Policy & Standard Background

Name: Acceptable Use Policy

Replaces IT Security Standard 141.10 (2.10)

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.

Most of the original standard is the same. Changes were made based on workgroup and community feedback to improve clarity for agency adoption and accountability.

Updates to this standard draws from NIST 800-53 Security and Privacy Controls for Information Systems and Organizations.

What is the business case for the policy/standard?

- Mitigate cybersecurity risks
- Reduce state exposure to illegal activities
- Maintain productivity of employees while on the network or accessing the internet

What are the key objectives of the policy/standard?

- Outline acceptable use of state IT assets.
- Protect state IT assets and workforce from risks that may result from the inappropriate or illegal use of the state IT assets.

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

Strategic Planning | Washington Technology Solutions

This standard supports efficient and accountable government by ensuring agencies are managing IT resources comprehensively.

What are the implementation considerations?

- Agencies will need to verify existing training aligns with the policy.
- Agencies can provide additional training internally or share materials state-wide.

How will we know if the policy is successful?

- Acceptable Use violations can be monitored, and statistics reported.
- Employees report that they understand the training materials.

USER-01
State CIO Adopted:
TSB Approved:
Sunset Review:

WaTech
Washington Technology Solutions

Replaces:
IT Security Standard 141.10 (2.10)
December 11, 2017

ACCEPTABLE USE POLICY

See Also:

RCW 43.105.450 Office of Cybersecurity
RCW 43.105.054 OCIO Governing
RCW 43.105.205 (3) Higher Ed

RCW 43.105.020 (22) "State agency"
RCW 39.26.340 Data Sharing- Contractors
RCW 39.24.240 Data Sharing – Agencies

Fraud Program - Office of State Auditor

1. **Individual accountability is required when accessing all Information Technology (IT) assets and organization information.**

2. **Agency information and information technology (IT) assets are the property of the State of Washington and must be used in conformance with this policy, and applicable laws**.

   a. Agency IT assets are to be used to conduct state of Washington business. Refer to sections 2(b)-Agency approved use and 3-Permitted personal use of state resources of WAC 292-110-010 - Use of state resources for additional information.

   b. The following requirements apply to removable storage media:

      i. Users may not copy agency data onto personal storage media.

      ii. Unauthorized devices may not be plugged into agency assets.

   c. Minimal personal use is permitted, provided such use is:

      i. Consistent with WAC 292-110-010 - Use of state resources

      ii. Does not impede the ability of the individual or other users to fulfill the agency's responsibilities and duties, including but not limited to utilization of extensive bandwidth, resource, or storage.

      iii. Does not compromise the security or integrity of agency IT assets.

      iv. Agencies may revoke or limit the personal use of state resources privilege at any time.

   d. Users are prohibited from unauthorized changes of IT asset configuration.

   e. Users cannot connect personal devices to the agency network without express permission from agency management.

3. **Use of state IT assets constitutes express consent for monitoring and/or inspection of**

   a. Any data users create, access, send, or receive.

   b. Any messages users send or receive.

   c. Any web sites that users access.

4. **Access to systems does not guarantee personal privacy for any activity when using such systems. This includes legitimate state purposes, minimal personal use, violations of**

acceptable use or any other use.

a. Anyone authorized to access systems expecting privacy for their minimal personal use should not use agency IT assets. See section 4 of WAC 292-110-010 - Use of State Resources.

b. See the Mobile Device Security Standard for additional information regarding use of personal devices for official state business.

5. **Anyone using agency-issued endpoints is expected to exercise a reasonable level of protection over those devices.**

a. Endpoints must be used and stored in a manner to prevent unauthorized physical access.

b. Users must physically secure unattended agency-issued endpoints from unauthorized access and must not leave the item unattended in publicly accessible areas.

6. **Agency policies and contracts may restrict access to any websites, domains, or content.**

a. Anyone using agency IT assets to access the intranet, or the internet, must comply with all security policies to protect the confidentiality, integrity, and availability of agency information assets.

b. The use of unauthorized software for content sharing is prohibited. Unauthorized connection of wireless access points, including cellular devices, to agency networks is prohibited.

