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

Infrastructure Deployment Certification Policy

1.0 Statement

Any computer infrastructure must undergo a battery of tests to determine if it is suitable to be deployed into production. Based on the test results, the Chief Information Officer (CIO) makes the final determination whether or not this infrastructure should be placed into production.

2.0 Purpose

While applications constitute the more visible components of I.T. from the customer perspective, applications cannot exist without a robust infrastructure foundation. A decisive part of the stability, reliability, scalability, security, and performance of an application is dictated by the underlying infrastructure. Therefore, it is extremely important to thoroughly vet any infrastructure before it is deployed into production. This policy establishes a uniform and objective battery of tests that enables the CIO to evaluate the suitability of an infrastructure to be deployed into production. A direct benefit of this policy is that it leads to pre-certified infrastructure that does not need to be vetted any further on a per-application basis.

3.0 Applicability

This policy applies both to new infrastructure (prior to installing any application), as well as modifications to existing infrastructure. Its scope is limited to infrastructure hosted by OIT.

4.0 Responsibilities

4.1 Associate CIO, Infrastructure: This Policy is owned, interpreted, executed, and enforced by the Associate CIO, Infrastructure. The Associate CIO, Infrastructure is responsible for executing this test battery. This certification consists of a summary result (Passed/Failed/Not Applicable) and a short paragraph clarifying that summary result, for each of the tests specified below.

4.2 Chief Information Officer (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 Director, PMO, the Associate CIO, Infrastructure, the Associate CIO, Applications, and/or other subject matter experts.

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 Brief general descriptions of the tests are provided below:

5.2.1 Operating Test: The infrastructure must operate as stated by its vendor, be it the original equipment manufacturer or the value-added reseller. All features listed by the vendor that are relevant to the State should be thoroughly tested in order to ensure that they indeed deliver as expected. For any feature that is relevant to the State, any compliance statement from the vendor is not adequate for this purpose. 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. These items are covered as part of the Operating Platform Test, identified in the *Application Deployment Certification Policy*[1].

5.2.2 Security Test: The infrastructure must ensure the highest levels of Confidentiality (No unauthorized access), Integrity (No tampering), and Availability (No denial-of-service). It must not compromise any data or workflow that either resides on it, or transits through it. It must support encryption, should the data or the workflow that is either in residence or transit merit encryption. A full vulnerability assessment and penetration test must be performed on the infrastructure. At a minimum, such an assessment should include hardened configuration, strong credentials, vetted access control lists, log mining, forensic auditing, integrity checks, and simulated denial-of-service attacks. All hosts, servers, and devices must have currently-supported and hardened operating systems, the latest anti-malware utilities and have the most aggressive intrusion-detection and firewall protection. The Enterprise Security Officer will provide further guidance on this item, as needed.

5.2.3 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, from the backup media in order to simulate recovery from a disaster. The second is to rollback the infrastructure to a previous state from archived media in order to simulate recovery from a disastrous upgrade, a series of flawed transactions, etc.

6.0 Document Information

Initial Issue Date: March 14, 2011
Latest Revision Date: January 11, 2018 – To update Document Information.

Point of Contact: Architecture Policy Administrator, OIT, Enterprise.Architect@Maine.Gov
Approved By: Chief Information Officer, OIT

Legal Citation: Title 5, Chapter 163: Office of Information Technology[2].
Waiver Process: See the Waiver Policy[3].

[1] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/application-deployment-certification_0.pdf
[2] http://legislature.maine.gov/statutes/5/title5ch163sec0.html
[3] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/waiver.pdf