WaTech
Washington Technology Solutions

Technology Service Board (TSB) - Security Subcommittee Meeting

Date: December 4, 2024
Time: 1:00 pm – 2:00 pm
Location: **In-person** - 1500 Jefferson St SE, Olympia, WA, 2nd Floor Conference Room 2331
Virtual - Zoom (see info below)

Agenda

1:00 pm	**Call to Order** • Roll Call • Approval of August 8, 2024 Minutes (Vote)	**Ralph Johnson** **Bill Kehoe**
1:05 pm	**Discussion: Enterprise IT Strategic Plan**	**Ralph Johnson**
1:15 pm	**Member Discussion: Security & Privacy and AI**	**Matt King**
1:25 pm	**Election Security Review**	**Ian Moore**
1:35 pm	**Policy/Standards for Voting:** • SEC-01 Cybersecurity Program Policy (Vote) • SEC-04-08-S Unsupported Technology Retirement Standard (Vote) • SEC-10-01 Traffic Light Protocol Standard (Vote)	**Ralph Johnson**
1:45 pm	**Executive Session: RCW 42.105.291(4) (Closed Session)**	**Ralph Johnson** **Tristan Allen**
1:55 pm	**Public Comment**	
2:00 pm	**Adjournment**	

WaTech
Washington Technology Solutions

Join Zoom Meeting

https://watech-wa-gov.zoom.us/j/81434617527?pwd=UjRI71zhSjipnb4lkuE0CaDdtfLbdM.1

Meeting ID: 814 3461 7527

Passcode: 961328

Dial by your location:

- +1 253 215 8782 US (Tacoma)
- +1 253 205 0468 US

WaTech
Washington Technology Solutions

Technology Services Board (TSB)
Security Subcommittee Meeting Minutes

August 8, 2024

Call to Order

Ralph Johnson opened the August 2024 meeting of the Technology Services Board, welcoming attendees and expressing gratitude to the members for their commitment to the committee, highlighting the group's potential to achieve impactful work in the coming months and years.

Ralph reminded attendees of the requirement under RCW 43.105.291 for the committee to meet jointly with the Military Department's Cybersecurity Advisory Committee. The closed meeting, scheduled for **September 26th**, will focus on drafting the **joint cybersecurity report** due to the Governor's Office and select legislative committees by **December 1st**.

TSB Security Subcommittee Charter Review

Ralph reviewed the TSB Security Subcommittee charter, which guides the group in advising the Technology Services Board on cybersecurity, addressing risks, and fulfilling RCW 43.105.291 objectives. Members are expected to attend quarterly meetings, maintain confidentiality, and collaborate effectively. The charter will be reviewed annually, with collaboration supported by WaTech's administrative team.

Policy & Standard Review

Three policies and standards were reviewed by Ralph:

1. **SEC-06-01-S: Identification of Standards**
   Focuses on controls for identifying and authenticating users to state systems, including multi-factor authentication, password management, and credential handling.
2. **SEC-04-09-S: Endpoint Detection and Response Standard**
   Requires endpoint security for state-issued and personal devices used for state business, with reporting to the Security Operations Center.
3. **SEC-10: Incident Response Policy**
   Establishes an enterprise incident response framework for agencies to adapt, defining incident types, communication protocols, and documentation requirements.

With no objections, all were approved to move to the Technology Services Board for review.

OCS Highlights: Security Operations

Deputy CISO Jack Potter outlined the Security Operations Center's role in centralized security, incident response, and collaboration under RCW 43.105.450. He highlighted evolving threats like phishing, vulnerabilities, and AI-driven attacks, and detailed the SOC's tools, 24/7 monitoring, and forensics support.

State & Local Cybersecurity Grant Program Update

Bill Kehoe presented on the State and Local Cybersecurity Grant Program, highlighting its role in funding local government and tribal cybersecurity initiatives. With $17M allocated over four years, the program supports critical projects, particularly for under-resourced rural areas, to address vulnerabilities and ransomware threats. In its second round, the program approved 125 of 189 applications, distributing $5.3M. Bill emphasized the strong collaboration between WaTech, the Military Department, and local governments, ensuring a united front against cyber threats.

