State of Maine

Department of Administrative and Financial Services

Office of Information Technology

Change Management Policy and Procedures (ChM)

Change Management Policy and Procedures (ChM)

Table of Contents

Change Management Policy and Procedures (ChM)

1.0. Document Purpose

The purpose of this document is to define the State of Maine policy and procedures that are in place for Change Management (ChM) for State of Maine information assets (see Definitions). This part of the security program is focused on protecting the confidentiality (see Definitions), integrity (see Definitions), and availability (see Definitions) of State information assets through consistent and effective change management processes. This document corresponds to the Configuration Management (CM) Control Family of National Institute of Standards and Technology (NIST) Special Publication 800-53 (Rev. 5).[1]

2.0. Scope

2.1. This policy applies to State of Maine employees and contractors (collectively referred to as personnel in this document) with access to:

2.1.1. Executive Branch Agency information assets, irrespective of location; and

2.1.2. Information assets from other State government branches that use Executive Branch-managed services.

2.2. All IT infrastructure and production environments, excluding exempted changes.

3.0. Policy Conflict

If this policy conflicts with any law or union contract in effect, the terms of the existing law or contract prevail.

4.0. Roles and Responsibilities

4.1. The Chief Information Officer (CIO):

4.1.1. Ultimate approval of the Office of Information Technology's (OIT's) ChM policies and procedures.

4.1.2. Appoint two members of OIT senior management with expertise in change management to serve as Change Advisory Board (CAB) Co-Chairs.

4.2. The Division Directors:

4.2.1. Appoint two individuals, one member and one alternate, from each division with expertise in their respective technology areas to serve on the CAB.

4.3. The CAB Co-Chairs**:**

4.3.1. Ensure the CAB adheres to ChM procedures and is robustly staffed with sufficient IT and stakeholder representatives;

[1] https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

4.3.2. Determine the schedule for CAB members to serve as CAB Facilitators on a rotating basis;

4.3.3. Approve Standard Change Classification Template requests for use in the Standard Change Catalog in the Enterprise Ticketing System;

4.3.4. Review the Standard Change Catalog in the Enterprise Ticketing System on an annual basis, or earlier as required, to ensure they remain current and valid;

4.3.5. Select emergency Change Advisory Board (E-CAB) members to serve on an ad hoc basis on the E-CAB, as the nature of the emergency requires;

4.3.6. Respond to Emergency Requests for Changes (E-RFCs) by standing up the E-CAB to conduct an accelerated ChM process; and

4.3.7. Provide conflict resolution as required at CAB meetings and, in the event the CAB is unable to reach a decision on a Request for Change (RFC), escalating the issue to the CIO; and

4.3.8. Appoint a designee to act on their behalf, as necessary, with any further designation requiring approval from the CIO.[2]

4.4. The CAB Members:

4.4.1. Authorize changes throughout the development and operational lifecycle of products and systems after ensuring the changes are held to approved criteria before implementation;

4.4.2. Ensure that changes are processed in an orderly and consistent manner;

4.4.3. Provide cross-functional visibility to RFCs that leverage the collective understanding of the impact across the organization;

4.4.4. Oversee how proposed changes could affect the functionality and secure state of the information system based upon the Configuration Item (CI)'s assessment; and

4.4.5. Provide support for the Major Incident Procedure plan[3], when applicable, as directed by the CAB Co-Chairs, if the back-out plan fails.

4.5. The CAB Facilitator:

4.5.1. Lead the CAB meetings on a predetermined rotating basis, as determined by the CAB Co-Chairs;

4.5.2. Prepare the CAB meeting agenda for distribution to CAB members, including the open RFCs that have been submitted and have met the CAB submission deadline;

[2] The CAB Co-Chairs are responsible for the actions taken by a designee on their behalf within the scope of this policy.

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

4.5.3. Prioritize open RFCs on the agenda for the CAB meeting based on the security impact level identified from the Security Impact Analysis[4] (SIA) (Appendix C);

4.5.4. Serve as a ChM gatekeeper by reviewing RFCs for completeness, appropriate approvals, and compliance with ChM procedure; and

4.5.5. Ensure that the Standard Change dashboard in the Enterprise Ticketing System is updated weekly and reviewed by CAB members before the weekly CAB meeting.

