ALAMO COLLEGES DISTRICT
Northeast Lakeview College

Procedure Number:	CS 407
Procedure Title:	Hardware and Software Management Procedure
Relevant Board Policy:	C.1.9 (Policy) Appropriate Use of Information Technology Resources
Relevant SACSCOC Principle:	13.7
Originating Unit:	Information Technology
Maintenance Unit:	Information Technology
Contact for Interpretation:	IT Security Specialist

I. Purpose:

A. The Northeast Lakeview College (NLC) IT department has implemented safeguards designed to mitigate the proliferation of threats and residual risk stemming from all inherent risks. In keeping with the philosophy of limiting complexity to minimize unnecessary attack surface exposure, the NLC IT department approaches the introduction of changes to the NLC infrastructure from a risk-based analytical standpoint in accordance with TAC202 best practices.

B. All new changes, software, or hardware that has not yet gone through the district-level Alamo Colleges ITS Configuration Change Control Policy vetting procedure must go through the NLC Change Control Management (CCM) Procedure before an approval of deployment on NLC assets is granted. In addition, the changes proposed to existing NLC systems and resources must also be vetted for potential detrimental impacts to the existing infrastructure.

C. This NLC CCM Procedure is not meant to act as a replacement to the district-level ITS Configuration Change Control Policy, but to act as a means for NLC IT to regulate changes, software, or hardware requests from NLC users in a timely manner. Additionally, this procedure will provide NLC IT with the means to effectively protect resources from new and emerging vulnerabilities.

II. Objectives:

A. The primary objectives of the NLC CCM Procedure include:
   1. Ensure the privacy and safety of NLC students, faculty, staff, and the public at large
   2. Ensure the stability and performance of NLC systems
   3. Minimize potential disruptions in services to students, faculty, and staff
   4. Reduce the risks to systems within the NLC infrastructure
   5. Effectively document and implement changes to NLC systems

B. When implemented effectively, the CCM Procedure will provide a reduction of the following threats on NLC systems, resources, and assets:
   1. Loss or unauthorized disclosure of confidential and sensitive information
   2. Technical conflicts and misconfigurations
   3. Corruptions of existing NLC resources
   4. Security weaknesses
   5. Malfeasance
   6. Unauthorized changes to systems

III. Roles/Responsibilities:

A. The IT Security Specialist is responsible for conducting preliminary risk analyses, including contacting the vendor to gather System and Organization Controls (SOC) reports (preferably SOC2 Type 1 and 2), and testing the software or hardware for potential vulnerabilities and corruption issues on existing NLC resources. Additionally, the ITSS is responsible for downloading software in a safe manner, while ensuring that the software's integrity is maintained before deployment. Hardware will be vetted in a manner that considers supply-chain risks, which may occur as a result of vendor's purchasing of system components. Changes to NLC systems and resources will be reviewed by NLC IT as a whole.

B. The NLC Change Advisory Board (CAB) will consist of the IT Director, IT Coordinator, IT Security Specialist, and at least two staff and/or faculty senate members. At least five total members must be present to establish a quorum, and an odd number of members is advised to prevent potential ties in voting. The CAB will convene on a weekly basis (if necessary) to discuss any new changes, software, or hardware offerings, and will conduct a vote on each new change proposed.

C. Because the criticality of some software or hardware can differ, and there may be potential access to confidential or sensitive data, the following chart should be employed to properly "weight" the decisions of the CAB:

TABLE 1: Approval Weighting Requirements by Information Classification

Access Required	Risk Level	Approval Needed
Confidential Information	High	100% Approval
Sensitive Information	Moderate	>75% Approval
Public Information	Low	>50% Approval
No Information	Nominal	>50% Approval

NOTE: All new software or hardware that accesses Confidential or Sensitive information must also go through the district-level ITS Configuration Change Control Policy prior to implementation.