Enterprise Strategic Plan: Security Alignment

Ralph presented how the state's cybersecurity governance aligns with the broader enterprise IT strategic plan, emphasizing four key pillars: shared governance, digital trust, service excellence, and equitable outcomes. He explained that the Office of Cybersecurity (OCS) aims to integrate its goals with the strategic plan through upcoming workshops and collaborative efforts with state agencies. Notably, cybersecurity, while not a standalone goal, is embedded across all pillars under the concept of digital trust. Ralph highlighted the importance of fostering public confidence in digital services, improving service delivery, leveraging data for decision-making, addressing technology debt, and enhancing workforce training. The vision is to position Washington as a national model for cybersecurity, ensuring secure, seamless operations while prioritizing customer focus, reliability, and innovation.

10:25 am - Executive Session

An executive session was held for 25 minutes to discuss sensitive security topics and information pursuant to RCW 43.105.291(4). The session closed at 10:50 am; no action was taken.

Public Comment

No public comments were received.

Adjournment

With no further business before the board, the meeting was adjourned at 11:00 am. The next meeting is scheduled for December 4, 2024.

Submitted by: Leanne Woods, Board and Committee Program Administrator

SEC-04-08-S
State CIO Adopted: Month 1 2024
TSB Approved: Month 1 2024
Sunset Review: Month 1 2024

[5]

WaTech
Washington Technology Solutions

Replaces:
IT Policy 186
Commonly Used Software Retirement
December 11, 2017
PC Procurement Policy 201
PC Procurement Guideline 201.10
September 30, 2013

UNSUPPORTED TECHNOLOGY RETIREMENT STANDARD

See Also:
RCW 43.105.054 WaTech Governance.
RCW 52.105.450 Office of Cybersecurity
RCW 43.105.020 (22) "State agency".
RCW 43.105.052 Powers and duties of agency—Application to higher education, legislature, and judiciary.
Executive Order on Improving the Nation's Cybersecurity
NIST SP 800-218 Secure Software Development Framework

1. **Agencies must maintain an awareness of software and hardware product roadmaps. See Center for Internet Security (CIS) End-of-Support Software Report List and vendor product lifecycle roadmaps. Agencies must:**

    a. Maintain all software and hardware used for state business at a version within the support lifecycle of the vendor or manufacturer. See NIST 800-53r5, SA-22 control. The latest version is preferred where multiple software versions are within the support lifecycle.

    b. Document a retirement plan for transitioning away from any product versions approaching the End of Support (EoS) within one year of the end-of-support date.

        i. Agencies will conduct a risk assessment and document the continued use of software and hardware beyond the end of support.

        ii. Include the software and hardware retirement plan within their Risk Treatment Plan in accordance with the SEC-11 Risk Management Policy.

        iii. Assign resources to support the agency software and hardware retirement plan.

    c. Discontinue the use of hardware before the product's End of Life (EoL).

    d. Include language in agency contracts to require vendors to maintain software and hardware at the current version.

2. **During the annual certification required by POL-01 Technology Policies, Standards, and Procedures:**

a. As part of the application inventory Technology Portfolio Foundation - Applications, agencies will submit a complete software inventory reporting whether versions of software installed on agency assets are within the vendor supported lifecycle.

b. As part of the MGMT-01-02-S Technology Portfolio Foundation - Infrastructure agencies will submit a complete hardware inventory reporting whether versions of hardware installed are within the vendor supported lifecycle.

3. **Agencies must submit a waiver request when needing to operate software or hardware beyond the support lifecycle.**

REFERENCES

1. NIST 800-53r5, SA-22 control.
2. Definition of Terms Used in WaTech Policies and Reports.
3. CIS End-of-Support Software Report List.
4. POL-01 Technology Policies, Standards, and Procedures
5. Technology Policies and Standards Waiver Procedure
6. NIST Mapping:
   - Protect.Data Security-3 (PR.DS-3): Resources are prioritized based on their classification, criticality, and business value.
   - Protect.Information Protection Processes and Procedures-1 (PR.IP-1): Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.
   - Detect.Security Continuous Monitoring-7 (DE.CM-7): Monitoring for unauthorized personnel, connections, devices, and software is performed.

CONTACT INFORMATION

- For questions about this policy, please email the WaTech Policy Mailbox.

PROPOSED DEFINITIONS:

Software
Computer programs and associated data that may be dynamically written or modified during execution. Includes firmware and drivers.

End of Life (EoL)
End of Life (EoL) refers to the point at which a product is no longer sold or produced

by the company. It usually follows the end of support. The product is considered obsolete and is fully retired. There is no official support or updates provided.

