UADA Policy 920.2
Division Information Technology
Change Management Policy/Process

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 of Arkansas System, Division of Agriculture (UADA). 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 the UADA network infrastructures (cabling, switches, etc.), servers, data, software, telecom configurations, and software configurations.

Policy

Roles and Responsibilities

All UADA 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. There are several technicians within AES and CES that are 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 according to regular UADA disciplinary processes.

Risk Matrix

Priority 1	Crosses organizational boundaries, serving the business functionality of many units. Is critical to the ability of UADA 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: MS Office 365, Azure SSO Apps, Active Directory/Azure, Core Network, Remote Learner/Moodle LMS, websites, etc.
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 organization to meet its business and regulatory obligations. Examples: AD/Workday account creation, DirSync, Argos, etc.
Priority 3	Any departmental system that supports the internal operations of any department or departmental function and does not cross organizational boundaries.

Change Classifications

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 are regularly made during normal business. A routine change follows pre-determined processes and can be performed with zero impact on users.	No notification is 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 appropriate IT personnel 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 UADA.	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 into the change management system
    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) Approvals will be completed by the appropriate IT personnel.
    a. If the request is approved, the change will be scheduled, and communications sent to the appropriate group(s).
    b. If the request is denied, 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 relevant approver and relevant users and peers that the change was implemented and was successful.
    b. If the change failed, communicate with peers and the relevant approver what steps were taken to restore the environment to a working state and to verify that the system is operating normally.

Accountability

The Chief Information Officer for UADA is charged with the responsibility to periodically review the policy and propose changes as needed.