4.6. The CAB Emergency Committee (E-CAB) members:

4.6.1. Serve on an ad hoc basis at the request of the CAB Co-Chairs in response to emergency RFCs (E-RFCs);

4.6.2. Provide subject matter expertise to the CAB Co-Chairs as required to assist with performing the SIA of an E-RFCs (Appendix C); and

4.6.3. Assist with the Post Implementation Review of any authorized E-RFCs.

4.7. The Change Requestors (CR):

4.7.1. Own the RFC from creation to closure, which includes:

4.7.1.1. Generating and submitting the RFC to start the process;

4.7.1.2. Providing details that must be included in the RFC (see Appendix D); and

4.7.1.3. If necessary, assign the RFC to a Change Owner (CO) in the Enterprise Ticketing System who is better equipped to manage the requirements of the RFC and takes over responsibility for the RFC from implementation to validation post-CAB.

4.7.2. Attend the CAB as necessary to assist the CAB with deliberation on the RFC; and

4.7.3. Shepherd the authorized RFC through implementation and validation post-CAB.

4.8. Change Owners (CO) are responsible for:

4.8.1. Once assigned by a CR in the Enterprise Ticketing System, assuming all the CR's responsibilities with respect to owning the RFC from creation to closure, including:

4.8.1.1. Completion of all required information for the RFC in the Enterprise Ticketing System necessary to meet the CAB submission deadline (see Appendix D);

4 Security Impact Analysis satisfies the NIST configuration management family of controls (CM-4).

4.8.1.2. Attend the CAB as necessary to assist the CAB with deliberation on the RFC; and

4.8.1.3. Shepherd the authorized RFC through implementation and validation post-CAB.

5.0. Management Commitment

The State of Maine is committed to following this policy and the procedures that support it.

6.0. Coordination Among Agency Entities

Please refer to the Configuration Management Policy and Procedures[5] document.

7.0. Compliance

7.1. For State of Maine employees, failure to comply with this document may result in progressive discipline, up to and including dismissal.

7.2. For State of Maine contractors and non-State of Maine personnel, failure to comply may result in the removal of the individual's ability to access and use State of Maine data and systems. Employers of contractors will be notified of any violations.

7.3. Personnel are also subject to any applicable penalties for statutory requirements compliance violations. Depending on the requirement and the nature of the violation, penalties could include fines and/or criminal charges.

8.0. Procedures

The following standards apply to and represent the security controls established to ensure an acceptable level of protection for the State of Maine's information assets through secure change management processes, which ensure that the appropriate steps are taken prior to implementing a change request.

8.1. Initiate the RFC (Pre-CAB):

8.1.1. Access and record keeping requirements (CM-5):

8.1.1.1. All documentation associated with ChM is maintained in the Enterprise Ticketing System.

8.1.1.2. Unless the CR assigns the request to a different "assigned to" individual (see Change Owner), the CR must provide all of the required documentation within the Enterprise Ticketing System for an RFC to be considered complete (see Appendix D for required information for the RFC in the Enterprise Ticketing System); and

8.1.1.3. The CR may only initiate RFCs on those components of the information system for which they are qualified and

[5] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/ConfigurationManagementPolicy.pdf

authorized to access for purposes of initiating such changes, including upgrades and modifications.

8.1.2. **Types of RFCs (CM-3)**:

8.1.2.1. There are four types of RFCs (described in Table 1):

Table 1: Types of RFCs

Change Type	Description
Standard Change	A Standard Change is created from preapproved Standard change templates that have satisfied specific criteria (see Appendix A) and been added to the Standard Change Template Catalog in the Enterprise Ticketing System: the change is repeatable, frequently implemented, is considered low risk and low impact according to the SIA, and has a proven history of success (completed the Normal change lifecycle process at least 3-5 times with no issues). Standard changes that are approved by Division Directors and CAB Co-Chairs are added to the catalog and considered pre-authorized, following a shorter ChM lifecycle outside of the CAB approval process (subject to dual authorization). CRs can request new Standard change templates or use an existing template from the catalog to create a new Standard change request.
Normal Change	A Normal Change is one that meets the defined lead time for testing and validation and is assigned an SIA level of no, low, medium, or high. A Normal Change is an RFC that is not a Standard, Expedited, or Emergency change and is subject to the full ChM review process, including review and authorization by the CAB.
Expedited Change	An Expedited Change does not meet the lead time requirement for a Normal change, but is not an Emergency Change. Service is at risk, although the service might not be down, and the RFC should be authorized due to a client request that has been validated by a Subject Matter Expert (SME)/technical expert or a Director, who has determined that the change needs to be implemented without waiting for the recommended lead time. The same Normal Change request information is provided in the Enterprise Ticketing System to implement the change, including the reason for expediting the RFC (SIA, back-out plans, scheduled time, and downtime required). However, lead times are significantly shorter. Authorization by a CAB Co-Chair is required, and Expedited Changes are subject to retroactive review by CAB.

