WaTech
Washington Technology Solutions

Enterprise Architecture Program Policy Background

New, Update or Sunset Review? 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.

This is a new policy. This policy was developed with a group derived from the Enterprise Architecture Committee. It is informed by RCWs. The policy draws from industry frameworks to create a framework relevant to the state.

What is the business case for the policy/standard?

The State Enterprise Architecture Program is necessary to strategically plan for business processes supported by information technology. The State EA program goals are centered around:

- Business-IT strategy, alignment, and collaboration.
- Standardization for consistency across the enterprise.
- Interoperability and integration.
- Risk management.
- Cost optimization and resource utilization.
- Innovation and agility.
- Enterprise-wide visibility and governance.
- Measurable performance for continuous improvement.

What are the key objectives of the policy/standard?

- Define enterprise architecture responsibilities.
- Create criteria for developing architectural standards.
- Require enterprise architecture data collection and analysis.
- Promote and mature agency enterprise architecture practices.

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

This policy is directly informed by RCWs.
RCW 43.105.265 (1) Enterprise Strategy
RCW 43.105.020 (6) "Enterprise Architecture"
RCW 43.105.450 (3f) Office of cybersecurity

This policy supports the statewide enterprise IT strategic plan Goal 1 "Create a Government Experience that Leaves No Community Behind" by ensuring that digital trust is a consideration from the planning and strategic lens. A digital equity principle is included in the guideline to help ensure equity is built in by design, rather than as an afterthought.

GOAL 2: **"**Better data, better decisions, better government, better Washington" is supported because the EA program includes data as decision assistance tools in the EA-01-02-S Decision Making Principles Standard. The policy calls out the importance of collecting EA data to make better decisions.

The program includes goals for driving innovation and modernization in line with GOAL 3 **"**Innovative technology solutions create a better Washington.**"**

The policy requires agencies to support opportunities for training and collaboration for enterprise architecture practice. This supports GOAL 4: "Transform how we work. Best workforce ever." Additionally, the program is required to establish metrics and strategies to ensure continuous improvement in all areas.

What are the implementation considerations?

Agencies may need additional support and resources to develop their enterprise architecture programs. Agencies will need to plan for changes to their business processes including new or updated governance models. This includes how decisions are made and who makes them, and a new architecture review board or group with supporting processes for evaluating and implementing new technologies.

How will we know if the policy is successful?

Specific: Architectural standards are created to support the enterprise. Agencies will develop enterprise architecture policies and practices for decision making.
Measurable: We can measure the number of architectural standards developed and waivers against the policy. We can also measure the number of agencies that are practicing enterprise architecture.
Achievable: We have a fully developed governance process to create, review and implement standards. We can support agency programs by providing model policies and guidance.
Relevant: Enterprise architecture plays a critical role in helping organizations leverage technology investments effectively, drive innovation, manage risks, and achieve strategic objectives in today's complex and dynamic business environment.

Timebound: This policy will be effective when adopted. This policy will be reviewed in three years at the sunset review to evaluate the effectiveness of the statements.
Equitable: Evidence-driven and data supported decisions help us avoid inequities and uncover bias.

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

Replaces: N/A

WaTech
Washington Technology Solutions

ENTERPRISE ARCHITECTURE PROGRAM POLICY

See Also:
RCW 43.105.054 WaTech Governance
RCW 43.105.205 (2a, 2c) Office of the state chief information officer
RCW 43.105.240 (2) Evaluation of agency information technology spending and budget requests.
RCW 43.105.205 (3) Higher Ed
RCW 43.105.020 (23) "State agency"
RCW 43.105.265 (1) Enterprise Strategy
RCW 43.105.020 (6) "Enterprise Architecture"
RCW 43.105.450 (3f) Office of cybersecurity
RCW 43.105.230 State agency information technology portfolio—Basis for decisions and plans.
RCW 43.88.092 Information technology budget detail.

1. **Enterprise Architecture (EA) is the ongoing process of turning business vision and strategy into effective organizational change. EA creates, communicates, and improves the key principles and models that describe the enterprise's future state and enables its evolution. WaTech will lead Washington State's EA Program and support effective enterprise change through technology and business alignment.**

2. **Washington State's EA Program includes the following functions:**

    a. Governance mechanisms to ensure alignment with organizational goals, accountability, and effective decision-making. The purpose of governance is to provide a structured framework for overseeing the development and implementation of architecture standards, policies, and practices, thereby ensuring consistency, transparency, and strategic coherence across the organization.

    b. Overseeing and developing an enterprise-based architecture strategy for state government informed by portfolio management, business, information technology, security, and data. The purpose of the strategy will be to mature EA practices statewide and model a strategy for agencies to follow.

    c. Provide leadership with recommendations to align IT investments with statewide strategy to support informed decisions.

    d. Maintaining a knowledge repository for agencies to view and utilize, along with a training program for agencies.

    e. Providing input for architecture employee classification in the Information

Technology Professional Structure (ITPS) job family.

f. Enhancing decision making through governance, partnership, and education.

g. Providing enterprise architecture services, which include policies, standards, principles, models, capability maps, and guidance to agencies that align with:

   i. Washington State's strategic goal and values.

   ii. EA-01-01-S Criteria for Developing Enterprise Architecture Principles for Decision Making Standard.

   iii. EA-01-02-S Enterprise Architectural Domains Standard.

   iv. A connected government approach to IT, cybersecurity, privacy, and digital trust.

h. Creating and maintaining an enterprise service roadmap and EA services catalog. See EA-02 Establishing an Enterprise Service Policy.

i. Supporting agency development of EA services such as policies, standards, guidelines, models, capability maps, and frameworks to align to EA program goals.

j. Establishing critical success factors (CSFs), key performance indicators (KPIs), Objectives Key Results (OKRs), and benchmarks for evaluating program effectiveness and maturity. Identifying the qualitative value achieved through EA.

