

Policy & Standard Background

Name: Policy 103 - Waivers

New, Update or Sunset Review? Update/Sunset Review

What is the business case for the policy/standard?

- Agencies are required to comply with technology policies and standards unless a specific waiver is granted. The policy allows the State CIO and designees to assess, manage and track instances of non-compliance.

What are the key objectives of the policy/standard?

- Lay out a standardized process for requesting waivers, responding to waivers and monitoring approved waivers.

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

- Waivers allow the state to understand where barriers exist to individual agency compliance with policy/standards and to understand where agencies are not complying with policy direction.

What are the implementation considerations?

- This is a procedural policy. The key change is to have policy match practice on delegated authority for waiver disposition.
- There are no new requirements or process changes for agencies as a result of these updates.

How will we know if the policy is successful?

of waivers submitted - policy/standard
% of approved waivers that result in compliance

CURRENT POLICY

Policy No. 103 – Technology Policy and Standards Waiver Request

Purpose:

This policy provides for a waiver process to request an exception from a state technology policy or standard.

Policy Statement:

1. Agencies must request a waiver when there is or is expected to be noncompliance with a technology policy or standard.
2. Waiver requests must be submitted to the State Chief Information Officer (CIO) (or designee) in writing and signed by the agency head and the agency CIO (or equivalent). The waiver request will contain at least the following information:
 - a. The specific section(s) of the policy and/or standard of which a waiver is requested,
 - b. A description of the extent of non-compliance with the section(s) identified,
 - c. An explanation of the technical, business or other factors that prevent compliance,
 - d. A description of all associated risks that could result from noncompliance.
 - e. Mitigations that have been or will be implemented to address the risks of noncompliance,
 - f. Steps planned to become compliant, and
 - g. The date by which compliance will be achieved.
3. The State CIO will endeavor to decide waiver requests within 30 days of receipt or within 30 days after receiving all information necessary to evaluate the request.
4. If needed, the State CIO will request additional information within 15 days of receipt of the waiver request or as soon as the need for additional information becomes known.
5. Waiver request evaluation criteria include, but are not limited to:
 - Security exposure
 - Increase in risk of loss or failure to the state, its communities and to citizens
 - Architectural alignment and interoperability
 - Economic impacts

- Impacts on agency operations
 - Legislative intent
6. The State CIO will decide waiver requests in one of several ways based on the information provided:
1. Approval in whole or in part for an unlimited period of time, with or without conditions;
 2. Approval in whole or in part for a specified period of time, with or without conditions; or
 3. A denial of the waiver request in whole or in part.
7. Following decision of the state CIO, the agency must complete all necessary steps and observe all conditions described in the waiver decision.
8. The agency will provide progress reports to the State CIO at least a quarterly basis on the status of actions undertaken in accordance with the waiver decision until compliance is achieved.

NOTE: Waiver requests and supporting documentation containing information that could potentially compromise the information technology security of the State are exempt from public disclosure pursuant to RCW 42.56.420.

Contact Information:

Contact the [OCIO Policy & Waiver Mailbox](#) if you have questions about this policy.

Sunset Review Date: May 31, 2018

Adoption Date: May 2015

Revision History – This is a new policy. Some material contained in the policy was separated from a prior version of Policy 101.

Approving Authority

/s/ Michael Cockrill 05/13/15
Chief Information Officer
Chair, Technology Services Board

PROPOSED UPDATES TO POLICY

Policy No. 103 – Technology Policy and Standards Waiver Request

PURPOSE

One of the statutory functions of the state Chief Information Officer and the Office of the Chief Information Officer is the establishment of technology policy and standards. Agencies are required to comply with technology policies and standards unless a specific waiver is granted.

This policy provides for a waiver process to be used when an agency is unable to be immediately in compliance with an established technology policy and/or standard. A waiver is generally intended to be time limited and granted only for the period of time necessary to achieve compliance.

By requiring the timely reporting of noncompliance with technology policy and standards through the waiver application and the granting of waivers setting the limits and conditions for future compliance, the OCIO is able to oversee and manage agency adherence to state-wide information technology requirements.

POLICY STATEMENTS:

1. Institutions and agencies subject to the State Chief Information Officer (CIO) as designated in [Technology Policy 101 - Technology Policies and Standards](#) are responsible for complying with all published technology policies and standards unless a waiver has been granted by the State Chief Information Officer.
2. The State Chief Information Officer (CIO) is responsible for decisions on all waiver requests associated with the state's Technology Policy and standard.
 - a. The State CIO (or designee) cannot grant a waiver of a statutory or regulatory requirement outside the scope of the office.
 - b. Only the State CIO may grant or deny waiver requests related to services or solutions which have been designated as an enterprise service as outlined in Policy 185 - [Establishing an Enterprise Service](#).
 - c. The State CIO delegates authority for disposition of certain other waiver requests:
 - i. The State Chief Information Security Officer (CISO) is given delegated authority to grant or deny all waivers for security related policies and standards.
 - ii. The Deputy Director, Office of the State Chief Information Officer (OCIO) is given delegated authority to grant or deny all waivers for non-security related policies and standards except for those related to the enterprise service designations.
3. Agencies must request a waiver in advance when they expect to be noncompliant with a state technology policy or standard or immediately upon discovery of noncompliance.
 - a. Waiver requests must be submitted in writing to the State CIO (or designee) using the [OCIO Policy and Waiver mailbox](#).
 - b. Waiver requests must be approved and signed by the agency head (or acting agency head) and the agency CIO (or equivalent if the agency does not have a CIO) prior to submission.
 - c. Waiver requests must contain at least the following information:
 - i. The specific section(s) of the policy and/or standard of which a waiver is requested,
 - ii. A description of the extent of non-compliance with the section(s) identified,
 - iii. An explanation of the technical, business or other factors that prevent compliance,

