Augsburg College Information Technology Change Management Policy

I. Overview

It is often necessary to make IT infrastructure changes that are broad in scope and are meant to address serious security or compatibility issues. For example, when a security flaw is discovered in a widely-used software application or a piece of hardware, all affected systems must be patched to address the vulnerability, and usually with a degree of urgency. Such "patches" may be in the form of new software or hardware, or even new methods or procedures used to support and use the affected product. In any case, the necessary change affects many or all people in the organization, but may also have negative consequences if applied haphazardly. Testing software updates for undesirable effects and weighing the urgency of a patch against the degree to which services are interrupted are just two ways to ensure change happens smoothly. A well-engineered change management process for updating and upgrading IT resources will aid in streamlining these procedures and reducing risks.

II. Purpose

The purpose of this policy is to ensure that a consistent and systematic approach is used for modifying Augsburg College's Information Technology resources. The intent is to streamline processes while mitigating security vulnerabilities and potential loss due to system outages. Modifications to IT resources and systems require planning, testing, appropriate communication and post-change evaluation. Changes to college IT resources must have the intended impact and avoid unintended consequences.

III. Scope

Any change that might affect IT resources upon which faculty, staff, and students rely on to conduct normal business operations are within the scope of this policy. The following non-exhaustive list depicts common types of change:

- Software upgrades, updates or additions
- IT Infrastructure changes
- Preventative maintenance
- Security patches
- System architecture and configuration changes
- Hardware upgrades
- Product management

This policy applies to all Network Managers, System Administrators, and Application Administrators who are responsible for installation, operation or management of systems or for a collection of data held either remotely on a server or on the hard disk of a computer.

All Augsburg College information systems must comply with the Information Technology Change Management process that meets the standards outlined below.

IV. Change Management Procedures

All changes to an Augsburg College Information Technology resource, including but not limited to operating system upgrades or patches, computing hardware changes, network reconfiguration, and application upgrades and patches are subject to the Change Management Policy and must follow the Change Management Procedures.

All changes affecting computing environmental facilities (e.g., air-conditioning, water, heat, plumbing, electricity, and alarms) need to be reported to or coordinated with the Director of Information Technology Systems.

A written change request must be submitted for all changes, both scheduled and unscheduled. These changes may be submitted to the request tracking system.

All scheduled change requests must be submitted in accordance with change management procedures so that there is sufficient time to review the request, determine and review potential failures, and make the decision to allow or delay the request.

Each scheduled change request must be approved by the Director of Information Technology Systems before proceeding with the change.

The Director of Information Technology Systems may deny a scheduled or unscheduled change for reasons including, but not limited to, inadequate planning, inadequate backout plans, the timing of the change will negatively impact a key business process such as year-end accounting, or if adequate resources cannot be readily available. Adequate resources may be a problem on weekends, holidays, or during special events.

Campus notification must be completed for each scheduled or unscheduled change following the steps contained in these Change Management Procedures.

A change review must be completed for each change, whether scheduled or unscheduled, and whether successful or not. This information may be included within the change management log.

A change management log must be maintained for all changes. This information may be attached to a ticket in the request tracking systems. The log must contain, but is not limited to:

- Date of submission and date of change
- Owner and custodian contact information

- Nature of the change
- Indication of success or failure

V. Enforcement

Anyone found to have violated this policy may be subject to appropriate disciplinary action.