3. Agencies must demonstrate their alignment with statewide EA policies and standards and incorporate EA practices and principles into the agency's business and technology decision making processes.

a. Agencies will develop policies, standards, guidelines, models, capability maps, and frameworks that align with the EA program.

b. Within their agency's EA program or practices, agencies must document procedures for making technology purchases and architectural decisions that align with EA-01-01-S Criteria for Developing Enterprise Architecture Principles for Decision Making Standard.

c. Agencies will ensure IT Investments align to statewide strategy.

d. Within their agency's EA program or practices, agencies must document

alignment with EA-01-02-S EA Domain Standard.

e. Agencies will attest to the agency's enterprise architecture alignment annually, as part of the technology policy certification requirement. See POL-01 Technology Policies and Standards Policy.

REFERENCES

1. RCW 43.105.265.
2. Washington State's strategic goals.
3. EA-01-01-S Enterprise Architecture Principles for Decision Making Standard.
4. EA-01-02-S Enterprise Architectural Domains Standard.
5. EA-02 Establishing an Enterprise Service.
6. POL-01 Technology Policies and Standards Policy.
7. Definition of Terms Used in WaTech Policies and Reports.

CONTACT INFORMATION

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

PROPOSED DEFINITIONS

- Enterprise Architecture: is an ongoing activity for translating business vision and strategy into effective enterprise change. It is a continuous activity. Enterprise architecture creates, communicates, and improves the key principles and models that describe the enterprise's future state and enable its evolution.

- Capability: (from Information Technology Infrastructure Library (ITIL)) The ability of an organization, person, process, application, configuration item, or IT service to carry out an activity.

- Digital Trust: The confidence in the integrity of relations, interactions and transactions among providers and consumers within an associated digital ecosystem.

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

Replaces:
N/A

WaTech
Washington Technology Solutions

CRITERIA FOR DEVELOPING PRINCIPLES FOR DECISION MAKING

See Also:
RCW 43.105.054 WaTech Governance
RCW 43.105.205 (3) Higher Ed
RCW 43.105.020 (22) "State agency"
RCW 43.105.020 (6) "Enterprise Architecture"
RCW 43.105.450 (3f) Office of cybersecurity
RCW 43.105.230 State agency information technology portfolio—Basis for decisions and plans.
EA-01 Enterprise Architecture Program Policy
TOGAF® The New Release | www.opengroup.org

1. **Agencies must develop and adopt Enterprise Architecture principles for making business and technology decisions according to this standard.**

2. **Definitions**

    a. Principles are general rules and guidelines, intended to be enduring and seldom amended, that inform and support the way in which an organization sets about fulfilling its mission.

    b. Enterprise Principles provide a basis for decision-making throughout an enterprise and inform how the organization sets about fulfilling its mission.

    c. Architecture Principles are a set of principles that relate to architecture work. They reflect a level of consensus across the enterprise and embody the spirit and thinking of existing enterprise principles. Architecture Principles govern the architecture process, affecting the development, maintenance, and use of Enterprise Architecture.

3. **Agencies must involve technology and business partners of the organization in the development of the principles to ensure their relevance, acceptance and adoption.**

4. **To develop a principle-based approach for decision making, agencies must use the following criteria:**

    a. Alignment with Business Goals.

        i. Purposeful: Each principle should support the organization's mission, vision, and strategic goals, ensuring that all architectural decisions

directly contribute to business objectives. This is often described in a rationale and implications statement.

ii. Compliance: Principles should align with applicable policies, standards, laws, and regulations.

b. Clear, concise, and focused.

i. Understandable: Principles should be clearly articulated and easy to understand by all interested parties, not just IT personnel. This fosters broader acceptance and adherence.

ii. Actionable: Principles should be specific enough to guide decision-making without ambiguity.

c. Comprehensive Coverage.

i. Inclusive: Principles should address key aspects of the enterprise architecture domains and pillars as described in the EA-01-02-S EA Domain Standard.

ii. Consistent: Principles should be designed to complement and support one another, avoiding contradictions or overlaps that could create confusion or inefficiencies.

iii. Balanced: Principles should ensure a balance between competing needs such as innovation vs. stability or centralized vs. decentralized control.

d. Stability and Adaptability.

i. Sustainability: Principles should be designed to accommodate future changes in technology, business, and physical environments.

ii. Scalable: Principles must work effectively at different scales of operation and anticipate growth.

5. **Agencies must document principles clearly and distribute them widely within the organization.**

6. **Agencies must provide training and resources to help employees understand and apply agency principles in their work.**

7. **Agencies must review principles in cadence with the enterprise strategy and updated as necessary to remain relevant to the agency's business.**

REFERENCES

1. Definition of Terms Used in WaTech Policies and Reports.
2. EA-01-02-S EA Domain Standard.

CONTACT INFORMATION

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

PROPOSED DEFINITION:

- Enterprise Architecture Principles:

  Enterprise Architecture (EA) Principles provide a basis for decision-making throughout an enterprise and inform how the organization sets about fulfilling its mission. EA Principles govern the architecture process, affecting the development, maintenance, and use of architecture.

- Architecture Principles:

  A set of principles that relate to architecture work. They reflect a level of consensus across the enterprise and embody the spirit and thinking of existing enterprise principles. Architecture Principles govern the architecture process, affecting the development, maintenance, and use of Enterprise Architecture.

- Enterprise Architecture:

  An ongoing activity for translating business vision and strategy into effective enterprise change. It is a continuous activity. Enterprise architecture creates, communicates, and improves the key principles and models that describe the enterprise's future state and enable its evolution. Enterprise Architecture (EA) is the ongoing process of turning business vision and strategy into effective organizational change.