7. **Agencies reserve the right to monitor agency-issued endpoints and computing devices.**

a. Agency-issued computing devices are assigned to users to assist them in the performance of their duties. Agencies have the responsibility and right to monitor all aspects of agency IT assets.

b. Agencies must seize and work with WaTech to inspect any information asset and/or data stored on agency-issued endpoints during the investigation of a security incident or fraudulent activity. Refer additionally to the IT Security Incident Communication Policy.

REFERENCES

1. Security Awareness and Training Policy (under development - see 141.10 (1.4)
2. Data Classification Standard
3. Access Control Policy (under development - see 141.10 (6.1)
4. Data Sharing Policy
5. Mobile Device Security Standard (under development - see 141.10 (5.8)
6. Encryption Standard
7. WAC 292-110-010 – Use of State Resources
8. Definition of Terms Used in WaTech Policies and Reports
9. IT Security Incident Communication

CONTACT INFORMATION

- For questions about this policy, please email the WaTech Policy Mailbox.
- For technical security questions or to request a Design Review, please email the Security Design Review Mailbox.

Policy & Standard Background

Name: Change Management Policy

Replaces IT Security Standard 141.10 (8.1)

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.

Most of the original standard is the same. Changes were made based on workgroup and community feedback to improve clarity for agency adoption and accountability.
Updates to this standard draws from NIST 800-53 Security and Privacy Controls for Information Systems and Organizations.

What is the business case for the policy/standard?

- This policy helps agencies ensure the smooth and timely application of patches and upgrades to systems; these both protect and enhance the confidentiality, availability, and integrity of IT ecosystems.
- This policy ensures that the roles assigned are at the appropriate level of authority, responsibility, and separation.

What are the key objectives of the policy/standard?

The objective of this policy is to refine the introduction of change into production by ensuring that the correct procedures are being followed, proper documentation has been completed, proper testing has been performed, and proper approval is in place.

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

Strategic Planning | Washington Technology Solutions
This standard supports efficient and accountable government by ensuring agencies are managing the alteration of IT resources comprehensively.

What are the implementation considerations?

- Agencies will need to update their documentation.
- Agencies may need additional training and support.

How will we know if the policy is successful?

- Agencies will have well-documented acceptance criteria that accurately reflect changes made to their IT assets.
- Employees will experience the minimum impact resulting from timely patches, upgrades, and quick rollback when changes encounter difficulties.

State CIO Adopted:
TSB Approved:
Sunset Review:

Replaces:
IT Security Standard 141.10 section 8.1

WaTech
Washington Technology Solutions

CHANGE MANAGEMENT POLICY

See Also:
RCW 43.105.054 OCIO Governing
RCW 43.105.205 (3) Higher Ed
RCW 43.105.020 (22) "State agency"

1. **Agencies must document change management roles and responsibilities to reduce opportunities for unauthorized changes.**

Role	Responsibilities
Requestor	The requestor submits the change request.
Implementer	The implementer deploys the change into production. The implementer is the person or team that records the implementation results.
Approver	The approver is responsible for deciding whether a change is fit to proceed to implementation by examining the evidence in the change request.
Change Advisory Board (CAB)	The group who assesses, prioritizes, and authorizes changes as part of the agency's change control process.

2. **Agencies must identify and document how they will ensure implementation of approved changes only.**

3. **Agencies must designate a change approver separate and distinct from the individuals authorized to request and implement changes.**

4. **Agencies must document acceptance criteria for all changes to minimally include:**

    a. A description of the change.

    b. The impact of the change.

    c. The justification for the change.

    d. The implementation and communication plan.

    e. A risk and impact analysis of the change. See the Risk Assessment Standard.

    f. A plan to test the change.

    g. A back out plan to roll back changes if something goes wrong.

h. The planned start date and planned end date of the change.

5. **Agencies must classify requested changes consistent with the change types in the table below:**

Change Type	Description
Normal	• A normal change must be evaluated, authorized, and scheduled according to a standardized change management process.
Standard	• Low risk, low impact, highly repeatable change with very little possibility of adversely impacting the production environment.
Emergency	• Not able to meet the minimum lead-time requirements for normal change request. Service Owner/Configuration Item (CI) Manager will approve instead of Change Advisory Board (CAB) due to time constraints. Separation of D~~d~~uties (SOD) may be deferred. Approvals that do not violate SOD should be provided as a follow-up to any emergency change. • Urgent changes must satisfy two criteria for auto-approval: 1. The change is related to a high or critical priority incident. 2. The incident is in a non-closed status.

