

# Technology Services Board Security Subcommittee

Date: Thursday, August 8, 2024

Time: 9:00 am - 11:00 am

Location: 1500 Jefferson St SE, Olympia, WA, 2<sup>nd</sup> floor, Room 2331

---

## Agenda

<b>9:00 am</b>	<b>Call to Order</b> <ul style="list-style-type: none"><li>Reminder of Joint meeting</li><li>Welcome New Members</li></ul>	<b>Ralph Johnson</b>
<b>9:10 am</b>	<b>Subcommittee Charter Review (<i>Discussion</i>)</b>	<b>Ralph Johnson</b>
<b>9:25 am</b>	<b>Policy &amp; Standard Review</b> <ul style="list-style-type: none"><li>SEC-06-01-S Identification and Authentication</li><li>SEC-04-09-S Endpoint Detection and Response Standard</li><li>SEC-10 Incident Response Policy</li></ul>	<b>Owner: Ralph Johnson</b> <b>SME: Kim Hort</b>
<b>9:35 am</b>	<b>OCS Highlights: Security Operations (<i>Discussion</i>)</b>	<b>Jack Potter</b>
<b>9:50 am</b>	<b>SLCGP Update (<i>Discussion</i>)</b>	<b>Zack Hudgins</b>
<b>10:00 am</b>	<b>Enterprise Strategic Plan: Security Alignment</b>	<b>Ralph Johnson</b>
<b>10:25 am</b>	<b>Executive session: RCW 42.105.291(4)</b>	<b>Board Members</b>
<b>10:50 am</b>	<b>Public Comment</b>	
<b>10:55 am</b>	<b>Closing Remarks &amp; Adjournment</b>	

# Identification and Authentication Background

## **New, Update or Sunset Review?** Sunset Review

### **What due diligence was conducted to determine the content of this policy/standard? If this is an update or sunset review, provide information as to what changes were made, if any, as well as reasons behind the policy/standard content.**

This standard expands on and replaces the current 141.10 (6.2, 6.3) requirements. Based on workgroup and community feedback, changes were made to improve clarity for agency adoption and accountability.

This policy's updates draw from the NIST 800-63 series publications: Digital Identity Guidelines, Enrollment and Identity Proofing, Authentication and Lifecycle Management, and Federation and Assertions.

### **What is the business case for the policy/standard?**

Ensuring the appropriate controls for identification and authentication of all organizational and non-organizational users and devices necessary for the conduct of state business.

### **What are the key objectives of the policy/standard?**

- Aligning the processes and tools used to link user and device identities to an account.
- Ensure authentication mechanisms are appropriate to the level of risk associated with the data category processed by the resource the user or device is authenticating to.
- Requiring detailed documentation of authentication methods and processes in the annual application inventory and the agency's security program, ensuring transparency and compliance.
- Managing user, group, role, service, and device identifiers to ensure unique and secure access controls, preventing unauthorized access and privilege escalation.

### **How does policy/standard promote or support alignment with strategies?**

#### [Enterprise Strategic Plan](#)

The digital trust pillar upholds and is interwoven in all of the 2023-2025 Enterprise IT Strategic plan goals.

This standard supports “Creating a Government Experience that Leaves No Community Behind” (Goal 2) by considering barriers to public access to data and security concerns when selecting authentication controls.

This standard also supports **Goal 3 “Innovative Technology Solutions Create a better Washington”** by emphasizing secure and inclusive access, leveraging secure technology, addressing systemic societal challenges, and supporting data-driven decision-making.

### **What are the implementation considerations?**

To ensure a smooth transition to the new authentication standards, it is essential to ensure that existing systems and applications are compatible with them, including MFA and encryption requirements. This involves assessing the current infrastructure to support new authentication mechanisms, such as additional servers or network upgrades.

Additionally, it is crucial to enhance helpdesk capabilities to assist users with the transition, including support for password resets and MFA enrollment. Detailed risk assessments are necessary to identify and mitigate potential threats related to the new authentication methods.

Creating channels for users to provide feedback on the new authentication processes will allow continuous improvement. Staying updated with the latest advancements in authentication technologies and incorporating them into the security framework as needed will help maintain their effectiveness and security.