EA-01-02-S
State CIO Adopted: Month 1 2023
TSB Approved: Month 1 2023
Sunset Review: Month 1 2023

Replaces:
N/A

ENTERPRISE ARCHITECTURAL DOMAINS STANDARD

See Also:
RCW 43.105.054 WaTech Governance
RCW 43.105.205 (3) Higher Ed
RCW 43.105.020 (22) "State agency"
RCW 43.105.020 (6) "Enterprise Architecture"
EA-01 Enterprise Architecture Program Policy
The TOGAF Standard, Version 9.2 - Core Concepts

1. **The Enterprise Architecture (EA) Program establishes the core domains of architecture for executing holistic business and technology strategies. Washington State Enterprise Architectural Domains are:**

    a. Business Architecture: Defines and aligns the business capabilities, maps, processes, and services with organizational strategy.

    b. Data Architecture: Defines the architecture that informs how enterprises collect, store and use information to make informed business decisions.

    c. Application Architecture: Designs architectural frameworks and connections between software solutions that enable agencies to deliver services that meet their mission and goals.

    d. Technology Architecture: Focuses on the design, deployment, and management of the Information Technology (IT) infrastructure.

2. **Security is an enterprise architecture pillar that crosses all domains. Security considerations are pervasive in all phases of architecture development.**

REFERENCES

1. Definition of Terms Used in WaTech Policies and Reports.

PROPOSED DEFINITIONS

Pillar:

A pillar refers to a foundational aspect or core component that supports and influences multiple domains across the enterprise architecture. Pillars represent key focus areas that are critical to the overall success and integrity of architecture, ensuring that essential considerations are consistently addressed across all domains.

Enterprise Architecture Domain:

An architecture domain refers to a specific area or category within the overall enterprise architecture framework. It represents a broad focus area that encompasses various components, activities, and considerations related to that particular domain.

Email Address Naming 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 Enterprise Architecture Committee committed a subcommittee for the policy development. The document was reviewed by the subcommittee, through the WaTech internal review, community review, and governance.

What is the business case for the policy/standard?

Primary email addresses will display when an email is received. Requiring a standard convention with a recognizable pattern ensures that anyone receiving an email from a state agency will have a high degree of confidence in the sender based on the email address displayed.

What are the key objectives of the policy/standard?

- Agencies will utilize the firstname.lastname@agency.wa.gov or firstname.mi.lastname@agency.wa.gov naming convention for primary email addresses.
- Email addresses standardization will ensure a consistent structure across state government.

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

This standard supports Learn Together, Build Together, Serve Together, by standardizing how government email appears to end users.

What are the implementation considerations?

Some agencies are not currently in compliance with the standard and will need waivers. These agencies may have technical connections that will make transitioning difficult.

Agencies may need to develop processes to determine how to apply alternate naming conventions where duplicates exist, such as whether to use a middle initial versus a number, and how to determine an email address should be obfuscated for the individual's protection.
How will we know if the policy is successful?
Specific: Response. **Measurable:** Response. **Achievable:** Response. **Relevant:** Response. **Timebound:** Response. **Equitable:** Response.

EA-01-04-S
State CIO Adopted: Month 1 2023
TSB Approved: Month 1 2023
Sunset Review: Month 1 2023

Replaces:
IT Enterprise Architecture Standard
171.10- Email Address Naming
December 14, 2021

WaTech
Washington Technology Solutions

EMAIL ADDRESS NAMING STANDARD

See Also:
RCW 43.105.054 WaTech Governance
RCW 43.105.205 (3) Higher Ed
RCW 43.105.020 (22) "State agency"
Microsoft 365 email address contains an underscore character after directory synchronization

1. **When creating email accounts for individuals, agencies must use the naming format of FirstName.LastName@agency.wa.gov or Firstname.mi.LastName@agency.wa.gov for the primary SMTP email address and the User Principal Name (UPN). This applies to any individual that is assigned a state email address.**

    a. LastName can be one or more last names. Examples: Person.Smith@agy.wa.gov, Person.SmithJones@agy.wa.gov, Person.Smith-Jones@agy.wa.gov.

    b. Email accounts must be unique within each agency namespace. Duplicates may be resolved by adding a middle initial or a number following the LastName of the email address. Examples: Person.Smith1@agy.wa.gov, Person.Smith2@agy.wa.gov or Person.A.Smith@agy.wa.gov, Person.B.Smith@agy.wa.gov.

    c. Where the name exceeds 64 characters, names may be shortened.

    d. The Primary SMTP and UPN must match.

    e. Exceptions to this requirement include:

        i. Employees where the email address of the individual should be obfuscated for the protection of the individual in accordance with agency policy.

        ii. An individual may use their legal name or their preferred name that they are commonly known by as long as it meets the agency's policy. This may include, but is not limited to, a single name or where a last name is traditionally first.

    f. Sub addressing, also known as plus addressing, is permitted. Sub addressing allows users to create a tag on the email address, for example first.last+billing@agy.wa.gov. See support documentation Plus Addressing in Exchange Online.

2. **The local part (before the @) of the address cannot exceed 64 characters total as outlined in Request For Comment (RFC) 7504 SMTP 521 and 526 Reply Codes, and the entirety of the address cannot exceed 256 characters.**

3. **The format for authoritative, administrative, service, and secondary/proxy addresses is at the discretion of the agency.**

REFERENCES

1. RFC 7504 SMTP 521 and 556 Reply Codes.
2. Plus Addressing in Exchange Online.
3. Definition of Terms Used in Policies and Reports.

CONTACT

- For questions about this policy, please email the WaTech Policy Mailbox.
- For support with email services, please file a support ticket.

WaTech
Washington Technology Solutions

Project Quality Assurance Policy & Standards 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.

We engaged with an external consultant with the oversight team to review all the policies and standards and align them to the revised future state of oversight processes and procedures. The current policy is more focused toward Project Management Institute (PMI) standards, and we changed it to be more project success focused. It is methodology agnostic now.

What is the business case for the policy/standard?