6. **Agencies must independently meet change management requirements from third-party regulatory authorities, such as CJIS or HIPAA.**

REFERENCES

1. Definitions of Terms Used in WaTech Policies and Reports
2. Asset Management Policy (under development - see 141.10 (8.2)
3. Configuration Management Policy (under development - see 141.10 (5.1.1. Network Devices)
4. Risk Management Policy
5. Risk Assessment Standard
6. NIST Cybersecurity Framework Mapping:
    - Identify.Governance (ID.GV-2): Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners
    - Protect.Information Protection Processes and Procedures (PR.IP-3): Configuration change control processes are in place.

CONTACT INFORMATION

- For questions about this policy, please contact the WaTech Policy Mailbox.
- For technical security questions and risk management document submissions, contact the WaTech's Risk Management Mailbox.

Policy & Standard Background

Name: Configuration Management Policy

Replaces IT Security Standard 141.10 (5.1.1)

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 standard draws from NIST 800-128, Guide for Security-Focused Configuration Management and NIST 800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy

What is the business case for the policy/standard?

A baseline configuration of IT systems enables agencies to make sound business, technical, and legal decisions.

Ensuring all information systems start and continue to use industry proven tactics by only supporting essential capabilities reduces the attack surface and downstream maintenance expenses.

Proper documentation of configuration baselines and changes.

What are the key objectives of the policy/standard?

- Ensuring agencies have a clear picture of the agency's infrastructure and software profile; a baseline configuration.
- Ensuring that all configuration changes to agency information assets and resources are done with management's knowledge and consent, appropriately tested, and do not introduce security weaknesses to the state's Information system.

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

Strategic Planning | Washington Technology Solutions

This standard supports efficient and accountable government by ensuring agencies are managing IT resources comprehensively.

What are the implementation considerations?

- Agencies will need resources to review and verify baseline configurations.
- Agencies may need additional training and support.

How will we know if the policy is successful?

- Agencies will not experience security events due to easily controlled vulnerabilities.
- Agencies update their configurations when changes happen.

State CIO Adopted:
TSB Approved:
Sunset Review:

WaTech
Washington Technology Solutions

Replaces:
IT Security Standard 141.10 (5.1.1, 5.6.2)
December 11, 2017

CONFIGURATION MANAGEMENT STANDARD

See Also:

RCW 43.105.450 Office of Cybersecurity
RCW 43.105.054 OCIO Governance
RCW 43.105.020 (22) State Agency
RCW 43.105.205 (3) Higher Ed.

1. **Agencies must create a configuration baseline for all systems that would impact the agency's security posture as part of the agency's security program:**

   a. Develop, document, and maintain under configuration control, a current baseline configuration of information systems referencing the Center for Internet Security (CIS) benchmarks, and/or vendor-provided secure baseline configuration requirements. See the Asset Management Policy..

      i. If CIS benchmarks and/or vendor-provided secure baseline configuration requirements are not available, the agency must develop, document, and maintain a secure configuration for the solution and may consult with WaTech.

      ~~i.~~ii. WaTech will offer additional guidance and services for securing endpoints using CIS benchmarks. Agencies must utilize the Endpoint Detection Response (EDR) solution where applicable.

   b. Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system baseline configurations. Identify, document, and approve any deviations from established configuration. See Access Control.

   c. Retain one previous version of baseline configurations of information systems to support rollback.

   d. Monitor and control changes to the configuration settings in accordance with the Change Management Policy.

   e. Review and update the baseline configurations annually or after changes to that baseline.

2. **Agencies must exercise configuration change control for all systems that would impact the agency's security posture:**

   a. Determine the types of changes to the information system that affect its configuration and their potential impacts. Configuration change control documentation must be handled, at minimum, as category 3 information.

   b. Test, validate, and document the proposed information system configuration change prior to implementation. This must include identification of potential security impacts.

   c. Document configuration change decisions associated with the information system.

   d. Implement approved configuration changes to the information system.

   e. Retain records of configuration changes for the period of one year after the date of the change according to the required retention period. See GS 14020 Rev. 1 State

Government General Records Retention Schedule v.6.1.

f. Perform an annual internal review of configuration changes to ensure compliance with internal change management processes.

