SECTION: 1.0 GENERAL

SUBJECT: CHANGE MANAGEMENT

Title: Information Technology Change Management Procedure

Background: System and program changes are required to ensure the enterprise resource systems are updated, secure, and aligned to data and process needs. This policy is established to protect Lewis-Clark State College (LC State) data, provide reliable enterprise tools, and reduce the risk of data integrity, data loss, or loss of service information productivity through negligence or intentional harm.

Point of Contact: Director of Information Technology / Chief Technology Officer

Other LC State offices directly involved with the implementation of this policy, or significantly affected by the policy: Office of the President, Vice President for Finance and Administration, Vice President for Academic Affairs, Vice President for Student Affairs, Vice President for Institutional Research and Effectiveness

Date of approval by LC State authority: August xx, 2024

Date of State Board Approval: N/A

Date of Most Recent Review: August xx, 2024

Summary of Major Changes incorporated in this revision to the policy: This is a new policy.

1. Philosophy

Formal Information Technology (IT) Change Management prevents unintended or malicious consequences introduced through system changes and ensures that all changes or alterations to systems are implemented according to an approved framework or model.

2. Definitions

A. Information Technology Change Management

IT Change Management seeks to minimize the risk associated with the additions, modifications, or removal of anything that could affect IT services, including changes to the IT infrastructure, processes, documents, interfaces, etc.

B. Change

Change refers to modifying the current state of a technology-related application, process, or service, which could impact end-user functionality or pose a significant risk to college production technology systems.

Examples of changes include but are not limited to:

i. new system implementations and the launch of new applications that may store or interact with college data;

ii. application modifications or updates such as a Colleague upgrade or new system implementation;

iii. hardware modifications or updates such as data storage system upgrades;

iv. software modifications or updates such as an SIS feature update or implementation;

v. network modifications or updates such as a college firewall upgrade or implementation; and

vi. process modifications or updates such as VPN approval process updates.

Note that data entry and regularly occurring low-risk operational changes are not considered changes subject to this policy.

C. Best Practices

Best Practices refer to change management procedures generally recognized by the industry for assuring secure, reliable, scalable, and efficient system management.

i. Tier 0 Systems

Foundational systems that are the infrastructure services necessary to operate Tier 1 systems.

ii. Tier 1 Systems

Mission-critical applications used by LC State. These are required for operation.

D. Hardware, Software, and Information Systems

Technology-related assets that work together or independently to provide a service to the college

E. Production Systems

Systems critical to the operation of a specific department or the college

F. Significant Risk

A risk that poses an operational concern for a majority of the college or might impair the operation of an entire department or division

G. System Administrator

An analyst, engineer, or consultant who implements, manages, and operates a system or systems at the direction of the System Owner, Data Owner and/or Data Custodian

H. System Owner

The manager responsible for the operation and maintenance of an IT system. IT systems may have only one System Owner. The System Owner manages system risk and develops security policies and procedures to protect the system in a manner commensurate with risk; maintains compliance with State of Idaho Information Security policies and standards; maintains compliance with requirements specified by Data Owners for the handling of data processed by the system; and designates a System Administrator for the system.

3. Policy

A. Review of Changes

All planned or proposed changes to Tier 0 and Tier 1 systems must follow one of the following processes as defined.

i. Standard Changes

Standard Changes are pre-authorized for Tier 0 and 1 Systems. These are low-risk changes associated with well-documented, well-tested projects and department procedures. They are documented in a system of record appropriate to the Tier system. For example, all quarterly updates to Ellucian Colleague are to be documented in Enterprise Applications Change Accounting.

ii. Emergency Changes

Changes for Tier 0 and 1 Systems, that must be implemented immediately or within less than five (5) business days, specifically to resolve a major incident or mitigate a critical security vulnerability. These must be approved by a manager or director from IT leadership, normally the individual responsible for maintaining the affected Tier 0 or 1 System.

iii. Normal Changes

The IT Management team reviews, calendars, and discusses all other changes that are not Standard or Emergency Changes.

iv. Blackout Periods

IT leadership will define blackout periods at the first of the semester, in which all standard and normal changes will follow the emergency change process and must be reviewed and approved by two members of the IT leadership team.

v. Separation of Duties

LC State will maintain a separation of duties and responsibilities. This will be enforced by user and group rights management within the given enterprise system. Group rights will be reviewed by managers twice per year.

vi. Best Practices

Managers of LC State IT services must seek and adopt, whenever possible, Best Practices with regard to change management. The IT Managers Team will review and adopt appropriate standards and procedures representing Best Practices for calendaring, documenting, and testing normal changes.

vii. Responsibilities

The Director of Information Technology / Chief Technology Officer is responsible for administering this policy, including its maintenance and compliance. The IT Management Team consists of all managers within IT and the cybersecurity engineer. In addition, the IT Administrative Assistant or IT Project Coordinator will document the Change Management meetings and requests. Appropriate notification is to be made in a timely manner (prior to the change) for disruptive changes, emergency changes, and any high-risk changes that has a high likelihood to disrupt services.

viii. Exceptions to Policy

A request for exception, along with a risk assessment and management plan, must be submitted for review by the Director of Information Technology / Chief Technology Officer. Non-compliance with these standards may result in revocation of access, notification to the supervisor, and reporting to the individual's manager, Human Resources, or Internal Audit.

ix. Enforcement

Failure to comply with this policy may result in suspending the individual's access to network resources until policy standards have been met.

4. Authority

Questions, requests for assistance or other issues regarding this policy should be directed to the Director of Information Technology / Chief Technology Officer.

5. Change Management Procedures

Purpose

A. Document the change management procedures used for enterprise systems at LC State

The purpose is to specify the details as referred to by the following policies:

- Policy 1.206 Vulnerability Assessment and Management
- Policy 1.214 Information Technology Change Management Procedures

B. Enterprise systems are governed by a variety of change control methodologies to authorize changes, coordinate change timelines to avoid conflict, and to support a successful implementation change.

6. Standards

A. Changes to our Tier 1 enterprise systems (services that are critical to the function of the college and directly impact the ability to teach and learn) are presented and discussed at the Change Management Team Meeting.

i. This meeting is facilitated by the Assistant Director of Information Technology.

ii. Items are documented on the change calendar.

iii. Items may be discussed and approved out of band through email to the entire team.

B. Technical changes to our Tier 0 systems (services that are required to be running so that other systems can function) need approval from their directors and may have additional reviews for approvals.

One example of additional checks are changes to the network firewall.

i. Requests are made to the cybersecurity engineer who reviews and documents the technical details.

ii. The IT leadership team reviews and approves the change before the network implements it.

iii. Afterwards the change is reviewed by cybersecurity for correctness.

C. A higher level of scrutiny happens the week before and the week of the fall and spring semester.

D. In addition to the change management listed above, specific directors will be assigned to review changes to ensure proper communication and stability have been established before a change in our busiest times.

7. Non-Compliance and Exceptions

A. A Request for exception, along with a plan for risk assessment and management, may be submitted at to the Help Desk at helpdesk@lcsc.edu.

B. Non-compliance with these standards may result in revocation of access, notification of supervisors, and reporting to the Executive Management Team.