- iv. A description of all associated risks that could result from noncompliance,
 - v. Mitigations that have been or will be implemented to address the risks of noncompliance,
 - vi. Steps planned to become compliant, and
 - vii. The date by which compliance will be achieved.
4. If additional information is needed, the State CIO (or designee) will request it within 15 days of receipt of the waiver request or as soon as the need for additional information becomes known.
5. The State CIO (or designee) will endeavor to decide waiver requests within 30 days of receipt or within 30 days after receiving all information necessary to evaluate the request.
6. The State CIO (or designee) will communicate decisions on waiver requests formally and in writing. Decisions may be in one of the following ways:
 - a. An approval of the request, in whole or in part, for an unlimited period of time, with or without conditions;
 - b. An approval of the request, in whole or in part, for a specified period of time, with or without conditions; or
 - c. A denial of the request in whole or in part.
7. Following the decision of the state CIO (or designee), the agency must complete all necessary steps and observe all conditions described in the waiver disposition memo.
 - a. The agency will provide progress reports to the State CIO (or appropriate designee) on at least a quarterly basis, or as otherwise required in the waiver disposition memo, about the status of actions undertaken in accordance with the waiver decision until compliance is achieved. Status reports should be sent to the [OCIO Policy and Waiver](#) mailbox.
8. Agencies which are neither in compliance with Information Technology Policy and Standards, nor in receipt of a valid waiver, may be subject to OCIO remedial action, including reporting to the Governor any matters relating to abuses or evasions of OCIO policy as required by RCW 43.105.025.

CONTACT INFORMATION:

Contact the [OCIO Policy & Waiver Mailbox](#) if you have questions about this policy.

SUNSET REVIEW DATE:

Proposed February 28, 2021

ADOPTION DATE:

Targeted date is February 8, 2018

APPROVAL DATE:

Targeted Date is March 13, 2018

Approving Authority

Policy 103 - CIO Review – Comment Reconciliation Document

Name	Org	Comment	Disposition
Beth Hutchins	MIL	Policy statement 8 Please provide specifics as to how “remedial action” is defined and what form such an action may take. How will agencies be put on notice that such an action is impending? Will agencies be given an opportunity to challenge / discuss the matter prior to such an action? Will they be able to respond to any reports to the governor? Also, is there an appeals process for those agencies who do not feel these actions are merited?	No change made. Will clarify with requestor that this would occur as part of escalation and only after other measures had been unsuccessful.
Michelle Tuscher	ACB	The policy revisions look good	No change needed.
Shelby Eagan	DOH	Policy statement 3.b. Change to ‘Waiver requests must be approved and signed by the agency head (or designee) and the agency CIO (or equivalent if the agency does not have a CIO)’	Instead of designee, will include (or acting agency head). Waivers are to some extent temporary acceptance of risk and want to make sure agency head is aware and not have this delegated to others in the organization.
Shelby Eagan	DOH	Add a new policy statement 4 to say “OCIO will provide confirmation of receipt of the agency waiver request within 5 business days of delivery.”	Will create a roles/responsibility document to incorporate this item and others of a similar nature.
Shelby Eagan	DOH	Modify Policy statement 4 to read: “If additional information is needed the State CIO (or designee) will request the information in writing within 15 days...”	Incorporated
Marie Finn	DSHS	Policy 3a: Recommend one point of contact (OCIO Policy and Waiver mailbox) and an internal OCIO process to ensure State CIO is copied.	That was the intent of the original language but sentence wasn’t worded well. Cleaned up language to make it clear submission is via the shared mailbox and to the State CIO (or designee).
Marie Finn	DSHS	Policy statement 5: If a decision on a waiver request exceeds 30 days, in either situation, the agency should be notified as to the reason for the delay and expected date of the decision.	Didn’t add this to the policy but will add to a companion roles/responsibility document.
Marie Finn	DSHS	Policy statement 7 a – Will there be a consistent approach for status reports or is that up to the agency.	No change made. Generally left up to the agency based on the waiver related activities. However, if

Policy 103 - CIO Review – Comment Reconciliation Document

Name	Org	Comment	Disposition
			there was a specific format, it would be noted as a condition in the waiver response.
Debbie Kendall	DOC	Ensure titles clarify State CIO and State CISO from agency CIOs and agency CISO throughout.	Incorporated
Steve Young	DNR	No issues from DNR	No action needed
	DSHS	Change policy statement 5 to “The State CIO (or designee) will provide a determination on all agency waiver requests within 10 working days of receipt or, in cases of an a time sensitive request, within 3 working days after receipt of all supporting documentation. Failure by the State CIO (or designee) to meet this timeline will result a temporary waiver approval for the agency to operate for a period of 30 calendar days or when the State CIO renders a decision (whichever is shortest).”	Unable to incorporate language. This comment was received late and have been unable to connect with commenter to understand underlying concern, and to confirm understanding of waivers as a vehicle for documenting compliance plans. It does not reflect level of conversation and negotiation that may be required to ensure the states interests are protected. The policy notes a timeline that the CIO can work to achieve (i.e., within 30 days). However, there have been rare situations where urgent response has been needed and those urgent timelines have been met. As noted, can create companion roles/responsibilities document to clarify how to make/identify urgent requests. Will continue to attempt to reach the commenter to understand concerns and address to the greatest extent possible via process.