Support Lifecycle
The support life cycle refers to the period during which a product or service is supported by its provider. This includes the availability of updates, patches, and customer service. The support lifecycle ensures that users have a predictable timeline for support and can plan for upgrades or transitions accordingly.

WaTech
Washington Technology Solutions

Unsupported Technology Retirement Policy 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.

The Commonly Used Software Retirement Policy included a list of required software that must be updated and encourages agencies to update other software not on the list. This policy removes the list and requires agencies to maintain awareness of their software's development lifecycle for all applications. References to federal guidance are provided.

The PC Procurement Policy required a four-year lifecycle for Personal Computer purchases over $20,000. DES procurement policies still cover PC procurement generally. This policy now requires that agencies manage and plan for all hardware lifecycles and replace IT equipment before the end of the vendor's support.

What is the business case for the policy/standard?

When software or hardware is unsupported, vulnerabilities typically cannot be patched, and business and technical problems are not resolved with support from the vendor. Managing the lifecycle of software and hardware is integral to a functioning technical space.

What are the key objectives of the policy/standard?

Agencies will replace software and hardware before it reaches vendor end of support to avoid security concerns and equipment failure.

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

This policy supports the Enterprise Strategic Plan Goal #1: Create a Government Experience that Leaves No Community Behind. By ensuring software and hardware are up to date, we are better able to ensure continued access to services. It also supports Goal #2 Better Data, Better Decisions, Better Government, Better

Washington. By tracking the product lifecycles, we are better able to make long term decisions and plan for replacement hardware and software.

What are the implementation considerations?

The Application Inventory and Infrastructure inventory will need updates.

Agencies will need to plan to collect more specific data regarding the vendor supported lifecycle.

Agencies are likely to file more waivers for hardware and software.

Agencies will need to document and implement a plan for product lifecycles and to provide resources to support it.

How will we know if the policy is successful?

Specific: Agencies will be aware of software development lifecycles for all agency software.
Measurable: Software will be replaced before becoming unsupported.
Achievable: Agencies will track software development lifecycles and maintain a replacement plan.
Relevant: Old software with unpatched vulnerabilities leaves a door open for bad actors.
Timebound: This policy is effective when adopted.
Equitable: Ensuring software is supported means it will be better able to serve more people without unexpected failures.

WaTech
Washington Technology Solutions

SEC-01 Cybersecurity Program Policy 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.

The SEC-01 Cybersecurity Program Policy rewrites Policy 141 Securing Information Technology Assets, which was last revised on January 10, 2008. This new policy follows the POL-01-01-S Naming Convention Standard and incorporates elements from the previous 141.10 Securing Information Technology Assets Standard.

The policy ensures compliance with relevant Washington State laws and regulations, including RCW 43.105.054 Information Technology Governance – powers and duties of agency, RCW 43.105.052 Powers and duties of agency—Application to higher education, legislature, and judiciary.
, RCW 43.105.020 (22) Definitions "State Agency", RCW 52.105.450 (6, 8) Office of Cybersecurity – Higher education, Judicial, and Legislative, and RCW 42.56.420 Security.

What is the business case for the policy/standard?

The policy defines the cybersecurity program and its components. This is necessary to ensure agencies are preparing their agencies to protect IT assets, maintain compliance with Washington State Laws and regulations, and align with industry best practices. By establishing clear guidelines and standards, the policy helps agencies manage cybersecurity risks, respond effectively to incidents, and safeguard sensitive information and systems.

What are the key objectives of the policy/standard?

- Define the state and agency cybersecurity program requirements.
- The policy sets the tone for a holistic chapter of IT security policies and standards to protect sensitive IT assets and meet regulatory compliance, reducing the risk of cyberattacks, maintaining business continuity, promoting a security culture, identifying cost savings and supporting strategic goals with the aim of enhancing the overall reputation of Washington state.

- Emphasize the importance of equity and accessibility to ensure fair treatment and inclusive access to secure systems for all authorized users.
- Adopt industry best practices from recognized standards.
- Require regular reviews and updates to keep the cybersecurity program effective against evolving threats and technological advancements**.**

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

This Cybersecurity Program Policy supports the pillars of Digital Trust and Shared Governance by ensuring agencies are working together to protect state digital assets through partner cybersecurity programs lead by the state's Chief Information Security Officer.