Change Type	Description
Emergency Change	An Emergency Change is one that must be implemented as soon as possible to correct or prevent a high-priority incident, or that must be introduced as soon as possible due to likely negative service impacts or situations where the impact to a service is imminent if action is not taken. These changes do not follow the complete lifecycle of a Normal Change due to the speed with which they must be implemented and authorized. All emergency changes are authorized by E-CAB and documented and entered into the Enterprise Ticketing System prior to implementation, or as soon as possible after the change has been implemented, depending on the nature of the emergency. Emergency changes are subject to a Post-Implementation Review (PIR) process by CAB.

8.1.3. **Standard RFCs (CM-3(2))**:

8.1.3.1. CRs can either choose from an existing Standard Change template in the Enterprise Ticketing System catalog or propose a new template for a Standard Change (see process described in Appendix B).

8.1.3.2. To create a new Standard Change RFC from an existing template, select the appropriate match from the list of approved Standard Changes listed in the Standard Change Catalog in the Enterprise Ticketing System.

8.1.3.3. Once the type of Standard Change is selected, the CR's Division Director, or Director's Designee, must sign off on the designation of the RFC as a Standard Change in the Enterprise Ticketing System to provide verification that the RFC is a match and properly categorized Standard Change.

8.1.3.4. Once a Standard Change RFC has been selected within the Enterprise Ticketing System and signed off on by the Division Director, it is considered pre-authorized and will be automatically included on a Standard Change Dashboard for CAB members to view on a rolling basis.

8.1.3.5. If an objection to the Standard Change is raised with the CAB Facilitator and/or CAB Co-Chairs, the Standard Change will be removed from the preauthorized list and added to the CAB agenda for discussion and approval at CAB.

8.1.3.6. If no objection is raised, the Standard Change is reviewed to be correct and authorized by the CAB Facilitator in advance of the CAB meeting.

8.1.3.7. The CAB Facilitator authorizes Standard Changes on a weekly basis preceding CAB.

8.1.3.8. All Standard Changes are tracked in the Enterprise Ticketing System and must follow implementation and validation procedures identified below (section 9.4).

8.1.4. **Normal Change RFCs (CM-4)**:

8.1.4.1. Unless the RFC is assigned to another individual (see Change Owner), the CR is the owner of the RFC from creation to closure.

8.1.4.2. The CR inputs the required Normal Change Request information in the Enterprise Ticketing System (for Required Information, see Appendix D). The CR enters the business needs, goals, and objectives of the change and ensures they are accurate, and provides supporting documentation for the change (i.e., install, test, and back-out plans).

8.1.4.3. The CR completes the SIA and consults with the Information Team for those RFCs with an impact level of moderate or high. In some cases, the CR will still need to discuss the RFC even though it has an impact level of low. Please send an email to the IT Security Team group (security.infrastructure@maine.gov).

8.1.4.4. The CR provides CAB representation when necessary.

8.1.4.5. CAB approval is required before implementation.

8.1.5. **Expedited Change RFCs (CM-3(4)):**

8.1.5.1. The CR follows the same process and approval flow as a Normal Change RFC, but lead times are shorter. Expedited Change RFCs must demonstrate that service is at risk, although service might not be down, and the RFC should be authorized because of a client request that has been validated by an SME/technical expert or a Director, who has determined that the change needs to go in without waiting for the recommended lead-time.

8.1.5.2. The same Normal Change request information is provided in the Enterprise Ticketing System to implement the change, including the reason for expediting the RFC (SIA, back-out plans, scheduled time, and downtime required).

8.1.5.3. It is the responsibility of the CR or CO to shepherd the Expedited change through the approval process.

8.1.5.4. All Expedited RFCs must be preauthorized by the CAB Co-Chairs. Retroactive CAB approval is required.

8.1.6. **Emergency Change RFCs (E-RFCs) (CM-4(2))**:

8.1.6.1. E-RFCs do not follow the complete lifecycle of a Normal change due to the speed with which they must be implemented. E-RFCs must meet the criteria that they are necessary to correct, or reduce the likelihood of a high-priority incident, or likely negative service impacts/situations where the impact to a service is imminent if action is not taken.

8.1.6.2. E-RFCs are authorized by E-CAB and documented and entered into the Enterprise Ticketing System prior to implementation, or as soon as possible after the change has been implemented, depending on the nature of the emergency.

8.1.6.3. The E-RFC is discussed at the earliest CAB meeting and is subject to a Post Implementation Review (PIR).

8.1.7. **Notice Requirement (CM-3)**:

8.1.7.1. All Normal Change RFCs require a minimum of two weeks' notice to impacted stakeholders, unless the stakeholders have agreed to waive this requirement.