QA and oversight provide guidance to keep projects on track with respect to time, budget, and scope. Regular assessments, continuous monitoring, and proactive sharing of findings to agencies supports successful implementation.

What are the key objectives of the policy/standard?

- Clear quality assurance requirements to align with tiered oversight.
- Focus efforts and budget based on the complexity and risk profile of the project.

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

Increasing our engagement on more complex and impactful projects and allowing flexibility to scale the engagement for low complexity investments supports Goal 4: Transform Service Delivery.

What are the implementation considerations?

- WaTech will need to communicate the new policy to agencies with current and pending projects.
- WaTech needs to communicate changes to the QA service providers.
- WaTech will include this information in the initiation phase of all upcoming projects.
- WaTech will post the changes on a public website.

How will we know if the policy is successful?

Specific: QA services are scaled based on the needs of the project.

Measurable: QA service delivery meets reporting engagement and reporting requirements as specified in the policy and the legislature.

Achievable: The changes allow the flexibility to scale activities to the need, which makes QA more achievable for all projects.

Relevant: QA services are essential, independent, forward-looking perspectives that support addressing risks and issues proactively for project success.

Timebound: This policy will be effective when adopted and implemented immediately for all new projects under oversight.

Equitable: By scaling requirements for QA, new vendors can gain experience with lower complexity projects. This offers opportunities for diverse vendors to grow into larger project engagements.

PM-03
State CIO Adopted: Month 01, 2024
TSB Approved: Month 01, 2024
Sunset Review: Month 01, 2027

Replaces:
IT Policy 132 Project Quality Assurance
March 15, 2023

WaTech
Washington Technology Solutions

PROJECT QUALITY ASSURANCE POLICY

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

1. **All Tier 2 and 3 projects are considered major IT projects and require quality assurance (QA) oversight as follows:**

   a. Agencies shall hire (or otherwise obtain) and use an external project QA provider.

   b. Project budgets must plan for adequate and appropriate levels of QA based on the scope over the full life of the project.

      i. Agencies are strongly encouraged to use QA during feasibility, procurement, and contracting phases, including the procurement or hiring of key project staff.

      ii. In all cases, the QA provider must be engaged prior to requesting WaTech approval of the investment and must continue until project close- out activities are completed.

   c. QA activities must be conducted using the minimum statement of work outlined in the Quality Assurance Standard – Minimum Project QA Activities.

      i. The State CIO may recommend additional required QA activities based on individual project risks and will communicate these to the Executive Sponsor.

   d. QA services must be provided by practitioners with at least the qualifications outlined in the Minimum Qualifications for Project Quality Assurance Providers.

   e. Agencies shall not use the services of a QA Practitioner on any project where the QA Practitioner is, or has been used, on any non-QA activities for the same project.

   f. Agencies will consult with WaTech on all QA solicitations and share

draft procurement documents prior to publication, posting or recruitment.

i. A representative from WaTech will be invited to participate in the QA selection process.

A. If WaTech does not respond to the invitation within five (5) days or if WaTech declines the invitation, the agency is free to proceed without a WaTech representative.

ii. The agency will make the final determination of the QA provider.

iii. The agency must ensure that there is no real or perceived organizational conflict in their selection, including ensuring the existence of clear managerial independence between the QA provider, the Project Manager, and the Executive Sponsor.

g. The QA Provider will develop a baseline QA Plan in accordance with section 1 of the Minimum Project Quality Assurance Activities and present it to the sponsoring agency for approval within the first 30 days of the engagement. The QA plan will be updated as needed over the life of the project.

h. A project readiness assessment will be required prior to moving beyond the planning phase. The QA provider will independently deliver this assessment to the Executive Sponsor and the State CIO or designee in accordance with Minimum Project QA Activities – Readiness Assessment Within the first 45 days of the engagement.

i. The agency must provide a written response to each QA recommendation to address an issue, a negative finding, and/or risk identified in the readiness assessment and post it on the Project IT Dashboard within ten (10) working days of receipt or the assessment.

ii. The results of the readiness assessment and agency's response to QA recommendations must be available prior to requesting WaTech approval of the investment.

i. The QA Provider will independently deliver draft and final QA reports, including risks, issues, findings; and recommendations to address an issue, a negative finding, and/or a risk, to the project Executive Sponsor and to the State CIO or designee in accordance with Minimum Project Quality Assurance Activities.

i. Each recommendation must correspond to the issue, risk or negative finding it will address, and how the recommendation will support project success.

j. The QA Provider will make QA reports available to the project Steering Committee. The QA Provider will provide regular and routine briefings at the project Steering Committee meetings.

k. The QA Provider will independently post all final QA reports on the WA State IT Dashboard within 2 working days of delivery.

l. If required for the project, the QA Provider may also provide QA reports or briefings to other external oversight and/or authorizing entities.

m. Following the readiness assessment, QA reports will be delivered on at least a monthly basis.

i. QA reports will be finalized and delivered within ten (10) working days following the end of the report period. This allows for prompt action on findings, recommendations, emerging issues, and risks as well as timely visibility to the Executive Sponsor and Steering Committee.

n. Following the delivery of a QA report, the sponsoring agency must provide a written response to each new QA recommendation to address an issue, a negative finding, and/or risk and must provide current status information on all open QA recommendations.

i. The response should clearly outline the action(s) to be taken (including additional investigation or assessment needed to determine other action(s) to be taken), by which person(s) and by what date.

ii. The agency must post the response to the Project Dashboard within five (5) working days of delivery of the final QA report.

iii. In all cases, the agency must finalize the plan of action for each new recommendation within thirty (30) calendar days of the delivery of the QA report.

