJCCIC, established within NJOHSP's Division of Cybersecurity, shall be the State's Information Sharing and Analysis Organization. The Director of the NJCCIC shall be responsible for:

i. Developing and managing a Cybersecurity Information Sharing and Analysis Organization to liaise with the National Cybersecurity and Communications Integration Center within the US Department of Homeland Security, other federal agencies, and other public and private sector entities on issues relating to cybersecurity;

ii. Coordinating cybersecurity information sharing, performing cybersecurity threat analysis, and promoting shared and real-time situational awareness between and among the public and private sectors;

iii. Coordinating information sharing related to cybersecurity risks, warnings, and incidents, and providing support on cybersecurity incident response and cybercrime investigations;

iv. Providing information and recommending best practices on cybersecurity and resilience measures to public and private entities, including on information security and data protection;

v. Developing and implementing a cybersecurity threat information exchange with appropriate sources, including public utilities and private industry;

vi. Implementing and monitoring a centralized Security Information and Event Management (SIEM) system and, where appropriate, identifying, containing, or eliminating unauthorized activity and other cyber threats;

vii. Developing and managing an incident reporting system;

viii. Developing and providing information security incident response assistance and subject-matter expertise, as required;

ix. Providing cyber threat intelligence reports, analysis reports, briefings, alerts, and trainings to private and public organizations; and

x. Developing working relationships with external organizations, including law enforcement, the private sector, academia, Information Sharing and Analysis Organizations, Information Sharing and Analysis Centers, and regulatory authorities.

## 5.6 New Jersey Chief Data Officer (CDO)

The State CDO reports to the State CTO and serves as the central point of guidance, leadership, vision and coordination of statewide data standards across the Executive Branch. At the CTO's direction, the CDO coordinates the planning, implementation, governance and management of enterprise information and data initiatives. The State CDO fulfills the following responsibilities in support of the State's Information Security Program:

i. Establish, statewide procedures, standards, and best practices regarding the definition and identification of critical business data and datasets;

ii. Develop cross agency protocols for data sharing and integration;

iii. Monitor and ensure compliance with the statewide data procedures, standards, and policies;

iv. Providing subject-matter expertise for data issues and policy regarding information security;

v. Assist the State CISO to support, enable and implement the Information Security Management Program.

## 5.7 Heads of Executive Branch Departments and Agencies

Heads of State Agencies (includes Secretaries, Directors, Commissioners, Chairpersons, or equivalent head of a state entity within the Executive Branch of State Government) are responsible for their respective agency's operations. Likewise, they are responsible for the overall protection and use of information assets owned, managed, or licensed by the agency. To these ends, they are charged with:

i. Driving commitment and support for the information security program;

ii. Accepting risk on behalf of the agency;

iii. Assigning appropriate IT management responsibilities within their respective agency to a designee who has the responsibility for the implementation and management of information technology systems in support of agency goals and objectives, and in accordance with the Executive Branch of State Government Information Security Policies and Standards;

iv. Assigning appropriate responsibilities within their agency to a designee who has the authority and responsibility for ensuring the implementation of, and the adherence to the Information Security Program;

v. Promoting adherence to information security policies and cyber awareness programs.

## 5.8 Agency Chief Information Officer (CIO)

The Agency CIO shall be responsible for the direction, planning, and implementation of information technology systems in support of agency business goals and objectives. In accordance with NJOIT standards, directives, and enterprise information strategy, the agency CIO directs the planning and implementation of the agency's IT systems. The agency CIO does this through the following:

i. Design, acquisition, implementation, and operation of IT systems in compliance with approved policies and standards;

ii. Operation/Support of IT systems in compliance with approved security procedures, including, but not limited to:

1. *IT asset management;*
2. *Malware protection;*
3. *Patch management; and*
4. *Web proxying and Content filtering;*
5. *Secure file exchange;*
6. *Data encryption;*

iii. Management of third parties providing managed information services to the agency;

iv. Identity and access management;

v. Disaster recovery planning and operations in coordination with NJOIT;

vi. Providing recommendations regarding policy and control enhancements to NJOHSP's Division of Cybersecurity;

vii. Monitoring the agency IT environment and, where appropriate, identifying, containing, and eliminating unauthorized activity;

viii. Assisting in the implementation of the Cybersecurity Incident Response Plan;

ix. Executing the day-to-day security management of information, systems, and solutions through the application of controls as defined within the Information Security Policies and Standards;

x. Providing subject-matter expertise for technical issues regarding information security.

## 5.9 Agency Chief Information Security Officer (CISO)

The Agency CISO shall be responsible for protecting and maintaining the confidentiality, integrity, and availability of information assets under his/her purview. The Agency CISO fulfills the following responsibilities in support of the statewide Information Security Policies and Standards:

i. Identifying security requirements to limit cyber risks associated with the agency's business goals and objectives;

ii. Implementing and promoting information security awareness within their respective agency;

iii. Ensuring compliance with the Information Security Policies and Standards within their respective State agency, including, but not limited to:

1. *Coordination of risk assessments and compliance audits with NJOHSP's Division of Cybersecurity;*

2. *Coordination of vulnerability assessments of agency networks, applications, databases, and systems; and*

3. *Coordination of risk assessments of third parties having access to agency information assets;*

iv. In the implementation of the Information Security Incident Response Plan; and

v. Reporting all information security incidents to the NJCCIC.

# 6 Compliance and Enforcement

## 6.1 Compliance

Compliance with the policy will be monitored by the Information Security Governance Committee (ISGC).

## 6.2 Non-Compliance

Non-compliance will be referred to the ISGC for appropriate action.

# 7 Related Documents

- Statewide governance framework/model (Standard).
- Information Security Management Governance Procedure.

## 8 Policy Administration

This Policy is in force as of the effective date and does not expire unless superseded by another Policy.

The Policy must be reviewed annually, however the Director OHSP and CTO reserve the right to change or amend it at any time.

The Policy shall be administered and monitored by the New Jersey Chief Information Security Officer (CISO) and the NJOIT Deputy CTO for Policy.

## 9 Document History

| Version | Description of Modification | Publication Date |
|---|---|---|
| 1.0 | Original Publication Date | 10/18/2017 |
| 2.0 | Annual Review | 04/12/2023 |
| | | |
| | | |

****Printed copies of this document are uncontrolled; please refer to the NJOIT internet for the current version in effect.****