8.1.8. **Deadline for CAB; Lead time (CM-3)**:

8.1.8.1. All Normal RFCs must be submitted via the Enterprise Ticketing System and be fully complete no later than noontime on Wednesday for consideration at the CAB meeting to be reviewed by the CAB that week, subject to the following lead times:

8.1.8.1.1. Normal RFCs with an SIA impact level of No to Low must provide at least one week of advanced notice to CAB, depending on the urgency of the RFC.

8.1.8.1.2. Normal RFCs with an SIA impact level of Moderate to High must provide at least 3 weeks' advanced notice to the CAB, with the amount of lead time dependent upon the complexity of the RFC.

8.1.9. **Cloud Assets (CM-9) -** For Cloud Assets, based upon an evaluation of the business criticality, Cybersecurity risk assessment, etc., the OIT Service Vertical Director will make a determination and will direct the creation of Informational Standard RFCs for major lifecycle milestones of said Cloud Asset.

8.2. CAB Agenda - Prioritized Based on RFC Type (Preparation for CAB):

8.2.1. **CAB Agenda Preparation (CM-3) -** The CAB Facilitator prepares the weekly CAB agenda for distribution to CAB members, including all RFCs that are open and complete and have met the RFC CAB submission and lead time requirements;

8.2.2. **Prioritization by Impact and Post-Implementation Review (CM-4(2)) -** The CAB facilitator prioritizes RFCs on the CAB agenda based on the RFC's SIA impact level (no, low, moderate, high) as listed in the Enterprise Ticketing System. Any emergency RFCs that were authorized by the E-CAB during the previous week, as well as any unsuccessful or failed RFCs, are added to the agenda for PIR.

8.2.3. **High-Impact RFC Coordination (CM-4) -** The CAB Facilitator communicates with the CAB Co-Chairs, Chief Information Security Officer (CISO), and information security team representatives to review any RFCs with an SIA impact level of High to review the timeline and implementation steps necessary prior to CAB.

8.3. Assessment and Evaluation of the RFC (in CAB):

8.3.1. **CAB Recordkeeping (CM-5) -** During CAB, the CAB Facilitator adds his/her name to the RFC documentation in the change record (for all RFCs during their leadership term).

8.3.2. **CAB Meeting Conduct (CM-3) -** The CAB meeting is conducted in accordance with the CAB agenda.

8.3.3. CAB Members:

8.3.3.1. **Assessment, Prioritization, and Scheduling (CM-3) -** Advise on the assessment, prioritization, and scheduling of RFCs, authorizing their release.

8.3.3.2. **Testing and Evaluation (CM-3(2) -** Ensure the CR has adhered to OIT policy and RFCs are sufficiently tested and evaluated to determine the impact on system security before implementation to ensure the lowest possible risk to services.

8.3.3.3. **Security Impact Assessment (CM-4) -** Use the SIA as the framework for the evaluation of the RFC, which allows for the assessment of the potential impact of changes to the information system in a repeatable manner that ensures a balance of security, business, and technical viewpoints.

8.3.3.4. **Authorization Decisions (CM-3(4)) -** Determine by consensus to authorize, defer, or reject the RFC.

8.3.3.5. **Post-Implementation Review (CM-4(2)) -** Perform any necessary PIRs on expedited or emergency RFCs authorized

during the previous week, as well as any unsuccessful or failed RFCs.

8.3.4. **Prohibition of Unauthorized Changes (CM-5) -** Unapproved changes to OIT-managed information systems are prohibited.

8.4. Implementation and Validation of the RFC (Post-CAB):

8.4.1. **Implementation Verification (CM-4(2)) -** The CR (or CO) implements the RFC and verifies that approved changes are implemented correctly, operating as intended, and meeting security requirements.

8.4.2. **Update of Configuration and Documentation (CM-6) -** The CR includes changes to applicable/related configuration parameters as well as updates system documentation to reflect the changes.

8.4.3. **Closure of Successful RFCs (CM-3) -** For successful RFCs:

8.4.3.1. The CR confirms the change was deployed without issues and closes out the change request.

8.4.4. **Handling Failed RFCs and PIR (CM-4(2)) -** For failed RFCs:

8.4.4.1. In the event the RFC is unsuccessful, fails, or is partially implemented and cannot be completed, the change may need to be backed out. In this case, the approved Backout Plan is implemented.

