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

Infrastructure Deployment Certification Policy

1.0. Purpose

1.1. Any critical infrastructure technology ready to be deployed must undergo a battery of tests. Based on the test results, the Chief Information Officer (CIO) makes the final determination if the infrastructure is suitable for deployment.

1.2. As technology becomes more complex, more interconnected and integrated with infrastructure, and more exposed to the external world, it has become even more important to thoroughly vet them before they are deployed into service. This policy establishes a uniform and objective battery of tests that enables the CIO to evaluate the suitability of infrastructure assets to be deployed into service. A direct benefit of this policy is that it leads to pre-certified infrastructure.

2.0. Definitions

2.1. **Infrastructure**: Systems and assets, whether physical or virtual, refer to the composite hardware, software, network resources, and services required for the existence, operation, and management of an IT environment. It allows an organization to deliver IT solutions and services to its employees, partners and/or customers.

2.2. **Application**: A system/application used by any Agency to manage business programs and data including the underlying services that support them. This includes applications that may be supported by some entity other than OIT.[1] This includes external and internal interfaces. It also includes Internet applications used by any Agency regardless of where hosted (contracted, housed, and remotely hosted etc.).

2.3. **Infrastructure Owners**: With respect to the infrastructure considered for deployment, the Project Manager, Infrastructure Manager, IT Director, and Executive Director are jointly and collectively identified as the Infrastructure

[1] https://legislature.maine.gov/statutes/5/title5ch163sec0.html

Owners. If any of the roles are vacant, the same person fulfils more than one role, or if there is a difference in opinion with respect to this policy among the three roles, for this policy, the decision of the Executive Director, Client and Infrastructure Services, will be final and binding.

2.3.1. **Project Manager:** is the OIT representative whose responsibilities include the coordination and completion of projects managing budget, scope, and schedule targets.

2.3.2. **Manager:** is the OIT representative who works with any Agency and whose responsibilities include building and deploying the asset.

2.3.3. **IT Director:** is the OIT representative with the authority to determine the business objectives of the infrastructure and the priority of the asset features that are developed.

2.3.4. **Executive Director:** is the OIT representative that has accountability for the strategic direction and budget of the infrastructure.

2.4. **Infrastructure Tester**: is one or more designee(s) of the Infrastructure Manager and the Infrastructure Owner whose responsibilities include testing and validation of the performance, security, accessibility, and functionality of the infrastructure.

2.5. **Vendor Infrastructure Manager**: is the vendor representative for a purchased infrastructure, responsible for the infrastructure roadmap, release plan, product patches/updates and features. This may include Commercial off the Shelf (COTS), Platform as a Service (PaaS), subscriptions, Infrastructure as a Service (IaaS) and other vendor managed and maintained technology solutions.

2.6. **Chief Information Security Officer (CISO):** is the State of Maine Chief Information Security Officer or designee.

3.0. Applicability

This policy applies to all State of Maine infrastructure being deployed under the purview of the CIO as defined in Statute.[2] This applies both to new critical infrastructure (prior to installing any asset), as well as significant modifications to existing infrastructure that is hosted or managed by OIT as determined by the IT Director. This policy defines how to certify infrastructure assets which: align with OIT architecture principles, and meet OIT policy requirements, and how to certify them for deployment into production. Please refer to the Change Management Policy[3] for communication protocol.

4.0. Roles and Responsibilities

4.1. IT Directors: Enforce this policy and determine applicability.

4.2. Infrastructure Manager: Is responsible for ensuring appropriate tests are conducted and determining who should perform each test. This certification consists of:

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

[3] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/ChangeManagementPolicy.pdf

4.2.1. The names and signatures of the Infrastructure Manager, Project Manager, IT Director, and Executive Director.

4.2.2. A summary result (Passed/Failed/Not Applicable) and a short paragraph clarifying that summary result, for each of the tests specified below, and the location of the test results.