2. Tier 1 Projects are considered major IT projects and require quality assurance oversight as follows:

a. Agencies are recommended to engage a quality assurance resource over the life of the project. This resource must be independent to the project organization, unless otherwise required by statute and meet the qualifications outlined in the Quality Assurance Minimum Qualifications Standard.

b. As a best practice, agencies should establish a QA plan and assess their readiness prior to moving beyond the planning phase.

c. Projects should regularly assess the progress and discuss any deviations, risks and issues with executive leadership following the minimum QA standards as described in Minimum Project QA Activities Standard. See Principles of Quality Assurance.

REFERENCES

1. PM-03-03-S - Minimum Project Quality Assurance Activities Standard.
2. PM-03-01-S - Minimum Qualifications for Project Quality Assurance Providers
3. PM-03-01-G - Principles of Quality Assurance Guideline
4. Definition of Terms Used in Policies and Reports | WaTech.

CONTACT INFORMATION

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

PM-03-02-S
State CIO Adopted: Month 1 2024
TSB Approved: Month 1 2024
Sunset Review: Month 1 2024

WaTech
Washington Technology Solutions

Replaces:
Standard132.20
Minimum Project Quality Assurance
Readiness Assessment
March 16, 2016

MINIMUM PROJECT QUALITY ASSURANCE ACTIVITIES – READINESS ASSESSMENT

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

1. **The readiness assessment shall include an evaluation of the following areas at a minimum:**

    a. Aligned business value to be achieved upon project implementation and which measures will be used to track business value.

    b. The SMART project objectives to be achieved at completion.

    c. Agency readiness assessment for the project and for the expected organizational model once the project is completed.

    d. Ensuring there is sufficient level of detail for the project planning activities to date including timeline of future decision points and major milestones.

    e. Project sponsorship and planned governance model and processes.

    f. Detailed project resources plan showing committed resources, stakeholders, and subject matter experts.

    g. The stakeholder engagement and communication plan, including both internal and external stakeholders as appropriate.

    h. Planned project methodologies and practice standards.

    i. An assessment of Organizational Change Management plan activities over the life of the project, including an initial assessment of the readiness of the organization for the culture change.

    j. Recommended future stages/gates for the project.

    k. Risk identification, impact assessment and mitigating planning.

2. **The Readiness Assessment Report shall contain the following:**

a. A cover letter addressed to the project sponsor and to the State CIO and signed by the QA provider responsible for the content that attests to the independent preparation of the report. The cover letter should also contain contact information for the preparer.

b. A summary level assessment of the readiness of the project to proceed, including identification of critical issues that must be addressed prior to the project proceeding.

c. A detailed narrative describing issues, negative findings, and/or risks; and corresponding recommendations to support project success.

REFERENCES

1. PM-03-01-G Principles of Quality Assurance Guideline
2. Definition of Terms Used in WaTech Policies and Reports.

CONTACT INFORMATION

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

PM-03-03-S
State CIO Adopted: Month 1 2024
TSB Approved: Month 1 2024
Sunset Review: Month 1 2024

WaTech
Washington Technology Solutions

Replaces:
IT Standard PM-03-03-S
Minimum Project QA Activities
January 19, 2016

MINIMUM PROJECT QUALITY ASSURANCE ACTIVITIES STANDARD

See Also:
RCW 43.105.054 WaTech Governance
RCW 43.105.205 (3) Higher Ed
RCW 43.105.020 (22) "State agency"
PM-03 Project Quality Assurance Policy

1. **The Quality Assurance (QA) provider will deliver a baseline quality assurance plan within 30 days of the start of the engagement that includes, at a minimum:**

    a. The methods and criteria to be used in conducting the QA engagement and assessing practice areas noted in Section 2. below.

    b. The timing and audience for draft and final reports and the template(s) for the ongoing report.

    c. The QA provider will present the plan to the agency for approval within the first 30 days of the engagement. The QA plan will be updated as needed over the life of the project.

2. **Each regular QA report must include, at a minimum, an assessment of the overall project performance, variances on Scope, Schedule and Budget and cover key practice areas or domains that align with the project's management methodology and industry best practice including but not limited to:**

    a. Overall health – Over the life of the project, are effective project management processes being used and coordinated within the project and with all project participants to achieve desired results and represents the combined assessment for all performance areas 2(b) through 2(l) as applicable.

    b. Scope – Does the project include an approach to managing scope to ensure the project success?

    c. Schedule – Is the project effectively managing the timely completion of the project?

d. Budget – Is the project routinely estimating, budgeting, managing, and controlling costs so that the project can be completed successfully?

e. Quality measures and business outcomes– Is the project defining quality measures and continuously improving processes to achieve project outcomes?

f. Team – Is the project acquiring, developing, and managing appropriately skilled and adequately staffed project teams?

g. Communications and Stakeholders - Is the team identifying stakeholders (people, groups, or organizations) that could impact or be impacted by the project? Is the project using appropriate strategies to engage stakeholders and supporting timely, appropriate, and accessible communications over the project's life?

h. Governance, escalation, and decision-making: Does the project have effective and engaged executive leadership and governance structure? Does the team follow established escalation process and work with project leaders to timely decision making for project success?

i. Risks, Issues, Action items, and Decisions – Is the project effectively identifying, analyzing, and controlling project risks and issues? Does the project have an effective process to manage action items and decisions?

j. Procurement and vendor management - Is the project appropriately managing the acquisition of products, services or results needed from outside the project team? Is the project effectively managing the resulting contracts over the life of the contract?

k. Training and business readiness – Is the project actively managing organization, user, and stakeholder readiness to effectively adopt, use and realize intended benefits? Are appropriate training, outreach, and reinforcement frameworks in place?

l. Deliverables (if in scope of work) – Has the project established acceptance criteria for deliverables that the deliverables are following and adhering to? Do deliverables align with industry best practice and overall project goal in achieving planned objectives?

3. **As the project nears implementation, regular assessments will focus on the current phase of the project and include discussion on organizational readiness,**

planning and readiness activities for transition to operations including governance following implementation.