8.4.4.2. A PIR is conducted at the direction of the CAB Co-Chairs to determine how the change was handled throughout its lifecycle and identify opportunities to improve implementation of similar RFCs in the future.

8.4.5. **Biannual CAB Audit (CM-3) -** The CAB audits and reviews activities related to changes to the information system at least biannually.

9.0. Document Details

9.1. Initial Issue Date: July 18, 2019

9.2. Latest Revision Date: January 27, 2026

9.3. Point of Contact: PolicyTeam.OIT@Maine.Gov

9.4. Approved By: Chief Information Officer, OIT

9.5. Legal Citation: Title 5, Chapter 163: Office of Information Technology[6]

9.6. Waiver Process: Waiver Policy[7]

9.7. Distribution: Internet[8]

---

[6] https://legislature.maine.gov/statutes/5/title5ch163sec0.html
[7] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/waiver.pdf
[8] https://www.maine.gov/oit/policies-standards

10.0. Review

This document will be reviewed triennially, and when substantive changes are made to Policies, Procedures, or other authoritative regulations affecting this document.

11.0. Records Management

OIT security policies, plans, and procedures fall under the *Major Administrative Policies and Procedures* and *Internal Control Policies and Directives* records management categories. They will be retained for a minimum of six years after withdrawal or replacement and then destroyed in accordance with guidance[9] provided by Maine State Archives. Retention of these documents will be subject to any future State Archives General Schedule revisions that cover these categories.

12.0. Public Records Exceptions

Under the Maine Freedom of Access Act (FOAA),[10] certain public records exceptions may limit disclosure of agency records related to information technology infrastructure and systems, as well as security plans, procedures, or risk assessments. Information contained in these records may be disclosed to the Maine State Legislature or, in the case of a political or administrative subdivision, to municipal officials or board members under conditions that protect the information from further disclosure. Any aggrieved person seeking relief for an alleged violation of the FOAA may bring suit in any Superior Court in the State.

13.0. Definitions

13.1. Backout Plan*:* A plan that is used in the event a change moved into production causes unwanted results and the system must be returned to a previous functional version to restore business operations.

13.2. Change Advisory Board*:* The CAB is comprised of representatives from all areas of OIT, who are considered standing, regular members of the CAB, as well as other individuals who may participate on an ad hoc basis, depending on the nature of the RFC being reviewed: CAB Co-Chairs; CAB Leaders; User managers and groups; Applications representatives; Information security representative; and Technical experts.

13.3. Change Calendar: A centralized schedule maintained by the CAB to track all approved and pending changes across systems and services, used to prevent scheduling conflicts.

13.4. Change Management Lifecycle: The end-to-end process of proposing, evaluating, authorizing, implementing, validating, and closing out a Request for Change (RFC).

13.5. Change Management*:* The process that controls the lifecycle of all changes to the infrastructure or any aspect of services in a controlled manner, enabling beneficial

[9] https://www.maine.gov/sos/sites/maine.gov.sos/files/content/assets/GS1Administrative.pdf
[10] https://legislature.maine.gov/statutes/1/title1sec402.html

changes to be made with minimum disruption to IT services. It applies to any change that might affect OIT systems, infrastructure, and services in the IT environment, including changes to all architectures, applications, software, tools, and documentation.

13.6. Change Owner: For any RFC assigned, this role is deemed the owner of the RFC from creation to closure. The CO is assigned to this role by the CR and is responsible for owning the change request from creation to closure.

13.7. Change Requestor: The CR is the individual who creates the RFC in the Enterprise Ticketing System. Unless the CR assigns the RFC to a different "assigned to" individual (see Change Owner), the CR owns the change request from creation to closure. The CR must complete all the required information in the Enterprise Ticketing System for Normal RFCs (Appendix D).

13.8. Change Window: A pre-established time period during which approved changes may be implemented to minimize operational disruption.

13.9. Configuration Item (CI): A discrete component of an information system (such as hardware, software, documentation, or process) that is subject to configuration management. Each configuration item is uniquely identified, tracked, and managed throughout its lifecycle to maintain system integrity, accountability, and change traceability.

13.10. Emergency Change Advisory Board (E-CAB): A group dynamically convened at the call of the CAB Co-Chairs, on an ad hoc basis, to reduce the likelihood of service interruption or restore service during an outage, as the nature of the emergency requires. Individuals who may be called to serve on the E-CAB include subject matter experts, information security representatives, team leaders, and others within OIT with relevant ChM expertise.

13.11. Emergency Change: A request for Change that must be implemented as soon as possible to correct, or prevent, a high-priority incident, or that must be introduced as soon as possible due to likely negative service impacts.