### **How will we know if the policy is successful?**

**Specific:** Implement robust credential management and authentication policies to enhance security by reducing credential sharing incidents, achieving password security compliance, increasing MFA adoption, ensuring proper identity verification, minimizing credential exposure, and securing service accounts.

**Measurable:** Response. Enhance security by eliminating fraudulent identity incidents, attaining compliance with password policies, implementing MFA for all high-risk scenarios, verifying the identity of all IT systems users, minimizing temporary authenticator exposure, and ensuring all service accounts comply with duplicate account and password documentation requirements.

**Achievable:** Implement strict policies and provide education to prevent credential sharing; deploy tools and training for managing complex passwords; roll out MFA solutions with necessary support; establish a standardized identity verification process; automate the expiration of temporary credentials; and conduct regular audits to ensure service accounts meet security standards.

**Relevant:** Enhancing credential security reduces the risk of unauthorized access, identity fraud, and security vulnerabilities. Ensuring compliance with password policies, implementing MFA, verifying user identities, minimizing temporary authenticator exposure, and securing service accounts are critical measures to protect systems and data.

**Timely:** We will review the progress toward the objectives at the three-year sunset review mark.

**Equitable:** Ensure all employees, regardless of role or department, have equal access to security tools, training, and support. Apply security policies and processes consistently across the organization to maintain fairness and inclusivity.

**SEC-06-01-S**

State CIO Adopted: Month 1 2023

TSB Approved: Month 1 2023

Sunset Review: Month 1 2023

**Replaces:**  
IT Security Standard 141.10 (6.2, 6.3)  
December 11, 2017

januar

# IDENTIFICATION AND AUTHENTICATION SECURITY STANDARD

**See Also:**RCW [43.105.054](#) OCIO GovernanceRCW [43.105.205](#) (3) Higher EdRCW [43.105.020](#) (22) "State agency"See [NIST 800-63B](#) Digital Identity Guidelines - Identification and Lifecycle Management[SEC-08-01-S Data Classification Standard](#)

1. Agencies will establish and implement administrative procedures for issuing, replacing, and revoking credentials. Agencies are required to safeguard credentials by:
  - a. Prohibiting the sharing of user authentication credentials, such as usernames, passwords, or any other form of identification, to access systems.
  - b. Utilizing a secure password, [passphrase](#) or secrets management methodology for credentials not managed using agency directory services and documenting the method in the agency's security program, including but not limited to:
    - i. Directory Services Root credentials.
    - ii. API Keys.
    - iii. Built-in account, root, and system passwords/passphrases.
    - iv. Database root passwords.
    - v. Password manager/password vault master passwords.
    - vi. Encryption keys. See section 7 of [SEC-08-02-S Encryption Standard](#).
2. Agencies must manage [identifiers](#) for users, groups, roles, services, and devices by:
  - a. Requiring approval from designated agency staff to assign user, group, role, service, or device identifiers.

- b. Assigning a unique identifier to each user, group, role, service, or device.
- c. Preventing the reuse of identifiers for different users, groups, roles, services, and devices for a minimum of two years or longer as needed by agency compliance requirements. If a previously enrolled user, group, role, service, or device is re-enrolled, the same identifier should be reused to maintain continuity and avoid duplication.

**3. Agencies must manage the identity of users in the following manner:**

- a. Agencies must verify the identity of [organizational](#) IT system users before issuing credentials.
- b. Agencies must perform a risk assessment to determine the impact of a non-organizational user's fraudulent or compromised identity accessing data on internet-facing systems.
  - i. Agencies must establish and implement the necessary actions based on the risk assessment.
  - ii. Agencies must establish and implement processes to support objective measures for assessing the impact levels identified in the risk assessment.

**4. State IT systems must [authenticate](#) an identity prior to:**

- a. Permitting access to modify any data regardless of category.
- b. Providing access to category 2 data or higher.
- c. Except, agencies may allow users to submit data without authentication regardless of category classification if there is a business need. Documented processes for evaluating associated risk and validating and categorizing the data upon submission are required.

**5. Agencies must manage information system [authenticators](#) by:**

- a. Documenting the authentication methods for each system in the annual application inventory. See [MGMT-01-01-S Application Inventory](#).
- b. Requiring unique authenticators for all system access.
- c. Requiring unique temporary authenticators and requiring them to be changed immediately after first use to establish initial access.