3. **Agencies must configure all information systems that would impact the agency's security posture to provide only business-related capabilities and prohibit the use of functions, ports, protocols, and/or services that are not required for business functions.**

REFERENCES

1. NIST 800-128, Guide for Security-Focused Configuration Management
2. NIST 800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
3. Risk Assessment Standard
4. Asset Management Policy - under development – see Securing Information Technology Assets Standards (Parts Rescinded) 141.10 (8.2)
5. Change Management - under development – see Securing Information Technology Assets Standards (Parts Rescinded) 141.10 (8.1)
6. Access Control Policy (under development – see Securing Information Technology Assets Standards (Parts Rescinded) 141.10 (2).
7. CIS Benchmarks
8. Definitions of Terms Used in WaTech Policies and Reports
9. GS 14020 Rev. 1 State Government General Records Retention Schedule v.6.1
10. NIST Cybersecurity Framework Mapping:
    - Detect.Anomalies and Events (DE.AE-1): A baseline of network operations and expected data flows for users and systems is established and managed.
    - Protect.Information Protection Processes and Procedures (PR.IP-1): A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality).
    - Protect.Information Protection Processes and Procedures (PR.IP-2): A System Development Life Cycle to manage systems is implemented.
    - Protect.Protective Technology (PR.PT-3): The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.

CONTACT INFORMATION

- For questions about this policy, please email the WaTech Policy Mailbox
- For a Security Design Review or for technical security questions, please email the Security Design Review Mailbox.
- For questions about risk assessments and management, please email the Risk Management Mailbox**.**

Policy & Standard Background

Name: International Travel Technology Policy & Standard

New

What due diligence was conducted to determine the content of this policy and 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 and standard content.

The Department of Ecology proposed the creation of a workgroup within the Enterprise Security Governance committee to address the following areas of concern:

- The state's official policy on travel (OFM 10.10.50) is geared toward finance and does not address technology concerns.
- Understanding and practices of agencies engaging in international travel varies widely.
- Technical security concerns vary by international locations.
- A growing number of statewide technical controls, implemented and planned are increasingly impacting the ability for unmanaged connections from outside the U.S**.**

What is the business case for the policy and standard?

Currently there are varied approaches to digital access for employees traveling internationally on behalf of the state. A unified strategy for ensuring security of state resources by assessing risk prior to international travel ensures technical controls are planned and implemented to protect state data and systems.

What are the key objectives of the policy and standard?

Create a unified state position on the use of technology during foreign travel that will:

- Supplement the current financial international travel policy with statewide technology policies and standards.
- Promote a single statewide strategy for IT security during international travel.
- Align the state's policy, processes, expectations, and technical solutions for addressing risks related to the use of technology during travel outside of the U.S.
- Formalize the policy and standard for assessing, preparing, and approving the use of state-managed technology and resources during travel outside of the U.S.

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

StrategicPlanBrief.pdf (wa.gov) The policy and standard promote the security of state data and protects the public's interests by ensuring a review of technical access for internationally prior to travel (Goal 2). It also Champions governance and accountability (Goal 3) by requiring approvals for technological risks.

What are the implementation considerations?

Agencies may need additional training and guidance to implement this policy. Agencies may need to develop internal policies and processes to implement the policy.

How will we know if the policy and standard are successful?

- Agencies will develop processes to implement controls to safeguard resources while employees travel internationally.
- Employees will be able to access resources while traveling internationally on behalf of Washington State.

State CIO Adopted:
TSB Approved:
Sunset Review:

Replaces: N/A

WaTech
Washington Technology Solutions

INTERNATIONAL TRAVEL TECHNOLOGY POLICY

See Also:

RCW 43.105.450 Office of Cybersecurity
RCW 43.105.054 OCIO Governance
RCW 43.105.020 (22) "State Agency"
RCW 43.105.205 (3) Higher Ed

U.S. DOJ FBI Safety and Security for the Business Professional Traveling Abroad
U.S. DOJ FBI OPS Business Travel Tips Guide
WA State Office of Cybersecurity Best Practice While Traveling
OFM Travel Policy 10.10.50

1. **Agencies must approve technical access for international travel on official state business.**
   a. Agencies must assess, authorize and configure technology to minimize risk to state resources prior to departure.