13.12. Enterprise Ticketing System (ETS): The system used by OIT to log, track, approve, and document Requests for Change and related artifacts throughout the change lifecycle.

13.13. Exempt Change: Certain changes that are not included under ChM policy, as identified by the CAB Co-Chairs, include: database content updates, creating/removing/updating accounts, and creation or deletion of user files are examples of exempt changes.

13.14. Post Implementation Review (PIR): A formal review conducted after a change is implemented to verify outcomes, identify lessons learned, and determine process improvements.

13.15. Request for Change: A formal request for a change to any component of an IT infrastructure or to any aspect of an IT service that is made to the OIT production

environment. The formal change request is logged into OIT's Enterprise Ticketing System, which includes all the information required in Appendix D.

13.16. Security Impact Analysis: The SIA is based on three security categories for both information and information systems based on methods described in Federal Information Processing Standards (FIPS) Publication 199, "*Standards for Security Categorization of Federal Information and Information Systems,*" and NIST Special Publication 800-53, "*Security and Privacy Controls for Federal Information Systems and Organizations*." The categories are based on the potential impact on an agency should certain events occur that jeopardize the information/information systems necessary to accomplish its mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. The SIA is conducted to determine the extent to which changes to the information system will affect the security state of the system.

13.17. Standard Change Catalog*:* The collection of pre-approved Standard Changes that have been authorized by the CAB Co-Chairs and are subject to a streamlined ChM process outside of CAB.

13.18. Standard Change Dashboard: A live reporting interface within the Enterprise Ticketing System used to track preapproved Standard Changes and their implementation status.

13.19. Standard Change Template: An approved form for submission of requests for routinely and frequently performed, low-impact/risk RFCs determined to be Standard Changes by the CAB Co-Chairs and subject to a streamlined process outside of the CAB.

13.20. Waiver Policy: The enterprise policy governing requests to temporarily deviate from an established OIT policy, procedure, or control, subject to formal approval and documented justification.

14.0. Abbreviations

14.1.	CAB	Change Advisory Board
14.2.	ChM	Change Management
14.3.	CI	Configuration Item
14.4.	CIO	Chief Information Officer
14.5.	CO	Change Owner
14.6.	CR	Change Requestor
14.7.	E-CAB	Emergency Change Advisory Board
14.8.	ETS	Enterprise Ticketing System
14.9.	E-RFC	Emergency Request for Change
14.10.	FOAA	Maine Freedom of Access Act
14.11.	NIST	National Institute of Standards and Technology

14.12.	OIT	Office of Information Technology
14.13.	PIR	Post Implementation Review
14.14.	RFC	Request for Change
14.15.	SIA	Security Impact Analysis
14.16.	SLA	Service Level Agreement
14.17.	SME	Subject Matter Expert

Appendix A: Standard Change Classification Template

Standard Change Classification Template

Name of Proposed Standard Change Classification (Type):	**Date Requested:**
Requested by (Section Manager and above):	**Reviewed by (Division Director or Director's Designee):**
Questions	**Response**
Provide a brief description of the change and identify why it should be categorized as a Standard Change for inclusion in the Standard Change catalog.	
Does this type of change satisfy the criteria for Standard Changes identified in the Checklist?	YES _____ NO _____
How frequently is this type of change made?	
Are there documented procedures describing the steps necessary to complete the change?	YES _____ NO _____
Is there a viable back-out procedure that can be documented in the RFC?	YES _____ NO _____
Is the change considered low risk/ impact to the OIT production environment, security, services, infrastructure, customers/users, and business processes?	YES _____ NO _____
Has this type of change ever failed before? If so, what happened? Did you have to back it out?	

Approved YES _____ NO _____ CAB Co-Chairs' Signatures: _____ / _____

Date of decision: _____

Standard Change Checklist

A Standard Change is considered a subset of Normal Change RFCs (low risk, low impact) that also:

1. Has a proven history of success and predictable outcomes;

2. Is scriptable (step-by-step work procedures), frequently implemented, and subject to successfully repeatable implementation steps;
3. Has been proven to be a low-risk and low-impact change to the OIT production environment, security, services, infrastructure, customers/users, and business processes;
4. Has documented build procedures;
5. Install plan (time to install, steps required) is documented;
6. Applicable customer, user, and internal notifications/communications are built into the workflow;
7. Procedural documentation for execution of each Standard Change request is maintained; and
8. Back-out or Recover procedure is documented and tested.

Appendix B: Standard Change Classification Process and Checklist

Maine Office of Information Technology

Standard Change Classification Process and Checklist

This document outlines the process and checklist for classifying standard changes, to be used in accordance with the standards outlined in the Change Management Policy and Procedures document.

