Change Management Policy

Information Technology

Purpose

The configuration change management plan is used to document and track the necessary information required to implement changes in the technology we use to serve the University. By applying a repeatable process to control change, we will improve the effectiveness of changes, improve cross-functional communication, and minimize downtime.

Scope

The scope of this document deals with non-routine changes related to Stetson's network infrastructures (cabling, switches, etc.), servers, data, software, telecom configurations, and software configurations. All changes regarding Banner and EIS systems must refer to the EIS change management procedure.

Roles and Responsibilities

All technicians requesting a change within the scope of this document are responsible to follow the configuration change management plan. That includes researching the request, understanding the risks, communicating the change to appropriate parties, and obtaining the necessary approvals. The change approval board (CAB) is responsible for reviewing change requests and either approving, making modifications to, or denying the request.

Failure to adhere to this policy may be subject to disciplinary actions deemed appropriate by the AVP of IT according to regular Stetson University disciplinary processes.

Risk Matrix

Priority 1	Crosses organizational boundaries, serving the business functionality of many units. Is critical to the ability of the University to meet its business and regulatory obligations, support the delivery of education, or administer research. Has strategic value to the campus such that encouragement of widespread use is desirable. **Examples:** Banner, Email, SSO, Active Directory, Core Network, Call Manager, Blackboard, my.stetson.edu, website.
Priority 2	The system is a feeder to Priority 1 systems; or is a system that does not cross organizational boundaries, but is still critical to the ability of the University to meet its business and regulatory obligations. **Examples:** Account creation, DirSync, DegreeWorks, Argos, UR/Web.

Priority 3	Any departmental system that supports the internal operations of any department or departmental function and does not cross organizational boundaries. **Examples:** Bloomberg Terminal, Titanium, Terra Dotta.

Change Classifications

Changes will be classified into four categories: Routine, Minor, Major, and Emergency.

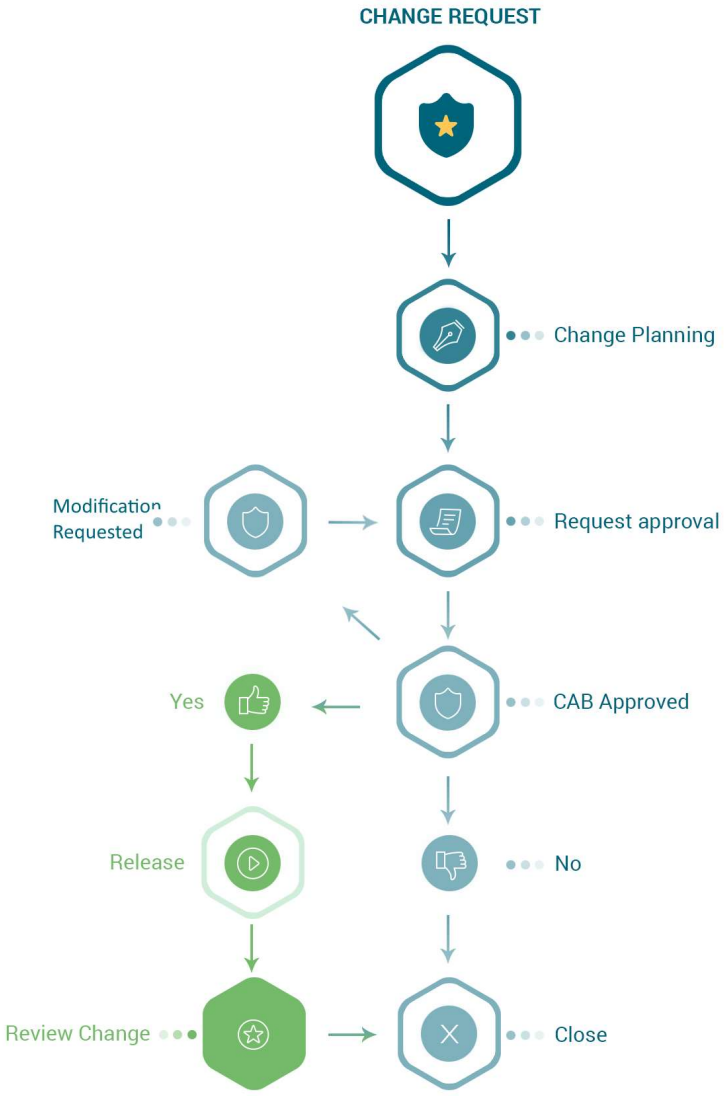
Classification	Description	Written Notification and When	Approval Required	Communication to Users Required
Routine	A Routine change is one that has relatively low risk with well-understood outcomes that is regularly made during normal business. A routine change follows pre-determined processes and can be performed with zero impact on users.	No notification required.	No	No
Minor	A Minor change is one that has low to medium risk for critical services, involves less understood risks, has less predictable outcomes, and/or is a change that is not regularly made during normal business. Because of the ability to affect downstream or upstream services, the CAB must review any proposed change.	Required before the change.	Yes	Yes, unless the impact is transparent to users.

Major	A Major change is one that has medium to high risk for critical services, involves unknown risks, and involves downtime which impacts a large percentage of users across the University.	Yes, at least two days before implementation.	Yes	Yes
Emergency	An emergency change is one that involves services which are already impaired and requires utmost urgency to resolve. Approach is fix first and document change afterwards. Root-cause analysis must be performed to determine if the issue can be prevented in the future.	N/A	N/A	N/A

Change Process

1) **Write Change Request:** All requests should answer the below questions at a minimum and be entered in the CAB in Zendesk.
    - **a.** Type of change (Minor or Major).
    - **b.** What is the requested date to perform the change?
    - **c.** What are the proposed technical changes?
    - **d.** What systems are impacted?
    - **e.** Why is the change necessary?
    - **f.** What people will be involved in performing the change?
    - **g.** Was this change tested in non-production and by whom?
2) **CAB Approval**
    - **a.** If the CAB approves, the change will be scheduled and communications sent to the appropriate group(s).
    - **b.** If the CAB denies the change, the request will be closed or modifications will be requested.

3) **After proper approved notification,** change is released/performed on the date and time communicated.
4) **TEST** the change thoroughly to verify success.
5) **Review Change**
    a. If the change is successful, communicate with the CAB and your relevant users and peers that the change was implemented and was successful.
    b. If the change failed, communicate with your peers and the CAB what steps were taken to restore the environment to a working state and to verify that the system is operating normally.



Questions

If you have questions or concerns regarding this policy or other Information Technology Security Policies, please contact the Office of Information Technology via phone: 386-822-7045, or email: support@stetson.edu.