2. **Agencies must formally approve the business need to technical access to state resources for international travel not on official business, such as informal, leisure, or vacation.**
   a. When not traveling for business but when a business justification for SGN access exists, agencies must perform a risk assessment and document the decision.

3. **WaTech or the agency may restrict or disallow access to state resources during officially sanctioned international travel.**
   a. WaTech is authorized to impose technical controls to restrict access from international locations to state resources. See the International Travel Technology Standard.
   b. Agency IT security teams are authorized to impose technical requirements to protect user accounts and state resources.

4. **Agency IT security teams must evaluate devices on return and certify as safe before reconnecting to the state network.**

REFERENCES

1. Definition of Terms Used in WaTech Policies and Reports

CONTACT INFORMATION

For questions about this policy, please contact the WaTech Policy Mailbox

State CIO Adopted:
TSB Approved:
Sunset Review:

WaTech
Washington Technology Solutions

Replaces:
N/A

INTERNATIONAL TRAVEL TECHNOLOGY STANDARD

See Also:
RCW 43.105.450 Office of Cybersecurity
RCW 43.105.054 OCIO Governance
RCW 43.105.020 (22) "State Agency"
RCW 43.105.205 (3) Higher Ed
OFM Travel Policy 10.10.50.a

FBI: Safety and Security for the Business Professional Traveling Abroad
FBI: OPS Business Travel Tips Guide
WaTech's Best Practice While Traveling

1. **Any computing device needing international access to state resources must meet the requirements in the International Travel Technology Policy and additional security requirements.**

   a. Devices must meet requirements specified by the agency IT security team.

   b. Devices must adhere to the Encryption Standard.

   c. Mobile devices must be managed with a Mobile Device Management (MDM) solution approved by WaTech as required by the Mobile Device Usage Policy.

   d. Computing devices not managed by an MDM must meet agency IT security team requirements. Devices accompanying international travel must be:

      i. Assessed and configured following the risk-based security measures below to minimize risk prior to scheduled departure date.

      ii. Quarantined on return and validated as safe before being allowed to reconnect to the state network.

2. **Access to state data for international travel must be protected.**

   a. Category 3 or Category 4 data must be protected as described in the State Data Classification Standard.

   b. Category 3 or Category 4 data must be approved by the agency IT security team for use on mobile devices or laptops.

3. **Access to state resources requires risk-based security measures.**

   a. Agencies must base access decisions on a risk management methodology that follows the Information Security Risk Management Policy.

   b. Authentication must follow requirements from the Securing IT Assets Standard (6.3).

   c. The approach for each international travel scenario must include an assessment (see the Risk Assessment Standard) of risks associated with:

      i. The targeted travel location.
      ii. The nature and purpose of the travel.
      iii. The technical devices and services required/desired for the trip.
      iv. The access level and organizational responsibility of each traveler.

4. **WaTech manages connections from high-risk/unsafe countries or regions for the state.**

   a. WaTech determines whether to block cyber traffic or require additional controls from countries on the unsafe country list at entry points to the SGN, state-managed on-premises environments and the Enterprise Shared Tenant.

b. WaTech will maintain a list of high-risk countries or regions.

REFERENCES

1. Encryption Standard
2. Data Classification Standard
3. Securing IT Assets Standard (6.3)
4. Definitions of Terms Used in WaTech Policies and Reports

CONTACT INFORMATION

For questions about this policy, please contact the WaTech Policy Mailbox

Proposed Definitions for the International Travel Technology Policy

International Travel – Any travel outside the 50 United States. Travel to any of the U.S. territories is considered international travel.

Microsoft 365 Services – Microsoft 365 cloud-based services such as email, Teams, SharePoint Online, and OneDrive. These services are delivered to agencies from the Washington State shared tenant.

Informal, Leisure, or Vacation Travel – Travel scenarios where traveler's activities may include a desire or intention to connect or use to state resources such as email, agency-provided cellular service, Microsoft 365 services, the state network, etc. All international travel not authorized in writing as "officially sanctioned state business" is considered Informal travel.