The policy supports RCW 52.105.450 (3j, 7a) Office of cybersecurity—State chief information security officer—State agency information technology security, which requires each state agency to review and update its program annually, certify to the office of cybersecurity that its program is in compliance with the office of cybersecurity's security standards and policies, and provide the office of cybersecurity with a list of the agency's cybersecurity business needs and agency program metrics. It also outlines higher ed, judiciary, and legislative application of the policy.

What are the implementation considerations?

This policy requires agencies to update their policies and standards to reflect the cybersecurity controls required and to document and test their implementation including plans to mitigate risk.

Agencies will also need to report their compliance to policies and standards in future annual certification surveys. Agencies may need to file waivers while working toward compliance.

Agencies may need to consider adjustments to ensure the policy is effectively integrated into agency operations, providing robust protection for IT Assets and supporting the agency's strategic goals. This includes, but is not limited to:

- Resource Allocation
- Training
- Technical Infrastructure
- Risk Management
- Compliance, Monitoring, Incident Response

- Communication
- Vendor Management
- Change Management,
- Equity and Accessibility.

How will we know if the policy is successful?

Specific: Agency cybersecurity will align with the state enterprise cybersecurity program.
Measurable: Risk registers and plans of action and milestones (POAM) accurately reflect each agency's risk and are reported as required to WaTech annually.
Achievable: WaTech will support agencies by offering risk assessment and risk register/POAM templates. WaTech will continue to offer office hours, workgroups, committees, and will support agencies through consultations and Security Design Reviews.
Relevant: The policies and standards provided by WaTech reflect current best practices. Cyber threats continue to evolve with new advancements in technology, including artificial intelligence.
Timely: This policy is effective when adopted and will be reviewed within the three-year sunset review timeline. We will also review the effectiveness annually with the annual certification results.
Equitable: Community response is part of the development and review process of the policies, standards, and auditing process to ensure that no undue burden is placed on an agency and does not detract from their resources needed for daily operations. Cybersecurity protects vulnerable populations from exploitation of data exposure

SEC-01
State CIO Adopted: Month 1 2023
TSB Approved: Month 1 2023
Sunset Review: Month 1 2023

WaTech
Washington Technology Solutions

Replaces:
IT Policy 141
Securing Information Technology Assets
October 1, 2011
IT Standard 141.10 (1.1, 2.1-2.5)
November 13, 2017

WASHINGTON STATE CYBERSECURITY PROGRAM POLICY

See Also:
RCW 43.105.054 WaTech Governance.
RCW 43.105.020 (22) "State agency".
RCW 43.105.052 Powers and duties of agency—Application to higher education, legislature, and judiciary.
RCW 52.105.450 (6, 8) Office of Cybersecurity – Higher education, Judicial, and Legislative
RCW 52.105.450 (3j, 7a) Office of Cybersecurity – Agency IT Security Program
RCW 42.56.420 Security

1. **WaTech will establish enterprise information security programs, policies, and standards to provide the foundation for managing cybersecurity risk and maintaining compliance with applicable laws, regulations, contractual obligations, and alignment with industry standards.**

2. **WaTech and agencies should base information security programs, policies, standards, and technological decisions on information security and architectural principles. See SEC-01-01-G Security Principles Guideline.**

3. **The IT security policies and standards in this chapter apply to the executive branch agencies of the state of Washington, as well as agencies headed by separately elected officials, referred to in this and other policies and standards as "agencies."**

4. **The IT security policies and standards in this chapter apply to any entity using WaTech services in relation to the provided service(s).**

5. **State agencies will adhere to all WaTech policies and standards.**

    a. Institutions of higher education, legislative, and judiciary agencies are not directly subject to Washington state IT security policies and standards but must develop comparable documents appropriate to their respective missions and consistent with the intended outcomes of WaTech's security policies and standards to minimize cyber risks and secure data, systems and infrastructure.

    b. Agencies are responsible for adherence to these IT security policies and standards to protect IT systems and applications whether they are operated by or for an agency, and whether they operate internally on the State Government Network (SGN) or external to the SGN. Examples of environments external to the SGN include the Inter-Governmental Network

(IGN), the Public Government Network (PGN), business partner hosted services, and cloud services.

c. The IT security policies and standards outlined in the security chapter of the Washington State IT policies are the minimum requirements for state agencies. Agencies may create additional policies, standards, and controls based on their specific needs, as long as they do not conflict with the policies and standards in this chapter.

d. WaTech's Office of Cybersecurity (OCS) is responsible for interpreting policies and standards within the security chapter of the Washington State IT Policies. OCS will negotiate the implementation of compensating controls with agencies to ensure cybersecurity risks are reduced to an acceptable level..

e. Non-enforcement of any requirement in this or any information security policy or standard within the Security chapter does not imply consent of non-compliance by WaTech, OCS, or agency management.

