Maine State Government
Department of Administrative & Financial Services
Office of Information Technology (OIT)

Waiver Policy

1.0 Statement

Adherence to policy, standards, and procedures is a necessary part of conducting State business. It is equally important to document the process for exceptions.

2.0 Purpose

The purpose of this policy is to document the waiver workflow and compliance-tracking.

3.0 Applicability & Definitions

This policy is applicable to all Office of Information Technology (OIT) issued policies, standards, and procedures. The following definitions are applicable to this policy:

3.1 **Approved**: A waiver has been approved by the CIO or authorized designee. Depending on the context of the approval, there may be conditions formally connected to the approval.

3.2 **Expired**: A waiver has exceeded the time that was approved by the CIO which if filed and in place. Should a waiver still be required, please follow the Waiver Extension provision in this policy below. If the waiver has been satisfied, please follow the Waiver Satisfaction provision in Section (number) below.

3.3 **Modified:** A waiver that has been changed to reflect current state of conditions which can be either Minor or Significant

3.4 **Not Approved**: A waiver request was denied by the CIO or authorized designee.

3.5 **Replaced**: A waiver extension has been filed and accepted by the CIO. This waiver is no longer active and is marked "Replaced" The extension waiver will become the current waiver for the defined asset.

3.6 **Satisfied**: The CIO has approved the closure of the waiver based on evidence that explicitly shows that the waiver condition has been resolved.

3.7 **Withdrawn**: A waiver has been officially requested to be withdrawal and the waiver is voided.

3.8 **Waiver Close Out**: A waiver which has been satisfied, or the asset has been formally decommissioned, and the associated artifacts to record detailed actions (Request for Change (RFC) and Enterprise Tickets) have been referenced to confirm the status.

4.0 Responsibilities

4.1. The Chief Information Officer (CIO) is responsible for enforcement of this policy.

4.2. The Enterprise Architect facilitates the waiver workflow.

4.3. Those seeking a waiver are not permitted to proceed with their desired outcome until they receive an email from the Enterprise Architect on behalf of the CIO indicating the waiver has been approved. There is no transfer or accepting liability by the State of Maine involving a vendor product through a waiver being submitted, reviewed and approved by the CIO.

4.4. Those seeking a waiver must ensure that the business owner identified in section 5.1.1 supports the waiver request, understands and accepts the risk, and supports the remediation strategy to achieve standard/policy compliance within the timeframe specified.

4.5. The IT Manager identified in section 5.1.1 must be an IT Director, or a designee authorized on their behalf.

5.0 Directives

5.1. The waiver application is initiated by including any relevant documentation within an Enterprise Ticketing System ticket and detailing the answers to the following items (5.1.1 through 5.1.9) within the body of an email to OITEnterpriseArchitect@Maine.Gov. Please note that scans must be attached to an Enterprise Ticketing System ticket and noted in sections 5.1.7. or 5.1.8.

5.1.1. State the name of the person/agency requesting the waiver, the IT Manager approving the request to move forward, and the business owner accepting the risk identified in the waiver request.

5.1.1.1. The identified business owner must have the authority within their organization to form a binding agreement with the OIT CIO.

5.1.1.2. The identified IT Manager must be an IT Director, or a designee authorized on their behalf.

5.1.1.3. The three individuals identified as the requestor, IT Manager, and business owner must be different.

5.1.2. Identify the policy or standard for which the waiver is being requested.

5.1.3. Describe the compelling technical or business justification for the policy exception, including the impact if the waiver is not approved.

5.1.4. What are the business and technical risks to the State if the waiver is approved?

5.1.5. State the duration of the waiver.

5.1.6. Describe the exit strategy to terminate the waiver and to bring the product into our standard offering. The exit strategy for a technology (containment or retirement) waiver must include the support model to be used until compliance is achieved.

5.1.7. When requesting a security or accessibility waiver: Provide the Application Inventory ID number of the application, the Enterprise Ticketing System ticket number that contains a security scan no older than six months, an approximate number of both internal and external users, and the classification of the data transacted by the application (see the Data Classification Policy).[1]

5.1.7.1. If the most recent security scan is older than six months, a new scan must be requested from and evaluated by the Security Operations Center (SOC) team prior to submitting a waiver request.

5.1.7.2. Security scans completed by external parties must be submitted to the SOC team through the Enterprise Ticketing System for further evaluation.

5.1.8. When requesting an accessibility waiver: Provide the Enterprise Ticketing System ticket number that contains the most recent accessibility scan, and an approximate number of both internal and external users.

5.1.9. If requesting a waiver extension, the request must cite the waiver number and title of the most-current waiver.

5.2. Approval or denial of the request will be made within three weeks of the submittal via email to the requestor and will include the individuals outlined in 5.1.1. Emergency requests will be handled in the same manner only on an expedited scale.

5.3. Before the expiration date of the waiver period, it is expected that corrective actions would have been undertaken to convert to an accepted policy standard. All requests for waiver extensions, with justifications, must meet the minimum requirements outlined in 5.1, above.

5.4 Waivers close outs will be expected when an asset has been decommissioned, and the waiver is no longer required. Each waiver requestor will be responsible for the formal notification to the Enterprise Architect on any asset that has a waiver no longer needed as a result of decommissioning the asset. The requester is

[1] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/DataClassificationPolicy.pdf

responsible for providing to the Enterprise Architect through a formal email to OITEnterpriseArchitect@Maine.Gov include the following:

5.4.1 Artifacts of RFC or Enterprise Ticket Numbers related to the decommissioning of the asset, all data has been secured or destroyed and associated waivers are presented with the correctly identified asset name and waiver ID.

5.4.2 Confirming waivers connected to decommissioned assets be reflected in the enterprise waiver database.

6.0 Document Information

6.1. Initial Issue Date: February 22, 2010
6.2. Latest Revision Date: May 30, 2025
6.3. Point of Contact: OIT Enterprise Architect, OITEnterpriseArchitect@Maine.Gov
6.4. Approved By: Chief Information Officer, OIT
6.5. Legal Citation: Title 5, Chapter 163: Office of Information Technology[2].
6.6. Waiver Process: N/A

[2] http://legislature.maine.gov/statutes/5/title5ch163sec0.html