- d. Changing the manufacturer's default authenticator before implementing an information system or component (e.g., routers, switches, firewalls, printers, etc.).
- e. Only storing or transmitting encrypted representations of authenticators. See the [SEC-08-02-S Encryption Standard](#).
  - i. [System administrators](#) may transmit initial account authenticators and/or resets.
  - ii. If encrypted transmission is unavailable, helpdesks must use a documented alternate communication method, such as phone, text, or voice communications, to transmit authenticators to users.
- f. For self-service password/passphrase reset systems, requiring users to validate their identity through designated, previously established verification methods, such as multi-factor authentication, to ensure secure access to systems and data, where technically possible.
  - i. When not technologically possible within a self-service password/passphrase reset system (i.e., helpdesk password resets, etc.), the agency must establish and implement alternate identity verification methods strong enough to prevent account compromise, identity theft and other fraudulent activities.
- g. Expiring unused temporary authenticators within 14 days.
- h. As soon as a password/passphrase is suspected to have been compromised, requiring a password reset.
- i. Enforcing minimum password/passphrase complexity of:
  - i. A minimum of eight (8) characters.
  - ii. A minimum of one (1) numeric and one (1) special character.
  - iii. Contain a mixture of at least one (1) uppercase and one (1) lowercase letter.
- j. [Setting](#) the password history to disallow the reuse of the last nine (9) passwords/passphrases.
- k. Enforcing a minimum password lifetime restriction of one (1) day, except for temporary passwords.

- l. Educating users to use significantly different passwords/passphrases at reset and enforcing best practices through technical controls where available.
- m. Establishing a maximum of five (5) incorrect login attempts and locking the account for a minimum of fifteen (15) minutes or until reset by an administrator.
  - i. Prior to unlocking an account, the user must be identified with the same assurance method used when performing a password reset referenced in [5.f.i.](#) above.
- n. Implementing session and token expiration as required by [SEC-02-01-S Application Security Standard](#) and documenting the process.
- o. Utilizing authentication certificates issued by a WaTech-approved Certificate Authority (CA) for all website security purposes. The use of self-signed certificates is not permitted without [waiver](#).
- p. Disabling and de-provisioning inactive accounts following the [SEC-06 Access Control Policy](#) requirements.

**6. Access to state [IT resources](#) or the State Government Network (SGN) requires authentication via the applicable enterprise solution and must employ the following minimum controls.**

- a. Authenticated access for [organizational users](#) requires authentication via the enterprise solution according to the [Identity Management User Authentication Standard \(183.20.10 section 4.2.1\)](#) with the following minimum controls:
  - i. [Password](#) expiration requirements must not exceed 120 days and must be documented in the agency security program; OR password length must be a minimum of 15 characters with a maximum 365-day expiration.
  - ii. MFA is recommended for all organizational user access. Verified authentication using MFA is required for high-risk scenarios as determined by the agency's risk assessment process.
    - 1. The outcomes of these evaluations and the final decision must be thoroughly documented.
    - 2. MFA is required for remote access. See the [SEC-06-02-S Remote Access Standard](#).

iii. [System administrator](#) accounts must be discrete and used only for administrative functions and must be managed with the following controls:

1. Passwords/passphrases must have a minimum length of 20 characters. Password/passphrase expiration must be every 60 days and meet standard complexity requirements.
2. [Multi-Factor Authentication \(MFA\)](#) is required for all system administrator accounts where technically possible. Compensating controls must be documented and implemented in the agency security program when not technically possible.
3. Built-in hosted or cloud service provider accounts may be used to establish and configure services, administrator accounts, and single sign-on (SSO) configurations.
4. Time-bound access and least-privileged authorization based on the duration needed to complete necessary activities are recommended to secure system administrator accounts.

iv. [Service accounts](#) must employ the following controls:


1. A discrete account used only for the defined privileges and functions. These accounts must never be used for interactive login. If an individual performs the set up and configuration of service accounts, the password must be reset whenever possible.
2. Passwords should be as long as possible ideally at least 20 characters balancing security with manageability. Complexity requirements should be adjusted to ensure they can be managed efficiently, especially for devices like desk phones. Password expiration policies must be documented in the agency's security program. Provisions must be made for non-expiring passwords when necessary, such as for desk phones to ensure reachability by emergency responders.
3. Authenticators and account secrets must be rotated whenever employees change roles and no longer require access, as feasible. In cases where physical changes are



impractical, alternative security measures must be considered and documented.

