



George Mason Information Technology Change and Configuration Management Policy

Document Version Number:	2.2
Document Control Number:	ITS.ESD-POL001
Last Updated:	12/4/2025
FOIA Exempt?	No

Process Owner:

- ITS Enterprise Service Delivery – Technology Support & Quality Management

SCOPE:

This policy establishes requirements and guidance for configuration and change management controls over systems critical to delivering IT services. ITS personnel responsible for managing enterprise services (e.g., Service Managers) are accountable for ensuring their services are accurately represented in the Configuration Management Database.

POLICY STATEMENT:

This policy is intended to guide and promote consistent application of controls over system and service changes, thereby:

- Reducing risk of unplanned service outages.
- Improving communication with all affected parties regarding service availability.
- Enhancing operational efficiency by fostering communication and coordination between ITS constituent groups.
- Ensuring that configuration changes are reviewed for potential impact to security and availability before implementation.

RESPONSIBILITIES:

Responsibility for configuration management of resources at all campuses of George Mason University resides with the Assistant Vice President for Information Technology.

Director, IT Governance

- Is responsible for maintaining the Change and Configuration Management Policy and ensuring that supporting procedures and standards are in place and being followed.
- Directs staff to work with IT groups to identify Configuration Items and dependencies represented in the Change Management Database (CMDB) and to perform periodic audits to verify accuracy.

Titles and department names are subject to organizational changes.



Change Manager:

- Chairs the ITS Daily Stand-Up/Change Review Board (CRB) Meeting and generates meeting notes.
- Review all requested changes for completeness and compliance with required information.
- Reviews all outstanding Request for Changes (RFCs) and notifies the requester of status or required updates and escalates to management as needed.
- Produces and maintains regular management reports as needed or requested.
- Verifies that RFCs submitted to be performed during Change Freeze periods meet the requirements to be approved. If the RFC does not meet the requirements, the Change Manager works with the requesting department to reschedule.
- Adds Change Freeze periods to the Change Calendar.

Change Review Board (CRB):

- Reviews and approves/defers changes processed through the Change Management system, considering potential impact on security and service availability.
- Oversees scope as defined above, and as further specified by IT groups, including defined types of changes applicable to CM-controlled assets.
- Determines if an RFC qualifies to be considered a Standard RFC.
- Monitors compliance of RFC requirements.

Service Managers:

- Follow established ITS configuration and change management procedures and standards; develop, document, and follow any additional change management procedures needed for systems with unique regulatory requirements.
- Maintain inventory and baseline configuration information for hardware and software supporting ITS services, in compliance with the ITS Configuration Management Standard
- Ensure only authorized individuals can initiate and perform changes.

COMPLIANCE:

All ITS groups must abide by this policy. All service assets within the scope of this policy must be defined and maintained in the ITS CMDB.

Service Managers and ITS staff must follow the Change Management Procedure. In some cases, departments may need to define and follow additional supporting procedures for services having more stringent or unique requirements for regulatory compliance. (e.g., systems supporting Controlled Unclassified Information.).

A production environment Change Freeze period shall be enforced during Finals week during the Spring and Fall Semesters and for one week prior and two weeks after the Fall Semester starts. During the Change Freeze the only RFCs that will be approved are Emergency (break/fix) or RFCs for security issues (Vulnerability issues, etc.), or RFCs that do not affect systems used for Instruction, including but

Titles and department names are subject to organizational changes.



not limited to classes or grading. All others will be rescheduled to be completed outside of the Change Freeze.

Conflicts between the Change Manager and ITS groups or individuals are directed to the ITS Senior Leadership for resolution. If the conflict is not resolved to the satisfaction of the applicable parties, the matter may be escalated to the Vice President for Information Technology for further review and action.

REVIEW SCHEDULE:

Annually

DEFINITIONS AND ACRONYMS:

Terminology or Acronym	Definition
Asset	Any resource or capability. The assets of a service provider include anything that could contribute to the delivery of a service. All assets are also considered Configuration Items.
Asset Management	Information Technology Asset Management (ITAM) is the set of business best practices that join financial, contractual and inventory functions to support life cycle management and strategic decision making for the IT environment.
Baseline Configuration	A documented, reviewed, and agreed-upon set of specifications for a system asset or configuration items attached to those systems assets. The specifications include information about system components, e.g., software version numbers, configuration settings and parameters, security controls, and the logical placement of those components within the system architecture. Baseline configurations are updated as the system evolves over time.
Change	The addition, modification, or removal of anything that could have an effect (outage, security compliance, altered application behavior, etc.) on IT services including changes to all assets, architectures, processes, tools, metrics and documentation, as well as changes to IT services and other configuration items.
Change Freeze Period	One week prior to and two weeks after classes start for Fall Semester and during final exam periods (aka Finals.) The University Calendar should be checked each semester to obtain the necessary dates for the Change Freeze. Note: The Law School traditionally starts final exams a week before the rest of the University, this should be factored into the Change Freeze period. Other Change Freeze periods may be created as needed for special events including, but not limited to, Board of Visitor meetings, Admissions events, and Mason Day.
Change Management	The process responsible for controlling the lifecycle of all changes, enabling beneficial changes to be made with minimum disruption to IT services.
Change Management Database (CMDB)	A repository of information regarding assets or configuration items. There can be multiple Change Management Databases in an ITAM environment. This repository will be maintained as part of the Information Technology Services IT Service Management tool.
Change Manager	A role responsible for ensuring the application of change management processes, tools, and assessment of the change impact of requests for change (RFC) are followed.

Titles and department names are subject to organizational changes.

