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

Change Management Policy

1.0 Purpose

Information Technology (I.T.) organizations require a process to manage changes to *Information Assets* to assure their highest performance, integrity, and availability.

The purpose of the Change Management Policy is to manage changes to Information Assets in a predictable manner. Adequate planning is necessary to mitigate risk and to minimize the potential adverse impact of a change.

2.0 Definitions

2.1 **Back-Out Plan**: Procedure to undo a change to return the system to the pre-change state.

2.2 **Change Advisory Board (CAB)**: Standing committee of OIT personnel that reviews all Requests For Changes (RFCs) for risk of impact and scheduling conflicts.

2.3 **Change Advisory Board (CAB) Co-Chair**: Co-chairperson of the CAB. Focus is on mitigating risk and minimizing impact of RFCs.

2.4 **Change Implementer**: Primary contact for RFC change execution. This person is most likely, but not always, identical to the Change Initiator.

2.5 **Change Initiator**: The person who submits the change request and provides required RFC documentation.

2.6 **Change Manager**: The OIT Director/Manager (CTS Hosting Manager or App Dev. Director, etc.) that is responsible for the section that includes the Change Implementer.

2.7 **Change Ticket Status**: (RFC Footprints Ticket; Project = OIT Change Management)

- 2.7.1 **Active**: All Change Tickets that are not in 'Closed' status.
- 2.7.2 **Authorized**: Change Ticket that contains all required information and has successfully completed the CAB review.
- 2.7.3 **Cancelled**: Change Ticket is no longer required. Change will not take place.
- 2.7.4 **Closed**: Change Ticket work is complete.
- 2.7.5 **Completed**: Change Ticket completed but not yet 'Closed'.
- 2.7.6 **Delayed**: Change Ticket postponed.
- 2.7.7 **Failed**: Change Ticket has not been successful.
- 2.7.8 **In Progress**: Change Ticket authorized and execution is underway. This category contains long-duration changes.

2.7.9 **Need More Info**: Change Ticket does not contain enough information for authorization. The Change Ticket will be moved to 'Open' status when this information is obtained.
2.7.10 **On Hold**: Change Ticket reviewed but put on hold because the change could not occur as scheduled. When the reason for the hold is resolved, the Change Ticket is will be moved back to 'Open' status.
2.7.11 **Open**: Change Ticket submitted for review.
2.7.12 **Past Implementation**: Change Ticket authorized but is still outstanding and 30 days past the implementation date. If no response from the Change Initiator in seven (7) days, then the Change Ticket is 'Closed'.
2.7.13 **Recurring**: Change Ticket scheduled for periodic (usually monthly) execution.
2.7.14 **Rejected**: Change Ticket not authorized to proceed.
2.7.15 **Request**: Automatic Footprints default. Not used.
2.7.16 **Under Review**: Change Ticket needs a higher level or special authorization, also could be in an After-Action Review.

2.8 **FootPrints**: BMC-Numera application used by OIT for response tracking.

2.9 **Information Assets**: Business applications, system software, development tools, utilities, hardware, infrastructure, etc.

2.10 **Production I.T. Changes**: Any modification made to an OIT Production environment.

2.11 **Request for Change (RFC)**: This is the change lifecycle managed within the OIT Change Management Project of the Footprints application.

2.12 **Stakeholder**: Any group potentially impacted by the change. This could be a business partner, hosting partner, OIT organizational unit, etc.

3.0 Applicability

This Policy establishes directives intended to manage change to Information Assets that potentially could affect *Stakeholder* operations. This Policy applies to all *Production I.T. Changes*.

4.0 Responsibilities

4.1 *Change Advisory Board (CAB)* is responsible for reviewing all changes for risk of impact and scheduling conflicts.

4.2 *Change Advisory Board (CAB) Co-Chair* is responsible for reviewing, monitoring, and authorizing changes. The CAB Co-Chairs are collectively responsible for enforcing this Policy.

4.3 *Change Implementer* is responsible for executing the change according to the approved plan.