4. Service accounts must be limited to access only the systems and applications necessary for their functions, adhering to the principle of least privilege.
  5. Service accounts do not require MFA.
- b. Authenticated access for non-organizational users requires authentication via the enterprise service according to the [Identity Management User Authentication Standard \(183.20.10 4.2\)](#) with the following minimum controls:
- i. Password expiration is not to exceed 13 months.
  - ii. MFA is required for:
    1. Access to all category 4 data.
    2. Access to Category 3 data that is not the authenticated user's own personal information.
  - iii. MFA is recommended for access to category 3 data that is the authenticated user's own personal information.
- 7. When applicable, WaTech's Office of Cybersecurity will support agencies in determining secure configuration requirements for [federated](#) single sign-on integrations as part of the security design review process. See the [SEC-02 Security Assessment and Authorization Policy](#).**
- 8. Agencies unable to utilize the designated enterprise service must file a waiver request and implement security controls designated in this standard or equivalent WaTech-approved controls. See [POL-01-01-PR Technology Policies and Standards Waiver Procedure](#).**
- 9. Agencies must consider events that may cause a failure of established identification and authentication mechanisms.**
- a. As part of [SEC-12 IT Disaster Recovery Planning](#) and/or [Continuity of Operations Planning \(COOP\)](#), agencies must identify and document possible scenarios and procedures for modified identification and authentication mechanisms to facilitate operations in emergency situations.

**10. Beginning January 1, 2026, password length and expiration requirements discussed in 6.a. above will increase.**

- a. Password length will increase to a minimum of 15 characters.
- b.  Password expiration will increase to a maximum of 365 days.
- c. All other requirements will remain in effect.

**REFERENCES**

1. [Definition of Terms Used in WaTech Policies and Reports.](#)
2. [NIST 800-63B Digital Identity Guidelines - Authentication and Lifecycle Management.](#)
3. [SEC-02 Security Assessment and Authorization Policy.](#)
4. [POL-01-01-PR Waiver Request Procedure.](#)
5. [Organizational User Identity Management & User Authentication Enterprise Service Standard \(183.20.10 4.1\).](#)
6. [Non-Organizational User Identity Management & User Authentication Enterprise Service Standard \(183.20.10 4.2.1\).](#)
7. [NIST 800-63-3 Digital Identity Guidelines.](#)
8. [SEC-06-02-S Remote Access Standard.](#)
9. [NIST 800-53 Security and Privacy Controls for Information Systems and Organizations.](#)
10. [NIST 800-63A Enrollment and Identity Proofing.](#)
11. [NIST 800-63C Federation and Assertions.](#)
12. [Encryption Standard.](#)
13. NIST Cybersecurity Framework Mapping:
  - PROTECT.ACCESS CONTROL-6: Identities are proofed and bound to credentials and asserted in interactions.
  - PROTECT.ACCESS CONTROL-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)

**CONTACT INFORMATION**

- For questions about this policy, please contact the [WaTech Policy Mailbox](#).

**PROPOSED DEFINITIONS**

- **Identifier:** A sequence of characters used to identify or refer to a person, object, device, organization, etc. Depending on the application, it may be an

identifying name or something more abstract (e.g., a string consisting of an IP address and timestamp).

- **Authenticator:** Something the claimant possesses and controls or knows (typically a cryptographic module or password) that is used to authenticate the claimant's identity. This was referred to as a token in previous SP 800-63 editions. (adapted from NIST)
- **Organizational User:** An employee or an individual whom the organization deems to have equivalent status to an employee, including a contractor, guest researcher, or individual detailed from another organization. Policies and procedures for granting the equivalent status of employees to individuals may include need-to-know, relationship to the organization, and citizenship.
- **Service Accounts:** Service accounts are a special type of non-human privileged account used to execute applications and run automated services, virtual machine instances, and other processes.
- **System Administrator:** Individual who implements approved secure baseline configurations, incorporates secure configuration settings for IT products, and conducts/assists with configuration monitoring activities as needed.
- **Passphrase:** A passphrase combines words, numbers, and symbols to secure online accounts or systems. Unlike traditional passwords, which are typically shorter and composed of random characters, passphrases are longer and can be easier to remember.
- **Interactive Login:** The process by which an end-user actively engages with a system's login interface to gain access. This involves manually entering their credentials into the login screen, such as a username and password/passphrase. The system then authenticates these credentials to verify the user's identity and initiates a session if the credentials are valid.

