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

This policy is applicable to all Office of Information Technology (OIT) issued policies, standards, and procedures.

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. Any waiver by the CIO does NOT constitute acceptance by the State of any liability associated with a vendor product.

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 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.

5.1.1. State the name of the person requesting the waiver, the IT Manager approving the request to move forward, and the business owner accepting the risk of the change 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 IT Manager, business owner, and requestor 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 waiver: Provide the Enterprise Ticketing System ticket number which 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 which 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.

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

5.3. By the expiration of the waiver period, it is expected that corrective actions would have been undertaken to convert to an accepted standard or policy. Should that not be the case, the requester may petition for a follow-up waiver with an explicit explanation as to why they did not adhere to the terms of the original waiver approval. All requests for waiver extensions must meet the minimum requirements outlined in 5.1, above.

6.0 Document Information

6.1. Initial Issue Date: February 22, 2010

6.2. Latest Revision Date: May 29, 2024

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