Officially Sanctioned International Travel – Travel approved in advance and in writing by agency director or designee. Officially sanctioned business is approved in advance and in writing by the Office of the Governor. Officially sanctioned business requiring connectivity to any state or agency resources must be accompanied by specific, advanced technical preparations set forth and defined in this policy.

Policy & Standard Background

Name: Vulnerability Management Standard

New

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 2017 version of OCIO 141.10 addresses the handling of vulnerabilities in different contexts:

- **Application development – sections 7.2(6), 7.3(2), 7.4(1) and (2)**
- **IT Risk Assessment – sections 1.2(5) and (7)**
- **Physical and Environmental Protection – section 3**
- **System Vulnerabilities – section 5.6(1)**

This new standard draws from NIST 800-40 revision 4 - Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology to consolidate and build on the vulnerability management principles from those section. This provides agencies with a single document with vulnerability management requirements applicable across various contexts.

What is the business case for the policy/standard?

- **This standard helps agencies prioritize patching activities by severity threshold.**
- **This standard helps agencies track patching activities using descriptive metrics.**

What are the key objectives of the policy/standard?

The objectives of this standard are:

- **Consolidate vulnerability scanning, remediation, and management requirements in a single standard.**
- **Provide agencies with criteria for the prioritization and tracking of patching activities.**

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

This standard helps agencies reduce the vulnerabilities that attackers may exploit.
This supports a security and privacy for a safe community and effective government.

What are the implementation considerations?

- **Agencies will need a mechanism to track vulnerabilities and vulnerability severity ratings.**
- **Agencies will need to mechanism to provide the metrics required by this standard.**

How will we know if the policy is successful?

- **Agencies will prioritize vulnerability for patching consistently.**
- **Agencies will track the performance of their patching activities using consistent metrics.**

Number:
State CIO Adopted:
TSB Approved:
Sunset Review

WaTech
Washington Technology Solutions

Replaces:
IT Security Standard 141.10 (5.5 & 5.6)
December 11, 2017

VULNERABILITY MANAGEMENT STANDARD

See Also:

RCW 43.105.450 Office of Cybersecurity	RCW 43.105.020 (22) "State Agency"	RCW 43.105.450 (7c) IT Security
RCW 43.105.054 OCIO Governance	RCW 43.105.205 (3) Higher Ed	

1. Vulnerability scanning must include the following activities:

a. All computing and networking IT assets identified by the Asset Management Policy must be included in the vulnerability assessment scope.

b. Configure endpoints and network infrastructure and applications to allow access for vulnerability scans.

c. Schedule and conduct monthly scans of internal-facing computing and networking IT assets.

d. Schedule and conduct weekly scans of internet-facing computing and networking IT assets.

e. Perform vulnerability scans after the introduction of new computing or network devices into the agency IT environment.

f. Verify all findings identified during the vulnerability scan and document supporting evidence. The following types of evidence may suffice for documentation of a False Positive:

  i. Narrative with a screenshot showing that the information provided is incorrect.

  ii. Any other items that would indicate that the information provided is inaccurate.

2. Agencies must prioritize the vulnerabilities they will address.

a. Agencies must prioritize the assets to be remediated by the system’s business criticality.

b. Agencies must triage vulnerabilities listed in the Known Exploited Vulnerabilities (KEV) Catalog | CISA for remediation.

c. Agencies must use the highest vulnerability criticality from the Vulnerability Management Procedure or the Common Vulnerability Scoring System (CVSS) ratings in Table 1 to triage vulnerabilities not listed in the KEV Catalog.