4. **Each Quality Assurance report shall contain the following:**

    a. A cover letter signed by the QA provider responsible for the content that attests to the independent preparation of the report. The cover letter should also contain contact information of the preparer.

    b. An executive summary of project progress, execution strengths and weaknesses, and the most significant issues, risks or open recommendations.

    c. A detailed narrative describing issues, negative findings, and/or risks; and their recommendations to support project success. If the project is nearing a stage or gate, indicate whether the project is positioned to be successful in this next stage/gate.

    d. An assessment of the accuracy of the project's tracking of progress toward milestones and budget estimates.

    e. A risk assessment that identifies potential barriers to meeting project objectives and milestones, their probability of occurring and impact if they occur, and recommended and observed mitigations.

    f. An indicator suggesting the trend whether the risk in each of the assessment areas is increasing, decreasing or remains the same. Shorthand symbol and definitions:

        i. Risk is decreasing. 

        ii. Risk is increasing. 

        iii. Risk is the same. 

    g. A table that summarizes all open recommendations as well as those closed during the reporting period, including the QA provider's assessment of the agency's actions on the listed recommendations.

5. **As part of closeout, the Quality Assurance Provider will report on key lessons learned from the project within 30 days of project completion or termination.**

REFERENCES

1. Definition of Terms Used in WaTech Policies and Reports.

CONTACT INFORMATION

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

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.

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

Replaces:
N/A

WaTech
Washington Technology Solutions

SECURITY PRINCIPLES GUIDELINE

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

The following principles are a framework for Washington State information security practices and platform implementations:

a. Accountability – Clearly define accountability and responsibility for information security within a structured cybersecurity management framework. Both management and staff should acknowledge and accept their roles to ensure compliance and oversight.

b. Risks – Risks to information systems and data should be assessed periodically and managed continuously as part of a robust state cybersecurity risk management strategy that addresses emerging threats, vulnerabilities, and risks to maintain a secure environment.

c. Awareness– Ensure all users with access to information systems or data are consistently aware of the importance of information security and their role in maintaining it.

d. Cost Effective – Information security controls should be cost-effective and proportionate to the identified risks. Resource allocation for security measures will be optimized to ensure maximum protection without unnecessary expenditure.

e. Ethical – Information systems and data will be used and operated in accordance with the state's ethics policies and practices, ensuring ethical conduct in all information security activities.

f. Defense-in-Depth – Select and architect information security controls with a "Defense-in-Depth" approach, employing multiple layers of protection to comprehensively defend against potential security threats.

g. Equitable – Information security policies should balance the rights of customers, users, and third parties with the state's operational needs. This balance is crucial to achieving the state's objectives while respecting individual rights.

h. Governance—Information security policies and standards should be developed based on industry-recognized security standards and best practices. These policies and standards will undergo periodic reviews and corrective actions will be taken to remediate identified deficiencies promptly.

i. Integration – Information security is fundamental to sound business management. It should be integrated into the state's overall information management framework to support and enhance business operations.

j. Minimize Complexity – Information technology services and systems should be designed to minimize technological diversity and reduce complexity. Simplifying the technology landscape will enhance manageability and security.

k. Least Privilege – Grant only the minimum necessary privileges to users, systems, and processes required to perform their assigned functions, limiting potential damage from accidental or intentional misuse of access.

l. Separation of Duties – Responsibilities and privileges should be segregated to prevent any individual or small group from controlling multiple critical aspects of a process. This separation is vital to preventing inappropriate actions and mitigating potential harm or loss.

m. Timeliness – Agencies should act promptly and in a coordinated manner to prevent, detect, and respond to potential incidents affecting information systems or data. Timely action is essential to mitigate risks and maintain system integrity.

REFERENCES

1. Definition of Terms Used in WaTech Policies and Reports.

CONTACT INFORMATION

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

PROPOSED DEFINITIONS

Separation of Duties

The principle that no single user should have sufficient privileges to misuse the system or process on their own.

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.

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

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

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.

WaTech
Washington Technology Solutions

Digital Accessibility Policy and 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.

We worked as a small group drawn from the Accessibility Community of Practice. We looked at other state policies to consider how others are doing it.

We added requirements for general awareness training and specific training for roles directly impacting accessibility.

The standard requires adherence to version 2.1 Level AA. We added a deadline for the Standard for WCAG 2.2 Level AA for July, 2026 due to the upcoming WCAG 3.0.

What is the business case for the policy/standard?

Accessibility is about equity. Equity in access as a human right. Digital accessibility has unique characteristics compared to physical accessibility. A recent federal rule by the Department of Justice underscored the connection between the Americans with Disability Act (ADA) and digital accessibility by requiring government agencies to comply with Web Content Accessibility Guidelines in order to comply with the ADA. See the Fact Sheet: New Rule on the Accessibility of Web Content and Mobile Apps Provided by State and Local Governments | ADA.gov.

Services need to meet ADA standards Title II to ensure we are not discriminating against individuals with disabilities, as part of individuals' civil rights. Systems for hiring need to ensure equality, and access to talent. When systems are more accessible for people with disabilities, they are usually easier for all people.

What are the key objectives of the policy/standard?

- Define expectations for digital accessibility as compared to physical accessibility. Digital accessibility is about more than a website—it includes all digital content and digital interaction.
- Increase employment rates of people with disabilities.

- All people are able to contribute equitably at the workplace.
- Provide accessibility for customers and residents.
- Concepts around co-creation and "Nothing About Us Without Us" are incorporated.
- Consider all tools to support all people in an equitable manner.
- Be open to modify our approach as technology and human interactions with technology changes and our understanding of ability and disability improves.
- Ensure best practices for procurement to develop accessibility plans for technology that will not meet accessibility requirements.

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

This policy provides clarity and roadmap for maturation of IT accessibility to align with federal and state rules.

