Change Management Policy

Grambling State University Information Technology

Jay Ellis, Chief Information Officer

Revision History

Version Number	Revision Date
1.0	07/21/2023

PURPOSE

The primary objective of this policy is to ensure that a consistent and systematic approach is used for modifying GSU's Information Technology services and resources. The intent is to streamline processes while mitigating security vulnerabilities and potential loss due to system outages. Modifications to IT services require serious forethought, testing, appropriate communication and post-change evaluation. Changes to University Information Technology Resources must have intended impact and avoid unintended consequences.

Policy

Any change that might affect Information Technology services or resources or could poise potential disruptions and outages in academic and business operations are within the scope of this policy. The following non-exhaustive list show common types of change:

1. Software upgrades, updates or additions;
2. IT infrastructure changes;
3. Preventative maintenance;
4. Security patches;
5. System architecture and configuration changes;
6. Hardware upgrades;
7. New system implementations.

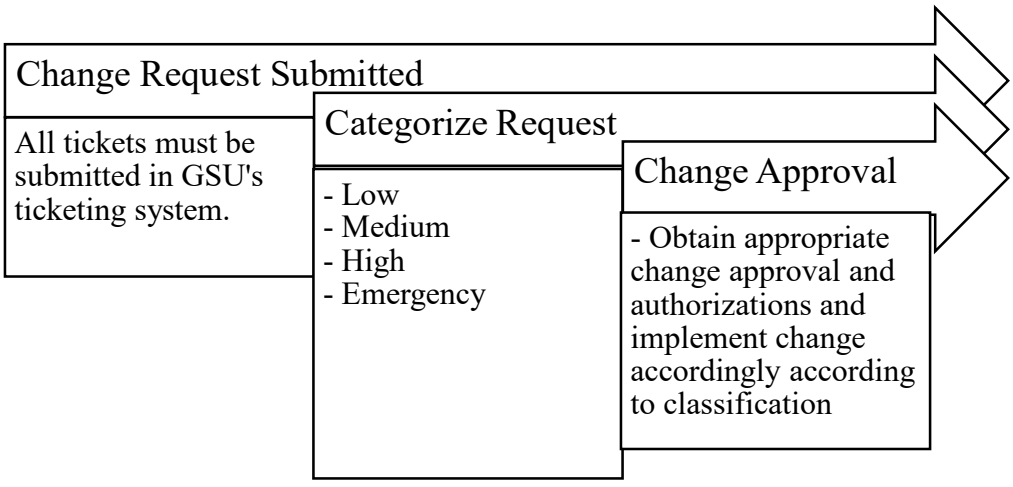
Any change to the University's Information Technology resources will be documented, coordinated, communicated and approved by the Change Control Committee (CCC), as well as adhere to the university's change management procedures and guidelines. The approval will be

obtained prior to updating or modifications being made to any IT resource as outlined in the "Classification of Change" table.

Classification of Change

Type	Approval	Description	Procedure	Examples
Low	CCC	A repeatable change that has been pre-authorized by the Change Control Committee that controls risk and has predictable outcomes.	Submit ticket with basic details via TrackIt	Microsoft Updates
Medium	CCC	A change that is not required immediately or required for a security purpose	Submit Change Control Request Form & Submit ticket with basic details via TrackIT	System/Application Releases; new product features; enhancements
High	CCC	Changes that are required to take effect in effort to correct a performance issue, incompatibility problem, etc.	Submit Change Control Request Form & Submit ticket with basic details via TrackIT	Security Patches (Zero Day); Patches/changes that are needed to fix an issue affecting operations
Emergency	CCC	A change that must be introduced as soon as possible due to likely negative service impacts, such as to mitigate a current cybersecurity threat or to correct a system disruption. Emergency Change must still be authorized retroactively.	Submit Change Control Request Form Post Change (Retroactively) and Submit ticket with details via TrackIT	Firewall firmware causing blockage of traffic, infrastructure change to prevent security incident spread, etc., Cybersecurity Event requiring immediate firewall change to block attack
For any change classification requests that are classified as Medium, High or Emergency, a Change Control Request Form is required.				

Procedures:



GSU's IT/Systems Change Management Process

Change State and Status

Changes can be in – open, closed, pending.

A change status can be, Approved/Rejected/Pending

- Approved – the change has been successfully approved for production implementation
- Rejected – the change has been rejected committee and will not be allowed to move forward unless a risk exception is submitted
- Pending – the request requires more information before making a decision

Emergencies:

In emergency cases, actions may be taken by the Information Technology department that may circumvent this procedure. In these cases, approval will be post change and will still follow the documentation and approval requirements.