## Endpoint Detection and Response Background

**New, Update or Sunset Review?** Sunset Review. Replaces Section 5.7.

**What due diligence was conducted to determine the content of this policy/standard? If this is an update or sunset review, provide information as to what changes were made, if any, as well as reasons behind the policy/standard content.**

**Changes were made based on workgroup and community feedback to improve clarity for agency adoption and accountability.**

Updates to this policy draw from [NIST SP 800-83r1 Guide to Malware Incident Prevention and Handling for Desktops and Laptops](#).

**What is the business case for the policy/standard?**

Protecting the state government network from malicious software prevents serious breaches of security including loss of availability, confidentiality, and integrity of state systems and data.

**What are the key objectives of the policy/standard?**

- Require agencies to implement anti-malware protection and address malware prevention, detection, and removal.
- Require agencies to report endpoint detection response logging information to the state enterprise Security Information and Event Management (SIEM) Service.

**How does policy/standard promote or support alignment with strategies?**

This standard aligns with WaTech's pillar of "Security, Privacy, and Digital Trust" and with the enterprise IT strategic pillar of Digital Trust.

**What are the implementation considerations?**

WaTech offers an endpoint detection and response service that agencies may leverage to meet this standard.

**How will we know if the policy is successful?**

**Specific:** Agencies will ensure malware detection and prevention software is deployed and kept current on all state-issued devices.

**Measurable:** Agencies can validate that all devices are running appropriate software. WaTech can measure the number of logs reported to the SIEM.

**Achievable:** WaTech offers a solution for this, and agencies should already have implemented software.

**Relevant:** Attempts to breach state security are on the rise due to improved technology leveraged by threat actors.

**Timely:** This standard is effective when adopted.

**Equitable:** WaTech offers a solution to ensure all agencies are successful with implementing malware protection.

## ENDPOINT DETECTION AND RESPONSE STANDARD

**See Also:**

RCW [43.105.054](#) OCIO Governance  
RCW [43.105.205](#) (3) Higher Ed  
RCW [43.105.020](#) (22) "State agency"  
SEC-06 Access Control Policy

1. Agencies must deploy an [Endpoint Detection and Response \(EDR\)](#) solution on state-issued [endpoints](#) and where possible configure reporting into the Enterprise Security Information and Event Management (SIEM) service. See [SEC-09-01-S Security Logging Standard](#).
  - a. Agencies must keep EDR agents and components up-to-date (N-1 version) on state-issued endpoints. The SEC-04-06-S Mobile Device Security Standard provides additional security requirements for devices.
  - b. Agencies must document and standardize the deployed EDR's configuration following industry standards and manufacturer's best practices. This includes, but may not be limited to: scanning frequency, inbound and outbound malware detection settings, Host Intrusion configurations, etc.
2. Agencies must configure the EDR to provide anti-malware protection and address malware prevention, detection, and removal.
  - a. Agencies must implement detection, prevention, and recovery controls to protect against malicious code.
  - b. Agencies must examine file transfers, email, and web browser-based traffic for malicious and inappropriate content.
3. Agencies must set requirements for malware protection for non-state issued endpoints used for work purposes in accordance with the [SEC-04-07-S Non-Agency Issued Device Security Standard](#).

### REFERENCES

1. [Definitions of Terms Used in WaTech Policies and Reports](#)
2. [SEC-09-01-S Security Logging Standard](#)
3. [SEC-04-06-S Mobile Device Security Standard](#)
4. [SEC-04-07-S Non-Agency Issued Device Security Standard](#)

5. [NIST SP 800-83r1 Guide to Malware Incident Prevention and Handling for Desktops and Laptops](#)
6. [SEC-05-02-S Remote Access Standard](#)
7. [SEC-09-01-Security Logging Standard](#)
8. NIST Cybersecurity Framework Mapping:  
Protect.Data Security (PR.DS-6): Integrity checking mechanisms are used to verify software, firmware, and information integrity.  
Protect.Maintenance (PR.MA-2): Remote maintenance of organizational assets is approved , logged, and performed in a manner that prevents unauthorized access.  
Detect.Security Continuous Monitoring (DE.CM-4): Malicious code is detected.  
Respond.Analysis (RS.AN-3): Forensics are performed.