Table 1 – Vulnerability Classification

Vulnerability Classification	Description	CVSS Rating
Critical	Indicates flaws could be easily exploited by an unauthenticated remote attacker and lead to compromise.	9.0 – 10.0

High	Indicates local users can gain privileges, allow unauthenticated, remote users to view resources that should otherwise be protected by authentication, allow authenticated remote users to execute arbitrary code, or allow remote users to cause a denial of service.	7.0 – 8.9
Medium	Indicates flaws are more difficult to exploit but could still lead to compromise under certain circumstances.	4.0 – 6.9
Low	Indicates vulnerabilities require unlikely circumstances to be exploited or where a successful exploit would cause either no adverse effect or result in minimal adverse consequences.	Below 4.0
Informational	Useful information that is more general about the system and how it operates. Mostly configuration choices rather than a real vulnerability.	0

d. Agencies must prioritize based on the risk assessed. See the Risk Assessment Standard.

i. Agencies prioritizing their remediation workload must consider existing network, IT system, and/or application security layers that may reduce the likelihood and/or impact of a vulnerability.

ii. Agencies must track backlogs of pending remediations.

e. Identify a vulnerability mitigation plan for assets for which no patch is available.

3. **After confirming the vulnerability scan results applicable to their systems, agencies are responsible for reducing the likelihood and/or the impact of exploitation of the vulnerabilities.**

a. Agencies must mitigate the vulnerability using vendor security patches, system configuration changes and/or application modifications, and other appropriate mitigation strategies. All changes must be documented per the agency's change management processes.

i. Agencies will reference the Common Vulnerability and Exposure (CVE) database.

ii. Agencies will take the necessary corrective actions. The corrective actions recommended in the vulnerability scanner and reports are to be used as a guideline for mitigation strategy.

iii. Agencies must verify the successful application of vulnerability patches. If the confirmation scan reveals that the mitigation was unsuccessful, further action must be taken to remediate the vulnerability.

b. If a recommended remediation step is not possible, agencies must develop and implement compensating controls.

i. The compensating controls will operate until vendor patches or configuration changes are available.

ii. If the vulnerability cannot be patched, agencies must harden the affected IT asset according to the Configuration Management Standard (under development - see 141.10 5.1.1) to reduce the likelihood of vulnerability exploitation.

4. **Agencies must maintain a documented patch management procedure for all computing and network assets under their control. The procedure must include the following steps at a minimum:**

    a. Identification and prioritization of patches to be installed.

    b. Applying patches in a timeline consistent with business criticality and risk.

    c. Coordination of a patch window with appropriate stakeholders.

    d. Validation of the appropriate application of patches.

    e. Evaluation and testing of patches prior to deployment.

    f. Agencies must install patches that address previously unknown exploits (Zero-Day Exploit) with a critical CVSS and high risk assessed within one calendar day of patch release.

    g. Agencies unable to meet their established deadlines for patching vulnerabilities with high CVSS scores for high-risk systems as assessed by the agency must identify and document compensating controls and notify WaTech by filing a ServiceNow ticket.

5. **Agencies must conduct ongoing external threat intelligence gathering, which at a minimum includes identification and use of threat intelligence feeds.**

6. **Agencies must document their vulnerability management plan based on the requirements in this standard. The vulnerability management plan must include:**

    a. A list of the vulnerabilities to be patched, including the CVSS severity ranking per Table 1

    b. Mean time to remediate.

    c. The computing and network IT assets the agency did not remediate.

REFERENCES

1. Asset Management Policy (under development - see 141.10 8.2)
2. NIST SP 800-40 - Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology
3. Common Vulnerability Scoring System (CVSS)
4. Configuration Management Standard (under development - see 141.10 5.1.1)
5. Definitions of Terms Used in WaTech Policies and Reports
6. Vulnerability Management Procedure (under development – will be confidential due to security)
7. Known Exploited Vulnerabilities Catalog | CISA
8. Common Vulnerability and Exposure (CVE) database
9. NIST Cybersecurity Framework Mapping:
    - Identify.Risk Assessment-1 (ID.RA-1): Asset vulnerabilities are identified and documented.
    - Protect.Information Protection Processes and Procedures-12 (PR.IP-12): A vulnerability management plan is developed and implemented.

- Detect.Security Continuous Monitoring-8 (DE.CM-8): Vulnerability scans are performed.
- Respond.Analysis-5 (RS.AN-5): Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g., internal testing, security bulletins, or security researchers).
- Respond.Mitigation-3 (RS.MI-3): Newly identified vulnerabilities are mitigated or documented as accepted risks.

CONTACT INFORMATION

- For questions about this policy, please contact the WaTech Policy Mailbox.
- To request a Security Design Review, please contact the Security Design Review Mailbox.