4.3. Executive Director, Client and Infrastructure Services: Owns and interprets this policy.

4.4. CIO: The CIO may delegate authority to certify or approve new or modified infrastructure for deployment. Regardless of approving authority, certification of infrastructure will be based on advice from the IT Director, Executive Director Client and Infrastructure Services, , Project Management Office (PMO), Project Manager, and/or other subject-matter experts.

4.5. CISO: Is accountable for the security of the infrastructure.

5.0. Directives

5.1. The following list defines the battery of infrastructure tests:

5.1.1. Operating Test: Ensures proper functioning of the infrastructure.

5.1.2. Security Test: Ensures the confidentiality, integrity, and availability of the infrastructure.

5.1.3. Backup and Recovery Tests: Ensures disaster recovery and planned rollback of the infrastructure.

5.2. Naming

5.2.1. Naming conventions must follow standards defined in the Device Naming Standard.[4]

5.3. Testing

5.3.1. Any part of the testing required by this policy may be outsourced to a third-party without affecting the responsibility or the prerogative of the Infrastructure Owners. Irrespective of who executes a test, the Infrastructure Owners remain accountable for its execution. The third-party exclusively conveys the test results directly back to the Infrastructure Owners.

5.3.2. For OIT–hosted infrastructure, the IT Director will designate State personnel who will perform assigned applicable infrastructure tests. The CISO will designate personnel who will perform security tests.

5.3.3. For remote-hosted infrastructure, it is a generally a combination of vetting vendor provided test results and State personnel performing applicable tests. If vendor-provided results for a specific infrastructure test are deemed acceptable by the IT Director and subject-matter experts (Chief Information Security Officer for Security, etc.), no further State personnel testing is required for that item. Should there be deficiencies, then additional testing

[4] http://inet.state.me.us/oit/policies/documents/DeviceNamingStandard.pdf

must be conducted by either the vendor or by State personnel, until acceptable results are achieved.

5.4. Brief general descriptions of the tests are provided below:

5.4.1. **Operating Test**: The infrastructure must operate to the accepted standards and requirements determined by the State of Maine. **Performance of the infrastructure must meet benchmark standards and the expected use for that infrastructure under anticipated conditions.** This test is intended to pre-certify infrastructure environments for usage. Should an application require an environment that is not already pre-certified or have unique infrastructure requirements that have not been previously tested, then additional testing is required.

5.4.2. **Security Test**: The infrastructure must ensure information security standards are met appropriate to the data it contains by:

5.4.2.1. Ensuring ***confidentiality***, preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information;

5.4.2.2. Ensuring ***integrity***, guarding against improper information modification or destruction, including ensuring information non-repudiation and authenticity; and

5.4.2.3. Ensuring ***availability***, ensuring timely and reliable access to and use of information.

5.4.3. Security assurances are maintained through a review of vulnerability scan results, available third-party security reports, network diagrams, and other appropriate documentation (e.g., system security plan) to the satisfaction of the CISO. The CISO will provide further guidance on this item, as needed.

5.4.4. **Backup and Recovery Tests**: Two distinct tests must be performed as part of backup and recovery. The first is to restore the current state, or as close to it as possible, according to the disaster and recovery plans. The second is to roll back the infrastructure to a previous state, according to the disaster and recovery plans to simulate recovery from a disastrous upgrade, a series of flawed transactions, etc.

6.0. Document Information

6.1. Initial Issue Date: March 14, 2011

6.2. Latest Revision Date: March 18, 2022

6.3. Point of Contact: Enterprise.Architect@Maine.Gov

6.4. Approved By: Chief Information Officer, OIT

6.5. Legal Citation: Title 5, Chapter 163: Office of Information Technology[5]

6.6. Waiver Process: Waiver Policy[6]

6.7. Distribution: Internet[7]

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

[6] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/waiver.pdf

[7] https://www.maine.gov/oit/policies-standards