## CONTACT INFORMATION

- For questions about this policy, please email the [WaTech Policy Mailbox](#).
- For technical assistance, please email <mailto:riskmanagement@watech.wa.gov>

## PROPOSED DEFINITIONS:

### Endpoint Detection and Response (EDR)

A cybersecurity technology that continually monitors an "endpoint" to mitigate malicious cyber threats. See "[Endpoint](#)."

## Incident Response Policy Background

**New, Update or Sunset Review?** Response.

**What due diligence was conducted to determine the content of this policy/standard? If this is an update or sunset review, provide information as to what changes were made, if any, as well as reasons behind the policy/standard content.**

This policy was developed with a workgroup derived from the Enterprise Security Governance group. The document is informed by the RCW, as well as NIST industry standards.

**What is the business case for the policy/standard?**

"A failure to plan is planning to fail." - Attributed to Benjamin Franklin.

This document is necessary for ensuring a coherent and cohesive response to cybersecurity incidents that can cause irreparable harm to critical data and infrastructure.

**What are the key objectives of the policy/standard?**

- Ensure enterprise framework for incident response actions that affect critical data and infrastructure.
- The enterprise incident response plan will be used as a model by agencies.
- Agencies will create agency-level incident response plans that align to the enterprise incident response plan.

**How does policy/standard promote or support alignment with strategies?**

This policy supports WaTech's strategic plan goal for statewide technology leadership by ensuring WaTech is supporting agencies in a cybersecurity incident, especially for high-impact incidents.

**What are the implementation considerations?**



Agencies will need support to develop their documentation. WaTech will create a template in addition to the model plan to support development of agency incident response plans.

Agencies will also need to support training for employees who will execute the plan in the event of an incident.

### How will we know if the policy is successful?

**Specific:** Agencies will develop and implement an incident response plan tailored to the needs of supported organizations/departments, outlining procedures for identifying, containing, and mitigating cybersecurity incidents. Agencies will support training for all relevant teams.

**Measurable:** Agencies will achieve a 100% completion rate of incident response plan documentation and training for all relevant internal agency teams.

**Achievable:** WaTech will provide a template and support for agency policy alignment. Agencies will utilize their plans in the event of an incident and update their plan.

**Relevant:** Cyber attacks are on the increase, and incidents will happen. Planning in advance is the best way to reduce the impact of cybersecurity incidents.

**Timebound:** This policy is in effect when adopted. This includes all phases of the incident response lifecycle.

**Equitable:** This policy aims to consider the needs of all agencies, and in the incident response plan the agencies will be directed to consider the needs of underserved communities when responding to incidents and developing equitable.

**SEC-10**  
State CIO Adopted:  
TSB Approved:  
Sunset Review:



**Replaces:**  
IT Security Standard 141.10 (10)  
December 11, 2017  
IT Security Incident  
Communication 143  
December 10, 2014

## **IT SECURITY INCIDENT RESPONSE POLICY**

**See Also:**

RCW [43.105.450](#) Office of Cybersecurity  
RCW [43.105.054](#) WaTech Governance  
RCW [43.105.020](#) (22) "State Agency"  
RCW [43.105.205](#) (3) Higher Ed  
RCW [38.52.030](#) Continuity of Government Operations Preparation  
Governor's Directive [13-02](#) Continuity of Government Operations Preparation

- 1. WaTech will provide an Enterprise Incident Response Plan (EIRP) that delineates state and agency responsibilities.**
- 2. WaTech will provide a template incident response plan guideline for agencies.**
- 3. Agencies must establish, maintain, document, and distribute an agency-level incident response plan (AIRP) that aligns with the EIRP.**
  - a. Agencies must keep multiple copies of the AIRP plans online and offline. Offline copies can be physically (printed) or digitally (USB/removable media) stored and must be kept secure. See the [SEC-08-02-S Encryption Standard](#) and the [SEC-07 Physical and Environmental Protection Policy](#).
  - b. Staff required to execute the plan must have access to both online and offline copies.
  - c. Agencies must incorporate Incident Command System (ICS) principles into their incident response processes. See ICS 100, 200, 300 [ICS Resource Center \(fema.gov\)](#).
  - d. The agency must redistribute the plan when updated.
- 4. At a minimum, the AIRP must address the following:**
  - a. Define incident response roles and responsibilities relating to both agency-specific and enterprise incidents.
  - b. Assign specific agency incident response roles and responsibilities.
  - c. Communication and contact processes that align with the EIRP.