6. **Each agency must develop and implement an agency cybersecurity program containing IT security policies, standards, procedures, and all necessary program-related documents.**

a. The agency will review this program at least annually and make appropriate updates after any significant change to its business operations, or information technology environment.

b. Agency Cybersecurity Program documentation must, at a minimum, include:

i. Alignment with the agency's risk management program and strategy.

ii. Clearly identified security objectives for agency systems.

iii. Policies, standards, and procedures in alignment with Washington State enterprise IT policies, standards, and applicable regulatory and contractual obligations.

iv. Details in proportion to the size, complexity, potential risk, and business exposure based on the agency's risk assessment results.

v. Details of the security controls applied to agency systems.

vi. Details, justifications, and waivers from WaTech regarding any deviation from state security policies or standards. POL-01-02-S Technology Policy & Standard Waiver Request Standard.

vii. Records from risk and security assessments and evaluations.

viii. Mechanisms for receiving, documenting, and responding to reported security issues.

7. **Agency heads and CIOs will attest in an annual certification to WaTech that the agency has developed and implemented the agency's Information Technology Security Program and that the program complies with all enterprise information security policies and standards. See POL-01 Technology Policies, Standards, and Procedures Policy.**

8. **Agencies will maintain systems, networks, and applications to minimize risks to:**

    a. **Confidentiality:** Protecting information from unauthorized access and disclosure.

    b. **Integrity:** Confirming that data remains accurate, complete, and unaltered during storage, processing, and transmission.

    c. **Availability:** Systems, networks, and data are accessible to authorized users when needed.

    d. **Compliance:** Adhering to relevant laws, regulations, policies and standards.

    e. **Operational Continuity:** Maintaining the ability to sustain essential functions during and after a cybersecurity incident.

    f. **User Privacy:** Safeguarding personal data and respecting the privacy rights of individuals.

    g. **Reputation:** Protecting the state's reputation by preventing breaches and safeguarding the trust of stakeholders.

    h. **Financial Stability:** Preventing financial losses from cyber-attacks, including direct theft, fraud, or costs associated with recovery and mitigation.

    i. **Intellectual Property:** Securing proprietary information and trade secrets from theft or unauthorized disclosure.

    j. **Third-Party Trust:** Safeguarding that interactions with partners, vendors, and customers are secure, maintaining trust and protecting shared data.

    k. **Equity and Accessibility**: Ensuring fair and equitable treatment in all cybersecurity practices, policies, and procedures, promoting inclusivity and access to secure systems for authorized individuals, regardless of their

background or circumstances. See USER-01 Accessibility Policy and USER-01-01-S Minimum Accessibility Standard.

9. **Organizational users who violate security policies and standards in the security chapter of the Washington State IT policies may be subject to appropriate disciplinary action up to and including discharge, termination of contractual agreements, denial of access to state information assets, and other actions as well as civil and criminal penalties.**

10. **Agencies must provide IT security orientation and supervision of organizational users with access to agency IT assets. Agencies will conduct reference checks and background investigations as required by the agency's IT security program.**

11. **Agencies must include appropriate language in vendor and partner contracts and agreements to ensure alignment with WaTech and agency security policies, standards, and requirements.**

REFERENCES

1. WaTech IT Policies Security Chapter.
2. POL-01-02-S Technology Policy & Standard Waiver Request Standard
3. POL-01 Technology Policies, Standards, and Procedures Policy.
4. Definition of Terms Used in WaTech Policies and Reports.
5. SEC-08-01-S Data Classification Standard.
6. SEC-08 Data Sharing Policy.
7. NIST Cybersecurity Framework Mapping:

- Identify.Asset Management-6 (ID.AM-6): Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.
- Identify.Business Environment-5 (ID.BE-5): Resilience requirements to support delivery of critical services are established for all operating states (e.g., under duress/attack, during recovery, normal operations).
- Identify.Governance-4 (ID.GV-4): Governance and risk management processes address cybersecurity risks.
- Protect. Information Protection Processes and Procedures-7 (PR.IP-7): Protection processes are continuously improved.
- Protect. Information Protection Processes and Procedures-8 (PR.IP-8): Effectiveness of protection technologies is shared with appropriate parties.