Standard Change Classification Process

1.0 Standard Change Classification Process

This document describes the process for classifying changes that qualify as Standard changes within the change management process.

1.1 A Standard change is defined as a repeatable change that has been pre-authorized by the CAB Co-Chairs by means of a documented procedure that controls risk and has predictable outcomes. Standard changes are considered pre-approved and follow a shorter lifecycle, omitting the CAB authorization steps.

1.1.1 Any request to have an RFC classified and preauthorized as a Standard change template must be submitted using the OIT Standard Change Classification Template (Appendix A) and approved by the respective Division Director[11]. All requests must be finally approved by the CAB Co-Chairs.

1.1.2 All submissions must meet the Checklist requirements in section 2 to the satisfaction and approval of the CAB Co-Chairs.

1.1.3 Once a change is pre-authorized as a Standard Change by the CAB Co-chairs, they are stored in a catalog of templates. Change requestors will be able to select from the existing Standard change catalog the appropriate option that matches their standard change RFC. The selection must be signed off on by a separate individual, the Division Director or Director's designee, and that individual is listed in the Enterprise Ticketing System.

1.1.4 All Standard change RFCs are tracked in the Enterprise Ticketing System and controlled by a pre-approved standardized process that occurs outside of the CAB.

[11] Individuals authorized to submit requests to the CAB Co-Chairs for classification of Standard changes include: Division Directors, or the Division Director's designee (typically the Deputy Division Directors). The completion of the Standard Change List Submission Template (Appendix B) may only be completed by Section Managers and above. To ensure separation of duties, the Submission Template must be reviewed by a different individual than the one who requested the submission.

2.0 Standard Change: Classification Checklist

2.1 The following checklist must be used for submission of any RFC for classification as a Standard change template by the CAB Co-Chairs and entrance into the Standard change catalog.

2.1.1 The change is a subset of a Normal RFC (low risk, low impact) that is:

2.1.1.1 Frequently implemented;

2.1.1.2 Subject to successfully repeatable implementation steps and standard documented procedure;

2.1.1.3 Has a proven history of success and predictable outcomes;

2.1.1.4 Considered a low-risk and low-impact change to the OIT production environment, security, services, infrastructure, customers/users, and business processes; and

2.1.1.5 Notification of impacted parties is built into the workflow.

3.0 Standard Change Catalog List; Annual Review

3.1 Standard change catalog; annual review

3.1.1 The standard change catalog must be reviewed annually, or earlier if required, by the CAB Co-Chairs to ensure it remains valid.

Appendix C: Security Impact Analysis

Maine Office of Information Technology

Security Impact Analysis

This document establishes the Security Impact Analysis to be used in accordance with the standards set forth in the Change Management Policy and Procedures document.

Security Impact Analysis (SIA)

Table 2: Security Impact Analysis

	Potential Impact			
Security Objective	**No**	**Low**	**Moderate**	**High**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	No adverse effect	The unauthorized disclosure of information is likely to have a limited adverse impact on organizational operations, assets, or individuals.	The unauthorized disclosure of information is likely to have a serious adverse impact on organizational operations, assets, or individuals.	The unauthorized disclosure of information is likely to have a severe or catastrophic adverse impact on organizational operations, assets, or individuals.
Integrity Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	No adverse effect	The unauthorized modification or destruction of information is likely to have a limited adverse impact on organizational operations, assets, or individuals.	Unauthorized modification or destruction of information is likely to have a serious adverse impact on an organization's operations, assets, or individuals.	Unauthorized modification or destruction of information is likely to have a severe or catastrophic impact on an organization's operations, assets, or personnel.

Level of CAB Review

	Potential Impact			
Security Objective	**No**	**Low**	**Moderate**	**High**
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	No adverse effect	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

The SIA establishes security categories for information systems described in FIPS Publication 199[12]. It provides the framework for determining an appropriate set of security controls within the ChM process required to protect information and information systems. The security categories are based on the potential impact on an agency should certain events occur that jeopardize the information and information systems required by OIT to accomplish its mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an agency. System information must be protected at a level commensurate with the most critical or sensitive user information being processed by the system, ensuring confidentiality, integrity, and availability.

The application of the SIA must take place within the context of OIT's organization and the overall State interest, and is provided as guidance ONLY:

The *potential impact* is **NO Impact** if —

– When the unauthorized disclosure of information, the unauthorized modification or destruction of information, or the disruption of access to or use of information or an information system could be expected to have a ***very limited or no*** adverse effect on organizational operations, organizational assets, or individuals that may, for example (i) little or no degradation in mission capability or effectiveness; (ii) result in little or no damage to organizational assets; (iii) result in very minor or no financial loss; or (iv) result in no harm to individuals greater than the potential for inconvenience caused by, for example, missing or misrepresented information.