D. When considering changes to the NLC infrastructure (migrations, system upgrades, network alterations, changes to websites, changes to Windows Active Directory, etc.), the CAB will be employed to determine approval or disapproval based on the potential impact of the proposed change:

TABLE 2: Level of Effort Requirements by Complexity/Magnitude of Change

Standard	**Normal**	**Major**	**Emergency**
e.g. - OS upgrade	*e.g. - Website Change*	*e.g. - Large Migration*	*e.g. - Breach, Outage*
• Frequent • Documented changes	• Important • Full review and documentation	• High-risk • Detailed full review & reporting	• Urgent • Incident resolution
Approval not required	Requires approval by CMC	Requires NLC and district-level approvals	Approval varies, based on scenario

NOTE: All changes to existing NLC resources, systems, and infrastructure must include a tested rollback plan and execution goals prior to implementation.

IV. Procedure:

A. The individual requesting the new changes, software, or hardware must either fill out the Change Request Form (APPENDIX A), or have a member of NLC IT fill it out for them. The form must capture the requesting person's information for purposes of contacting and making changes, installing software, or deploying hardware (if approved) or notification (if not approved).

1. **All approved software that is installed on NLC systems must be installed from an NLC-approved resource or location. All approved hardware purchases must go through approved vendors. All approved changes to NLC systems or resources will be implemented or supervised by NLC IT.**
2. **Under no circumstances should software be installed directly from the internet prior to integrity checking.**
3. **All hardware must be purchased through vetted vendors.**
4. **All changes to NLC systems or resources must include a full rollback plan in case an event occurs as a result of the change.**

B. Once the change, software, or hardware has been tested and analyzed by NLC IT, the Change Analysis Document (APPENDIX B) will be presented to the CAB for approval. The Change Approval portion of the Change Analysis Document must be completed during the CAB meeting. The ruling on the change request will be recorded on the Change Analysis Document. The proposed software or hardware must be approved by at least 51% of the CAB members to proceed to implementation.

1. **In cases where the proposed software or hardware accesses confidential or sensitive information, a larger percentage of the CAB members must approve. Additionally, full vetting through the district-level ITS Configuration Change Control will be required.**
2. **NLC has no control over the Change Management process that occurs at the district level, so no return time can be provided for the process if sensitive or confidential data is involved.**

C. After the completion of rollback planning, SOP creation, training, and other requirements, implementation of the change will be executed. The Change Readiness Checklist (APPENDIX C) will be completed partially before and partially after the change implementation. If an issue is discovered after implementation of the change that requires a rollback the justification for the rollback will be documented in the section “Additional Comments”.

1. **The typical turn-around time for a Low or Nominal risk change/addition request is approximately one week, depending on the magnitude of the change/addition.**

D. See the Software/Hardware Change/Addition Workflow Diagram (APPENDIX D) for the full procedure workflow identified for changes or new software/Hardware.

V. Definitions:

A. **Attack Surface:** The term identifying all of the points that an unauthorized individual could exploit in order to access systems, data, or resources. Attack surface can apply to software, hardware, network equipment, and sensitive physical locations.

B. **Change Management:** The collective term for all approaches to prepare, support, and help individuals, teams, and organizations in making alterations to the organization. In terms of IT, change management includes the controlled identification and implementation of alterations or additions within a computer system, network, software environment, or IT infrastructure.

C. **Infrastructure:** In terms of IT, infrastructure refers to all devices, systems, software, networks, and resources, both internal and external, which can be leveraged to execute or support business functions in an organization. The term “IT Infrastructure” is often used to describe logical assets and resources, but can also include hard-copy documentation.

D. **Inherent Risk:** The term that identifies the risk to an organization before any security controls are implemented. Inherent risk can either be expressed in quantitative or qualitative metrics, but should be an accurate measurement of the organization’s initial risk prior to applying security controls.

E. **Integrity:** The term describing the fact that devices, systems, software, or data has not been altered or modified in an unauthorized manner.

F. **Residual Risk:** The term that identifies the risk remaining to an organization once security controls have been applied. Residual risk can either be expressed in quantitative or qualitative metrics, but should be an accurate measurement of the organization’s inherent risk minus implemented security controls.

G. **Supply-Chain Risk:** The term that describes some threats involved in conducting business with outside vendors or third-party providers. Supply-chain risks can include the breaching or access of data stores, archives, devices, or software by unauthorized parties (confidentiality), the unauthorized alteration or adulteration of data, information, systems, software, or hardware (integrity), and the loss of a service or hardware (availability).