- d. Reference or include [Continuity of Operations Plan \(COOP\)](#), [Disaster Recovery](#) Plan(s) and data backup processes. See [Data Backup and Recovery](#) and [Disaster Recovery Planning](#).
  - e. Escalation procedures that align with EIRP.
  - f. Staff training, both technical and end user training, to meet incident response responsibilities. See the [IT Security and Privacy Awareness Training Policy](#).
- 5. Agencies must incorporate the AIRP in the agency IT Security Program.**
- a. Agencies must exercise the plan annually to test the effectiveness of the plan, the training, and to identify areas for improvement.
  - b. Agencies must develop processes to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.
- 6. Agencies must report cybersecurity incidents to WaTech according to the EIRP.**
- 7. WaTech’s Security Operations Center (SOC) must investigate agency-reported incidents to confirm the severity, conduct reporting and notification, and coordinate incident management according to the EIRP.**
- 8. The State CISO will appoint an Incident Commander who convenes the Enterprise Cybersecurity Incident Response Team eCIRT as defined by the EIRP.**
- 9. The eCIRT coordinates and approves all communications related to enterprise security incidents according to the EIRP. This includes communications from WaTech and impacted agencies.**
- a. State CISO will notify the state CIO and the Office of Privacy and Data Protection (OPDP) according to the EIRP.
  - b. The state CIO will notify the Governor’s office that an incident has occurred and may require public notification according to the EIRP.
  - c. Agencies will fully cooperate with the Governor’s office in support of disclosure of the incident and will coordinate with the eCIRT.

## REFERENCES

1. ICS 100, 200, 300 [ICS Resource Center \(fema.gov\)](#).

2. SEC-01-01-S [Data Backup and Recovery Standard](#).
3. SEC-12 [Disaster Recovery Planning](#).
4. SEC-03 [IT Security and Privacy Awareness Training Policy](#).
5. NIST Cybersecurity Framework Mapping:
  - Respond.Response Planning-1 (RS.RP-1): Response plan is executed during or after an event.
  - Respond.Communications-2 (RS.CO-2): Events are reported consistent with established criteria.
  - Respond.Communications -5 (RS.CO-5): Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.
  - Respond.Analysis-1 (RS.AN-1): Notifications from detection systems are investigated.
  - Respond.Analysis -2 (RS.AN-2): The impact of the incident is understood.
  - Respond.Analysis -3 (RS.AN-3): Forensics are performed.
  - Respond.Analysis -4 (RS.AN-4): Incidents are categorized consistent with response plans.
  - Respond.Mitigation-1 (RS.MI-1): Incidents are contained.
  - Respond.Mitigation-2 (RS.MI-2): Incidents are mitigated.
  - Respond.Improvements-1 (RS.IM-1): Response plans incorporate lessons learned.
  - Respond.Improvements-2 (RS.IM-2): Response strategies are updated.
  - Recover.Communications-1 (RC.CO-1): Public relations are managed.
  - Recover.Communications-2 (RC.CO-2): Reputation after an event is repaired.
  - Recover.Communications-3 (RC.CO-3): Recovery activities are communicated to internal stakeholders and executive and management teams.

## CONTACT INFORMATION

- For questions about this policy, please contact the [WaTech Policy Mailbox](#)
- For technical questions, contact [WaTech's Risk Management Mailbox](#).

## CURRENT vs. PROPOSED DEFINITIONS:

### CURRENT:

#### A security **incident** is:

Any attempted, successful, or imminent threat of unauthorized electronic and/or physical access, use, exposure, disclosure, breach, modification, loss, or destruction of information; interference with Information Technology operations; or significant

violation of agency or state policy.

**PROPOSED:**

**A cybersecurity incident is:**

Any attempted, successful, or imminent threat of unauthorized electronic and/or physical access, use, exposure, disclosure, ~~breach~~, modification, loss, or destruction of information; interference with Information Technology operations; or significant violation of agency or state policy.