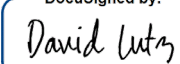


Change Review Board (CRB)	Members of ITS groups with subject matter expertise to review change requests and understand potential impacts of change to ITS managed services, security, and customers' use of the services.
Change Review Schedule	<ol style="list-style-type: none"> 1. RFCs will be submitted by Friday Close of Business for review the following Wednesday. 2. The Change Review Board will review these RFCs to ensure all the required data is in place for approval on the following Wednesday. 3. Notification can be crafted during this period, allowing for an earlier notification to the Mason Community of planned work. 4. Changes will be reviewed on Wednesday for all RFCs starting the following Thursday. There will be a best effort to send an Agenda for the meeting on Tuesdays by Noon with the list of RFCs being reviewed.
Configuration Item	Any component or other service asset that needs to be managed to deliver an IT service. Information about each configuration item is recorded in a configuration record within the configuration management system and is maintained throughout its lifecycle by service asset and configuration management. Configuration items typically include IT services, hardware, software, buildings, people, and formal documentation such as process documentation and service level agreements.
Configuration Management	The process responsible for ensuring that the configuration items and assets required to deliver services are properly controlled, and that accurate and reliable information about those assets is available when and where it is needed. This information includes details of how the assets have been configured and the relationships between assets.
ITSM	IT Service Management refers to the entirety of activities – directed by policies, organized, and structured in processes and supporting procedures – that are performed by an organization or part of an organization to plan, deliver, operate and control IT services offered to customers. It is thus concerned with the implementation of quality IT services that meet the needs of customers and is performed by the IT service provider through an appropriate mix of people, process and information technology.
ITSM Tool	ITS is currently using TeamDynamix as the ITSM Tool for Change Management and Configuration Management.
RFC	<p>The Request for Change (RFC) is a formal request for ITS to implement a change. A Request for Change is to be submitted to Change Management for any Change to a Production service managed by ITS. RFCs should be entered for non-Production changes if the testing is not being done as part of an existent ticket in the ITSM Tool. The RFC will also include Implementation Start and End date/Times. The work on the change will be performed within this window, as approved by the CRB. ITS has three categories of RFC-Emergency, Normal and Standard; the Late category has been deprecated and is being phased out.</p> <p>Emergency RFC: A change that must be introduced as soon as possible – for example, to resolve a major incident or implement a security patch. Emergency changes are defined as changes that need to be evaluated, assessed, and implemented in a short space of time, or will not meet the lead times described in the process. The</p>



	<p>CRB Approval for Emergency changes often comes after the work is completed. There are two types of changes that require time sensitive attention for several reasons:</p> <ol style="list-style-type: none"> 1) Changes required to restore service due to an incident or that must be implemented quickly to avoid one. Changes in this category may include, but are not limited to: <ol style="list-style-type: none"> a) Applying a software patch to address a zero-day vulnerability. b) Resetting, restarting, or reconfiguring a system in an abnormal or non-operational state. 2) Changes that are required quickly due to a pressing business or policy need such as to meet a legal requirement or to conform to a security posture mandate. Changes in this category may include, but are not limited to: <ol style="list-style-type: none"> a) Blocking network access to university systems from a known external threat. b) Blocking Mason’s access to external sites or systems that present a threat. c) Removing a compromised system from Mason’s network. <p>Normal RFC: A Normal change is a non-emergency proposed change that needs to be reviewed by Change Management and follows proscribed timelines.</p> <p>Standard RFC: Standard Changes are pre-approved changes considered minimal risk, performed frequently, and follow a documented (and Change Management approved) process. Standard changes have been designated as low or no security impact and/or low or no business impact and do not require security impact and business impact analyses and follow a documented, and Change Management approved, process. The List of Approved Standard RFC’s can be found here.</p>
Service Manager	A role accountable for managing one or more service components (network, server, database, software, etc.) throughout the components lifecycle, including day to day operations.
Service Owner	Usually a member of Senior Leadership, the person responsible for the overall service.

APPROVAL:

Title, Department Name	Name	Signature and Date
Director, ITS Enterprise Service Delivery, Technology Support & Quality Management	David Lutz	DocuSigned by:  12/4/2025 <small>184177D2DB924A6...</small>

REVISION HISTORY:

Date	Version Number	Department or Author	Brief Description of Changes
1/11/2019	1.0	ITS Enterprise Service Delivery, IT Process & Planning / David Robertson	Initial release. Supersedes TSD-1001 – Change Management (CM) for Network Devices Policy, TSD-1004 – Change

Titles and department names are subject to organizational changes.



			Management (CM) for Hardware/Software Supporting ITS Services Policy, and TSD-NET1002 – Firewall Management Policy
2/20/2023	1.1	ITS Enterprise Service Delivery, Technology Support & Quality Management / David Robertson	Annual review completed with minor edits
12/11/2023	2.0	ITS Enterprise Service Delivery, Technology Support & Quality Management / David Robertson	Annual review completed with minor edits
12/9/2024	2.1	ITS Enterprise Service Delivery, Technology Support & Quality Management / David Robertson	Annual review completed with minor edits; content reformatted using an updated template.
12/4/2025	2.2	ITS Enterprise Service Delivery, Technology Support & Quality Management / David Robertson	Annual review completed with minor edits; content reformatted using an updated template.

RELATED DOCUMENTS/REFERENCES:

- George Mason IT Change Management Process (IT.ESD-PRS001)
- Change Management Procedure (ITS.ESD-PROC002)
- Asset and Configuration Item Management Procedure (ITS.ESD-PROC001)