H. **Vulnerability:** The term identifying a quality or state of a system, software, logical location or physical location that could be exploited by unauthorized parties to gain access, or input/output information.

Attachments: Appendices A – E

Originator: Information Technology

Date Approved: 03/22/2022

Last Updated:

Approved: 3/30/2022
Title: VP, College Services

APPENDIX A: CHANGE REQUEST FORM FOR SOFTWARE/HARDWARE (Completed by Requestor)

Change Request Form (Hardware or Software)		
Submission Date:	Ticket Entry Date:	Ticket Number:
Requestor’s Information:		
Last Name:	First Name:	User ID:
Phone:	Email:	Banner ID:
Change Request Definition:		
Description of proposed change		
Justification for proposed change		
Impact of Not Implementing Change		
Special Instructions		
Move to Production Date: Communication: Other:		

APPENDIX B: CHANGE ANALYSIS DOCUMENT FOR SOFTWARE/HARDWARE (Completed by CAB)

Change Analysis Document		
Submission Date:	Ticket Entry Date:	Ticket Number:

Scope of Change

Affected systems and applications

Deployment Resources Required

Task	Applicable?		Name
Requirements	☐ Yes	☐ No	
Risk/Compliance Analysis	☐ Yes	☐ No	
Design	☐ Yes	☐ No	
Licensing	☐ Yes	☐ No	
Testing	☐ Yes	☐ No	
Integration	☐ Yes	☐ No	
Deployment	☐ Yes	☐ No	
Support	☐ Yes	☐ No	
	☐ Yes	☐ No	
	☐ Yes	☐ No	
	☐ Yes	☐ No	

Special Instructions

Change Review

Request Review		Review Results		
Review Date	Reviewer’s Name/Title	Routine		Emergency
		☐ Approve	☐ Reject	☐ Review
		☐ Approve	☐ Reject	☐ Review
		☐ Approve	☐ Reject	☐ Review
		☐ Approve	☐ Reject	☐ Review
		☐ Approve	☐ Reject	☐ Review
		☐ Approve	☐ Reject	☐ Review
		☐ Approve	☐ Reject	☐ Review

APPENDIX C: CHANGE READINESS CHECKLIST FOR SOFTWARE/HARDWARE (Completed by CAB)

Change Readiness Checklist

Submission Date:	Ticket Entry Date:	Ticket Number:

Readiness Review

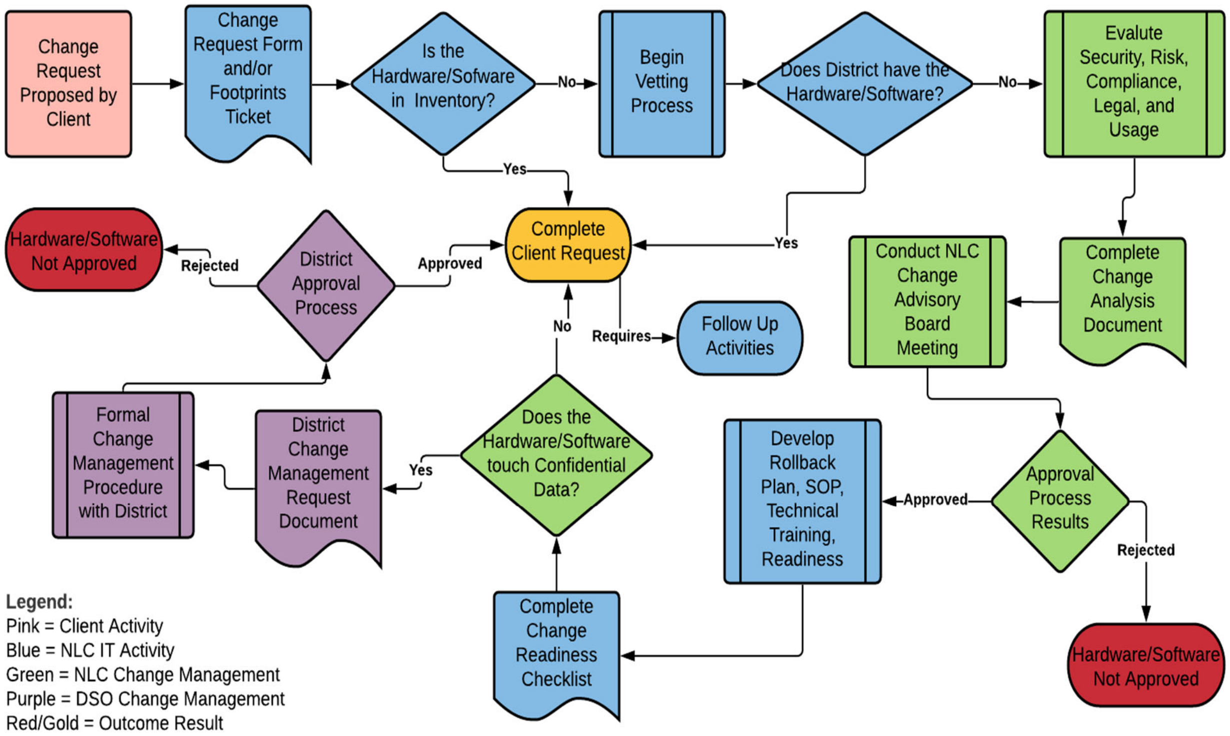
Item	Applicable?		POC Name	Completed
Rollback Plan	☐ Yes	☐ No		☐ Confirmed
SOP Development	☐ Yes	☐ No		☐ Confirmed
Technical Training	☐ Yes	☐ No		☐ Confirmed
Data Standards	☐ Yes	☐ No		☐ Confirmed
Budgeting	☐ Yes	☐ No		☐ Confirmed
Server Readiness Checklist	☐ Yes	☐ No		☐ Confirmed
District Change Management	☐ Yes	☐ No		☐ Confirmed
	☐ Yes	☐ No		☐ Confirmed
	☐ Yes	☐ No		☐ Confirmed

Milestones/Major Tasks

Milestone/Task	Target Date	POC/Comments
Change Control Management Review		
District CCMR		
Stakeholder Communication		
Implementation		
Post-Implementation Follow-Up		

Additional Comments

APPENDIX D: SOFTWARE/HARDWARE CHANGE/ADDITION WORKFLOW DIAGRAM


Change Request Proposed by Client
Change Request Form and/or Footprints Ticket
Is the Hardware/Sofware in Inventory?
No
Begin Vetting Process
Does District have the Hardware/Software?
No
Evalute Security, Risk, Compliance, Legal, and Usage
Yes
Yes
Hardware/Software Not Approved
Rejected
District Approval Process
Approved
Complete Client Request
Complete Change Analysis Document
Conduct NLC Change Advisory Board Meeting
No
Requires
Follow Up Activities
Formal Change Management Procedure with District
District Change Management Request Document
Yes
Does the Hardware/Software touch Confidential Data?
Develop Rollback Plan, SOP, Technical Training, Readiness
Approved
Approval Process Results
Rejected
Complete Change Readiness Checklist
Hardware/Software Not Approved

Legend:
Pink = Client Activity
Blue = NLC IT Activity
Green = NLC Change Management
Purple = DSO Change Management
Red/Gold = Outcome Result

APPENDIX E: PROCEDURE DOCUMENT TRACKING

Version:	Date:	Author/Title:	Description:
1.0	1/5/2022	William Raziano/ITSS	First draft of procedure
1.2	1/6/2022	William Raziano/ITSS	Second draft, including broadening of procedure
1.4	1/10/2022	William Raziano/ITSS	Development of review docs
1.5	1/11/2022	William Raziano/ITSS	Refining docs, minor alterations
1.6	1/12/2022	William Raziano/ITSS	Alteration of forms
1.7	1/14/2022	William Raziano/ITSS	Created Software/Hardware Change Workflow
1.8	1/18/2022	William Raziano/ITSS	Added Definitions section
1.9	1/19/2022	William Raziano/ITSS	Refactored/Formatted Document
2.0	1/21/2022	William Raziano/ITSS	Changes Made/Ready for Consumption