CONTACT INFORMATION

- For questions about this policy, please email the WaTech Policy Mailbox.
- For technical assistance, please email Risk Management.

WaTech
Washington Technology Solutions

Traffic Light Protocol Standard 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.

The policy workgroup reviewed Cybersecurity and Infrastructure Security Agency's (CISA) updated Traffic Light Protocol (TLP) and aligned this WaTech standard accordingly to ensure consistency with nationally recognized cybersecurity best practices. This updated standard replaces the previous IT Security Incident Communications – US-CERT Traffic Light Protocol 143.10. This standard coordinates with various state regulations and policies, such as RCW 43.105.054 (WaTech Governance), RCW 43.105.205 (3) (Higher Ed), and RCW 43.105.020 (22) ("State agency"). This ensures that the TLP standard aligns with governance requirements for information sharing and cybersecurity in Washington State. We also discussed the standard in the workgroup and added details to tailor it to the state enterprise.

What is the business case for the policy/standard?

The TLP is a set of designations used to ensure that sensitive communications related to cybersecurity events, alerts, and incidents are shared with the correct audience. Having a common understanding of these designations ensures that all parties communicate information with the same level of sensitivity and need to know. One notable update is the addition of TLP: Amber+Strict, which allows for a more granular differentiation of information-sharing categories. This change aims to improve the precision of information-sharing practices and address modern risks related to privacy, reputation, and organizational security.

What are the key objectives of the policy/standard?

- Agencies will understand the TLP color designations to ensure proper information sharing.
- Agencies will use the TLP designations for communications during information security events, alerts and incidents.
- Provide consistent sensitivity designations.
- Align with best practices and compliance requirements.
- Tailor information sharing to state enterprise needs.
- Prevent unauthorized information disclosure.
- Enhance clarity in cybersecurity communications.

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

It aligns with the Enterprise IT Strategic Plan through the 'Digital Trust' pillar by reinforcing secure and controlled communication protocols for information security events, alerts, and incidents. By ensuring that sensitive information is shared only with individuals on a 'need to know' basis, the TLP Standard helps maintain the confidentiality, integrity, and availability of information related to communication of cybersecurity events, alerts and incidents. This approach not only protects the privacy and security of data but also strengthens the trust agencies have in the state's cybersecurity practices, ultimately preserving the reputation of both the state and its agencies.

What are the implementation considerations?

Cybersecurity teams within agencies will need to ensure a comprehensive understanding of the TLP protocols and verify that all documentation concerning cybersecurity events, alerts and incidents is appropriately marked with the correct TLP designation. This includes training staff on applying and recognizing these designations consistently. Additionally, agencies must ensure that access to information is restricted based on the TLP designation (Red, Amber+Strict, Amber, Green, Clear), requiring a thorough evaluation of current information-sharing practices. This process may lead to revisions in who has access to sensitive data, potentially impacting workflows and requiring more stringent approval processes. These changes aim to enhance data security and ensure that information is only accessible to those with a legitimate need, thus maintaining compliance with the updated standards.

How will we know if the policy is successful?

Specific: Establishing procedures for identifying, sampling, and reviewing communications across various platforms (e.g., email, document sharing systems) to verify adherence to TLP protocols.
Measurable: Track compliance across different roles, locations, and demographics to ensure equal representation.
Achievable: As a nationally recognized standard by CISA, the TLP has been validated through established practices, with numerous reference examples to demonstrate its effectiveness.
Relevant: This goal aligns with the state's cybersecurity strategies and the Enterprise IT Strategic Plan. It directly contributes to the protection of sensitive information and ensures better coordination during cybersecurity incidents.

Timebound: Agencies are expected to implement this standard and ensure its continued use. Monitoring efforts will be used to identify the training needs for ongoing improvement and to maintain compliance.
Equitable: The policy will be implemented equitably across all agencies, regardless of size or cybersecurity maturity. Support will be provided to ensure smaller or less resourced agencies can meet the same compliance standards as larger agencies. Additionally, training will be inclusive, ensuring all relevant personnel across agencies have access to the necessary resources and guidance to follow the standard.