Applying the Standard: For example, NO impact systems may not store, communicate, or process any Privacy Act or confidential information.

The potential impact is **LOW** if —

– The loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.

Clarification: A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

Applying the Standard: For example, **LOW** impact systems store data that is open to public inspection or readily available through public sources. LOW impact systems may not store, communicate, or process any Privacy Act or confidential information.

[12] (http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf)

The *potential impact* is **MODERATE** if —

– The loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.

Clarification: A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the agency is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to agency assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

Applying the Standard: Is the information system affected primarily and routinely used to store, communicate, or process any of the following types of information: Collections and Receivables; Contingency Planning; Continuity of Operations; Cost Accounting/Performance Measurement; Energy Resource Management; Energy Supply; Environmental Remediation; Information Management; Information Security; Lifecycle/Change Management; Payments; Percentage Infrastructure Maintenance; Reporting Information; Research and Development; Scientific and Technical Research and Innovation; Security Management; System and Network Monitoring; System Development; System Maintenance.

- *Does aggregation of information on this system reveal sensitive patterns and plans, or facilitate access to sensitive or critical systems?*
- *Would unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) adversely affect operations or seriously damage mission function and/or public confidence?*
- *Would either physical or logical destruction of the system result in very large expenditures to restore the system and/or require a long period of time for recovery?*
- *Does the mission served by the system, or the information that the system processes, affect the security of critical infrastructures and key resources?*
- *Does the system store, communicate, or process any privacy act information or information protected under state or federal law (such as: Personally Identifiable Information, Personal Health Information, Federal or State tax information, Criminal Justice Information from the FBI, PCI data, information from the Social Security Administration, Centers for Medicare and Medicaid Services)?*
- *Does the system store, communicate, or process any trade secret information?*
- *Are there any other extenuating circumstances that may require the SIA to be elevated to the next higher level (such as, but not limited to, the system provides critical process flow or security capability, public visibility of the system, the sheer number of other systems reliant on its operation, or the overall cost of system replacement)?*

If **YES**, then the potential impact is MODERATE. If **NO**, then the potential impact is **LOW**.

The *potential impact* is **HIGH** if —

– The loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on agency operations, organizational assets, or individuals.

Clarification: A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the agency is not able to perform one or more of its primary functions; (ii) result in major damage to agency assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

Applying the standard: Is the information system affected primarily and routinely used to store, communicate, or process any of the following types of information: Emergency Response, Key Asset and Critical Infrastructure Protection, or confidential information that has the potential to cause great harm or damage to individuals or institutions if breached or disclosed to unauthorized users?

If **YES**, then potential impact is **HIGH**.

Appendix D: Normal Change RFCS: Required Information in the Enterprise Ticketing System

Normal Change RFCs: Required Information in the Enterprise Ticketing System	
Normal Change Request	**Required Information**
	• Select the appropriate change type from the dropdown list.
	• Indicate the business need and justification for the change.
	• Indicate the technical validity of the change.
	• Complete the Security Impact Analysis (Appendix C).
	• Indicate if communication has been made to impacted stakeholders regarding the goals and objectives of the RFC.
	• Perform a conflict check and indicate its completion (determine if the change is proposed to be scheduled at the same time as other changes; determine possible impacts of any scheduling conflicts on all affected stakeholders). This may include consulting the ChM Calendar and any applicable change windows for planning the implementation dates.
	• Ensure that the RFC does not interfere with the achievement of service level commitments to agency partners and customers.
	• Indicate the appropriate lead time notice has been provided to all impacted stakeholders, unless the impacted agencies agree to waive this requirement.
	• Indicate when approval of the implementation dates has been received from all impacted stakeholders.
	• Identify if additional assistance from Account Managers, as well as the Application Development staff, has been leveraged, when necessary, to assist with Agency notification - (CR/CO retains ultimate responsibility for obtaining and coordinating the approval of the RFC from all stakeholders).
	• Identify if any cross-functional (departmental/agency) issues are resolved/unresolved.
	• Indicate if Infrastructure Team resources are required for implementation of the change and if they have been contacted.

Normal Change RFCs: Required Information in the Enterprise Ticketing System	
Normal Change Request	**Required Information**
	• Properly complete all required RFC information in the Enterprise Ticketing System in a timely manner.