Executive Order 13-02 (wa.gov)
Title 1 & Title 2 of the Federal Americans with Disabilities Act
Sections 504 and 508 Rehabilitation Act of 1973
RCW 49.60.03 Discrimination – Human Rights Commission
RCW 70.84.010 Declaration – Policy
RCW 42.56 Public Records Act
Executive Order 23-02 Plain Language

What are the implementation considerations?

- Support agencies in meeting and exceeding the 'minimum' standard and understanding that digital accessibility is not for just websites.
- Establish a course of best practices/processes.
- Adopt a digital accessibility maturity model to help agencies assess their current accessibility status and chart a path toward improvement.
- WaTech will need to create Accessibility General Awareness Training through the Department of Enterprise Services (DES) Learning Management System (LMS).

How will we know if the policy is successful?

Specific: Agencies are implementing processes to prioritize accessibility at key points and following up on identified gaps.

Measurable: Agencies will maintain current IT Accessibility plans, include accessibility validation in procurement, and ensure all employees take general accessibility awareness training.
Achievable: WaTech will support agencies by providing general awareness training. Agencies may need to request funding for more specific training. Agencies will need to scrutinize all practices to ensure accessibility is considered by design.
Relevant: The federal government released new a rule requiring compliance with WCAG 2.1 AA by April 24, 2026. Accessibility is ripe with opportunity for innovative solutions that benefit everyone.
Timebound: The standard updates immediate compliance to Level AA with Web Content Accessibility Guidelines (WCAG) 2.1. We set July 1, 2026 as the expectation to comply with 2.2
Equitable: This policy and standard are intended to ensure agencies are providing equitable access to all state IT resources, and to plan for alternative solutions where native solutions do not exist.

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

Replaces:
Policy 188
March 10, 2010

Washington Technology Solutions

DIGITAL ACCESSIBILITY POLICY

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. **All covered technology must be accessible to and usable by individuals with disabilities, either directly or by supporting the use of assistive technology**. The USER-01-01-S Digital Accessibility Standard **outlines the minimum levels for compliance.**

    a. This includes all technology whether:

        i. Acquired.

        ii. Procured.

        iii. Developed.

        iv. Substantially modified.

        v. Substantially enhanced.

        vi. Technology available at no cost.

2. **Regardless of exceptions provided in this policy, agencies must provide individuals with disabilities with effective communication, reasonable modifications, and an equal opportunity to participate in or benefit from their services, programs, and activities.**

3. **The following exceptions apply to public facing content:**

    a. Web content that meets all four of the following points:

        i. The content was created before the date the state or local government must comply with this rule, or reproduces paper documents or the contents of other physical media (audiotapes, film negatives, and CD-ROMs for example) that were created before the government must comply with this rule; and

        ii. The content is kept only for reference, research, or recordkeeping; and

iii. The content is kept in a special area for archived content, and

iv. The content has not been changed since it was archived.

b. Preexisting conventional electronic documents that meet all of the following points:

i. The documents are word processing, presentation, PDF, or spreadsheet files; and

ii. They were available on the stated or local government's website or mobile app before the date the state or local government must comply with this rule; and

iii. Documents that are not currently being used to apply for, access, or participate in a state or local government's services, programs, or activities.

c. Content posted by a third party when outside of contractual, licensing, or other arrangements with a public entity. Tools and platforms that allow third parties to post content are not part of this exception.

d. Individualized documents meet all three of the following conditions:

i. The documents are word processing, presentation, PDF, or spreadsheet files; and

ii. The documents are about a specific person, property, or account; and

iii. The documents are password-protected or otherwise individually secured.

e. Preexisting social media posts.

f. Where strict adherence would result in a fundamental alteration in the nature of a service, program, or activity of the public entity or in undue financial and administrative burdens.

4. **Where a covered technology is not able to be brought into compliance, the system or content owner is responsible for providing individuals with disabilities equivalent access.**

5. **Effective July 1, 2029, in addition to the requirements set forth in this policy for covered technology, all content and tools that employees or users need to perform essential job duties, access information, or participate in programs must**

be accessible or content owner is responsible for providing individuals with disabilities equivalent access.

6. **Technology that agencies use at an enterprise level must be held responsible at the service owner level.**

7. **This policy does not release agencies of their responsibility to provide language access, physical access to buildings, accessible communications to their staff and the public with limited or no internet access, where digital communications may not meet the needs. Agencies must also follow the relevant state policies for language access and disability access.**

8. **WaTech will sponsor annual digital accessibility awareness training for state agency consumption. WaTech will update this training to keep up with changes in the industry as needed.**

9. **Agencies must develop an agency policy to support and ensure compliance with this policy and USER-01-01-S Digital Accessibility Standard.**

    a. Agencies must have a digital accessibility policy that describes how the agency will execute the state policy and defines accessibility roles and responsibilities within the agency to support this, including the accessibility coordinator.

    b. Agencies will require and document annual digital accessibility awareness training for all employees.

    c. Agencies will require and document additional training for roles with a larger impact on IT accessibility, such as software development. Agencies will determine and document the frequency of the training.

10. **Agencies must evaluate current technology accessibility to develop and implement an IT Accessibility Plan and update it at least annually.**

    a. The agency's IT Accessibility Plan identifies how the agency will ensure new covered technologies are accessible and the plan for making existing covered technologies accessible. See Guidance on Applying WCAG 2 to Non-Web Information and Communications Technologies (WCAG2ICT) (w3.org)

    b. Agency plans must minimally contain:

        i. A list of prioritized non-accessible covered technology recommended alternative access methods, and actions to correct the issue.

1. Agencies must consider impact to users and frequency of use when prioritizing corrective action, especially for users with disabilities and/or users of assistive technology.