4.4 *Change Initiator* is responsible for requesting a change, initiating an impact analysis for the change, and explicitly identifying the parties impacted by the change. The Change Initiator must also ensure that impacted parties are aware of and approve the change. Unless the

Stakeholders requested the change, any change request requires, at a minimum, a two-week notice to the impacted Stakeholders. They may leverage the TBCs or Application Development (App Dev) staff for Agency notification, yet the Change Initiator is ultimately responsible. If Core Technology Services (CTS) resources are required to help implement the change, the Change Initiator must arrange with CTS. If any of these items are not fulfilled the change request will not be considered for authorization.

4.5 *Change Manager* (or designee) is responsible for managing the change process, responding to emergency changes or unforeseen/unexpected changes, and communicating all changes.

4.6 Change Validator is responsible for testing change post-implementation to ensure that the change achieved the intended results and/or did not introduce any new faults.

5.0 Directives

5.1 The Change Initiator must submit any non-emergency *Request for Change (RFC)* via the Change Management *Footprints* Project, no later than noontime on the Wednesday immediately prior to the CAB meeting (Thursdays at 10:00am). In addition to the other required RFC elements, the Change Initiator will include in the RFC all actions (steps) germane to the requested change and the *Back-Out Plan*. The Change Initiator or their representative must also participate in the CAB meeting to answer any questions.

5.2 The following must be included in the initial description, or as an added comment:

- 5.2.1 All Stakeholders have been provided, at a minimum, a two-week notice (unless they are the group who requested the change and they are the only ones impacted by it) and approve of this RFC.
- 5.2.2 Specification of whether additional resources (CTS, App Dev., etc.) are required.
- 5.2.3 Confirmation that coordination with additional required resources has occurred and that all required parties have affixed their confirmation to the Change Ticket.
- 5.2.4 If any of the above items are not in place prior to the Thursday CAB meeting, the RFC will not be considered.

5.3 Recurring RFCs must have their *Change Ticket Status* set back to 'Open' or 'On Hold' after implementation. Each occurrence needs to be authorized by the CAB (deadlines for submission are the same as are listed in Directive 5.1).

5.4 The CAB reviews all RFC tickets (time permitting) with an 'Open' status. The CAB also reviews 'Delayed' and 'On Hold' RFC tickets, (time permitting).

5.5 Emergency RFCs are for extenuating circumstances only. In addition to the other required RFC information, the Change Initiator must also set RFC priority to Emergency and identify why they need change authorization prior to the next CAB meeting and what the risk is if the change does not take place at the requested time. The Change Initiator must follow-up with the CAB Co-Chairs to obtain authorization prior to change implementation.

5.6 The Change Implementer must follow the RFC steps meticulously.

5.7 Should it be revealed during execution that the actual execution deviates from the RFC

steps, or that the risk was underestimated, then the Change Implementer stops the execution and notifies the Change Manager, who determines appropriate action.

5.8 Should the Change Manager determine that a tested and proven remediation effort can safely resolve the issue; the Change Manager communicates the anticipated impact/duration to Stakeholder representatives and the RFC remains in 'In Progress' status until remediation is performed.

5.9 Should the Change Manager determine to back-out the change, the Change Implementer executes the Back-Out Plan. The Change Manager (or designee) communicates with the CAB and Stakeholder representatives, per the Back-Out Plan, documents the deviation, and updates the RFC, so that the Change Implementer can dedicate their focus on backing-out the change.

5.10 Should the change cause an unforeseen/unexpected outcome, and the Back-Out Plan fails, then the Major Incident Procedure[1] applies. Immediate notification must take place to Stakeholder representatives, the Help Desk, and the CAB.

6.0 Document Information

Initial Issue Date: October 24, 2007
Latest Revision Date: March 20, 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] http://www.maine.gov/oit/policies/MajorIncidentProcedure.pdf
[2] http://legislature.maine.gov/statutes/5/title5ch163sec0.html
[3] http://www.maine.gov/oit/policies/waiver.pdf