SEC-10-01-S
State CIO Adopted: Month 1 202_
TSB Approved: Month 1 202_
Sunset Review: Month 1 202_

WaTech
Washington Technology Solutions

Replaces:
Incident Communications Policy
Appendix 143a
December 10, 2014

TRAFFIC LIGHT PROTOCOL STANDARD

See Also:
RCW 43.105.054 WaTech Governance
RCW 43.105.052 Powers and duties of agency—Application to higher education, legislature, and judiciary.
RCW 43.105.020 (22) "State agency"

1. **The Traffic Light Protocol (TLP) is a set of designations used to ensure that sensitive information for cybersecurity alerts, events, and incidents is shared with the correct audience. TLP is for communications and not data classification. SEC-10 Incident Response Policy requires communications based on the Enterprise Incident Response Plan.**

2. **TLP employs colors to indicate different degrees of sensitivity and the corresponding sharing considerations to be applied by the recipient(s). TLP designations at Washington state agencies are derived from the Cybersecurity and Infrastructure Security Agency's Traffic Light Protocol (TLP) Definitions and Usage.**

    a. TLP:Red

        i. When should it be used? Situations when information cannot be effectively acted upon without significant risk to the privacy, reputation, or operations of the organizations involved. For the eyes and ears of individual recipients only.

        ii. How should it be shared? Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.

    b. TLP:Amber+Strict

        i. When should it be used? When information requires support to be effectively acted upon, yet carries a risk to privacy, reputation, or operations if shared outside of the organization.

ii. How should it be shared? Recipients may share TLP:AMBER+STRICT information only with members of their own organization on a need-to-know basis to protect their organization and prevent further harm.

c. TLP:Amber

i. When should it be used? When information requires support to be effectively acted upon, yet carries a risk to privacy, reputation, or operations if shared outside of the organization(s) involved.

NOTE: TLP:AMBER+STRICT limits the information to a single organization, whereas TLP:AMBER allows a broader distribution of the information to more than one specific organization.

ii. How should it be shared? Recipients may share TLP:AMBER information with members of their own organization, other organizations, clients or other partners on a need-to-know basis to protect their organization(s) and prevent further harm.

d. TLP:Green

i. When should it be used? Circumstances in which information is useful to increase awareness within their wider community.

ii. How should it be shared? Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. Unless otherwise specified, TLP:GREEN information may not be shared outside the cybersecurity or cyber defense community.

e. TLP:Clear

i. When should it be used? When information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.

ii. How should it be shared? Recipients may share this information without restriction. Information is subject to standard copyright laws and rules.

3. **If a recipient needs to share the information more widely than indicated by the original TLP designation, they must first obtain explicit permission from an authorized representative of the original source.**

4. **All communications must include the TLP color in capital letters in the following format: (i.e., TLP:RED, TLP:AMBER + STRICT, TLP:AMBER, TLP:GREEN, or TLP:CLEAR).**

    a. TLP-designated email correspondence must indicate the TLP color of the information in the subject line and the body of the email prior to the designated information.

    b. TLP-designated documents must indicate the TLP color of the information in the header and footer of each page. To avoid confusion with existing control marking schemes, it is advisable to right-justify TLP designations. The TLP color must be 12-point type or greater.

REFERENCES

1. Definition of Terms Used in WaTech Policies and Reports.
2. SEC-10 Incident Response Policy.
3. Traffic Light Protocol (TLP) Definitions and Usage.
4. NIST Cybersecurity Framework CSF 2.0 Mapping:
    - GOVERN.RISK MANAGEMENT STRATEGY (GV.RM-05): Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties
    - IDENTIFY.IMPROVEMENT (ID.IM-04): Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved.
    - RESPOND.INCIDENT RESPONSE REPORTING AND COMMUNICATION (RS.CO-03): Information is shared with designated internal and external stakeholders
    - RECOVER.INCIDENT RECOVERY COMMUNICATION (RC.CO-04): Public updates on incident recovery are shared using approved methods and messaging.

CONTACT INFORMATION

- For questions about this policy, please email the WaTech Policy Mailbox.

PROPOSED DEFINITION

Organization: Under the Traffic Light Protocol (TLP), an organization refers to a group of individuals who share a formal affiliation and are governed by the same organizational policies. This group can be as large as all members of an information-sharing entity, though it is rarely broader than that. An organization may consist of a single agency or a combination

of affected agencies, such as WaTech. Additional agencies may also be included depending on the specifics of the cybersecurity alert, event, or incident.