2. Agencies must consult community members with related lived experience in building IT Accessibility Plan priorities.

ii. Agencies must identify their key functions and how currently non-accessible content impacts their key functions. Agencies identify what key functions are needed (by state staff and members of the public) such as signing up for state services, distributing benefits, and grant reporting.

iii. Agencies will include an expected timeline for each corrective action.

c. Agencies must post a public version of their IT Accessibility Plan including recommended alternative access methods. This may be incorporated into the Americans with Disabilities Act transition plan. See ADA Update: A Primer for State and Local Governments, Planning for Success

11. Agencies must identify an information technology accessibility coordinator to be the key contact regarding the agency's information technology accessibility plan and to support complaint resolution.

a. Agencies must have contact information for the agency accessibility coordinator for any individuals who may encounter access issues or need to request alternate formats. See the

b. Agencies may need to meet additional requirements for federal or other partners.

12. Agencies must develop processes and procedures to ensure new covered technology is accessible according to the USER-01-01-S Accessibility Standard.

REFERENCES

1. Definition of Terms Used in WaTech Policies and Reports.
2. Guidance on Applying WCAG 2 to Non-Web Information and Communications Technologies (WCAG2ICT).
3. USER-01-01-S Digital Accessibility Standard.

CONTACT INFORMATION

For questions about this policy, please email the WaTech Policy Mailbox.
For technical assistance, please request support at support@watech.wa.gov.

DEFINITIONS

Covered Technology:
All public-facing digital content and tools, including:

- Websites,
- applications,
- documents and media,
- blog posts, and
- social media content.

Certain non-public-facing content that must also comply including:

- All electronic content used for official business to communicate,
- emergency notifications,
- initial or final decisions adjudicating administrative claims or proceedings,
- internal or external program or policy announcements,
- notices of benefits, program eligibility, employment opportunities, or
- personnel actions, formal acknowledgements or receipts.

Disability
An actual, perceived, or non-apparent physical, sensory, mental, or cognitive condition that has an adverse effect on a person's ability to carry out day-to-day life functions. Environmental barriers may hinder persons with disabilities from fully and effectively participating on an equitable basis (Diversity, Equity, Inclusion (DEI Glossary | SPSCC)

Equivalent Access
Equivalent access has such a minimal impact on access that it would not affect the ability of individuals with disabilities to use the agency's web content or mobile app to do any of the following in a manner that provides *substantially equivalent timeliness, privacy, independence, and ease of use*:

a. Access the same information as individuals without disabilities.
b. Engage in the same interactions as individuals without disabilities.
c. Conduct the same transactions as individuals without disabilities; and
d. Otherwise participate in or benefit from the same services, programs, and activities as individuals without disabilities.

Information Technology Accessibility/Digital Accessibility
Information technology accessibility or digital accessibility means all people can perceive, understand, navigate, and interact with electronic information and be active in the digital world. Accessibility supports social inclusion.

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

Replaces:
188.10 Minimum Accessibility Standard
August 31, 2021

WaTech
Washington Technology Solutions

DIGITAL ACCESSIBILITY 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 minimum level of accessibility compliance for covered technology is Level AA compliance with Web Content Accessibility Guidelines (WCAG) 2.1, including the guidelines associated with these principles:**

    a. Perceivable - Information and user interface components must be presentable to users in ways they can comprehend.

    b. Operable - User interface components and navigation must be operable.

    c. Understandable - Information and the operation of user interface must be understandable.

    d. Robust - Content must be robust enough that it can be interpreted reliably by a wide variety of user agents, including assistive technologies.

2. **WCAG 2.1 AA provides success criteria for measuring web accessibility and provides principles and useful metrics for products and services that are not specifically web based.**

3. **Effective July 1, 2026, the minimum level of compliance for accessibility is Level AA compliance with WCAG 2.2.**

4. **Agency covered technology procurement and contracting activities must include the following:**

    a. Accessibility requirements in the procurement, design, project scope, budget, and maintenance of IT Project/Systems applications and IT services.

    b. Accessibility validation:

        i. Ensure agency or third-party human user testing to validate accessibility, and;

        ii. A third-party accessibility validation report, or;

iii. Vendor Product Accessibility Template (VPAT) or;

iv. Compliance review documentation showing an evaluation of the solution's compliance with the applicable WCAG level.

c. Remediation activities:

i. Require a remediation plan from the vendor for addressing accessibility issues.

ii. Evaluate the vendor's remediation plan and timeline and determine contractual clauses to enforce remediation.

iii. Where the vendor does not have a remediation plan, and no other accessible solution will meet the agency's needs, agencies must:

1. Ensure alternative methods for access are incorporated into the agency's IT Accessibility Plan. Alternative access methods must also comply with applicable Washington State IT policies and standards.

2. Reserve the right to reduce the amount or terminate contracts where vendors demonstrate a lack of accountability to timely response and remediation and accessibility improvements with new releases and updates. This also applies if a vendor misrepresents the current accessibility of their products.

3. Consider the track record of vendors through comprehensive evaluation of accessibility and prioritization of accessibility, including contract violations, in renewal processes or new procurement processes.

REFERENCES

1. Web Content Accessibility Guidelines (WCAG) 2.1.
2. Web Content Accessibility Guidelines (WCAG) 2.2.
3. Definition of Terms Used in WaTech Policies and Reports.
4. Guidance on Applying WCAG 2 to Non-Web Information and Communications Technologies (WCAG2ICT)

CONTACT INFORMATION

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

DEFINITIONS

Covered Technology:
All public-facing content, including websites, applications, mobile applications, documents and media, blog posts, and social media content. Non-public-facing content available to employees to consume and/or interact with must also comply. Examples include but are not limited to:

- All electronic content used for official business to communicate emergency notifications, initial or final decisions adjudicating administrative claims or proceedings, internal or external program or policy announcements, notices of benefits, program eligibility, employment opportunities or personnel actions, formal acknowledgements or receipts, questionnaires or surveys, templates or forms, educational or training materials, and intranets.
- Administrative systems employees interact with, such as a timecard system, or any other systems used to perform work.