Change Management Policy

1. Overview

Controlling changes to the MicroSociety Academy Charter School (MACS) Information System is critical to maintaining a stable, available and highly efficient environment. Change Management best practices must align with availability and compliance goals for the Information System.

2. Purpose

The purpose of this policy is to manage risk appropriately while ensuring effective change management. Effective change management builds on an existing high-quality system baseline and introduces controlled improvements and configuration updates to the Information System.

3. Scope

Change Management procedures must be utilized for the following ***systems***:

1. Major systems that contain Sensitive/Confidential Data (Alma, QuickBooks, etc.)
2. Major System Changes such as Network Devices

Change Management procedures must be utilized when the following ***functions*** change:

1. Anytime that an adverse change could cause downtime and loss of operational ability, revenues or reputation
2. Major Database changes
3. Change in Information System Standards or Systems Policies
4. Anything that needs approval from school leaders or key stakeholders

4. Roles & Responsibilities

The roles and responsibilities for Change Management may vary by change, however the Change Advisory Board should remain consistent and should include key stakeholders from across the organization to ensure a comprehensive view of changes to the organization.

1. **Change Advisory Board (CAB)** – The CAB is the decision-making authority for MACS. *This is likely the MACS Management Team, in conjunction with MACS' Board Members and Mainstay Technologies.*
2. **Change Manager (CM)**– The CM is responsible for managing the change management process and coordinating workflow. The CM is also responsible for post implementation review and

communications. *This is likely going to be the Curriculum Coordinator or the Technologies Specialist, depending on the change type.*

3. **Change Sponsor** – The Change Sponsor is the stakeholder or the entity requesting the change. *This is the individual or group requesting the change.*
4. **Change Owner** – The Change Owner is the person responsible for implementing the change and presenting any related technical or operational procedures. *This is likely the Mainstay IT Team, in conjunction with the MACS Management Team.*
5. **System Owner** – Some changes may require a system owner. The System Owner could be a third party, organization partner or internal individual or entity that owns the system. *This will vary by the requested change.*
6. **Security & Impact Assessor** – Individual or group with the technical, security and operational knowledge required to assess change risk and impact. *This would be the MACS Management Team, in conjunction with and with support from Mainstay IT and Mainstay InfoSec.*

It is possible, and even likely, that an individual may play multiple roles depending on the complexity, size and risk profile of the school and or information system. In addition, it is likely that these roles will vary by change, depending on the nature of that change.

5. Change Priority

The following change management exist and should be used to govern the change management process:

1. **Emergency** – Emergency priority changes are changes that will leave the Information System at critical risk if not implemented quickly. The CAB should be notified immediately, and Emergency changes should be implemented and tested as soon as possible to reduce imminent or existing risk to MACS.
2. **High** – High priority changes are important changes that must be implemented soon prevent negative impact and or significant organization disruption.
3. **Normal –** A Normal priority change is a standard change that is not urgent but represents benefit to MACS and should be documented and scheduled to reduce risk.
4. **Routine** – Routine changes are listed below and will not follow the change management process. These are general organization and system activities that are low risk, low impact, high volume and or high value and efficiency.

6. Impact Assessment

Change management impact analysis should be conducted for each change and the following should be carefully considered:

1. Risk to the school if the change is implemented or not implemented
2. Impact if the change fails

3. Roll back process needed to recover to the previous system baseline
4. Internal and External communications
5. Timing of the change to minimize operational impact
6. Measure security impact to be sure that security baseline is met or improved
7. Determine how success will be measured to determine if organization objectives have been met

Risk levels should also be assigned when assessing impact. The following risk categories will be used:

1. **High Risk Change** – The change will impact several employees and/or students or other stakeholders. This change may cause major critical system disruption. The change is highly complex and or involves multiple cross functional organization and technical resources. The change could introduce several hours of service disruption and or outages during production periods. The change impacts critical data or systems housing sensitive data.
2. **Moderate Risk Change** – The change may impact some number of employees and/or students or other stakeholders but is under tight control and is easily communicated. The change may cause major critical system disruption but is unlikely due to proper planning and mitigating controls. The change has some complexity and may involve multiple cross functional organization and technical resources. The change could introduce a minor service disruption and or outages during production periods.
3. **Low Risk Change** – The change will not impact employees and/or students or other stakeholders or the impact will be minimal, and some form of communication may or may not be needed. The change will not cause critical system disruption or will be scheduled during maintenance windows. The change is not complex and does not require cross-functional resources. The change will not introduce service disruption and or outages during production periods.

7. Change Management Process Flow

1. Change is identified and entered into the tracking system. Change form should be used or elements necessary to fill out change form should be included in the tracking system.
2. Change management form is completed (Sample Form Below).
3. Change Owner presents change to CAB.
4. CAB reviews and confirms critical elements to include proper Description, Impact Analysis, Testing Plan, Roll-Back procedures and any required Technical review by system owners.
5. CAB Approves, Denies, Places on Hold or asks for additional information. Approvals must be documented.
6. Once approved, the change is scheduled. An intentional approach should be taken when scheduling the change. All impact to production systems and organization productivity should be considered. Efforts should be made to schedule high risk/impact changes outside of normal organization hours or in test environments if available.
7. The Change is performed or rolled back. If a roll back occurs, the details should be presented to the CAB.
8. Any post Change notes should be documented in the Change form.

9. Existing processes, and baselines should be updated post change if necessary.
10. Change is closed and Change records retained for audit and follow-up per records management retention schedules.

8. Routine Changes (Pre-Approved Changes)

Changes that are deemed high volume, low risk and or low impact will be considered routine and will not follow the change management process flow. This list includes:

1. Password resets - Users (non-critical system or service accounts)
2. User level addition, deletion and modification
3. Group creation, deletion and modification
4. Re-booting systems where there is no change to critical system configuration
5. Directory or file level access or permission changes
6. General user level support activities within applications
7. Settings changes that improve security, functionality, reduced risk and increase efficiency without negatively impacting the Information System or current baseline configuration.
8. System or service restoration to re-constitute the current baseline configuration (system or service in a downed state).

The CAB may modify this list periodically to increase efficiency or reduce risk

9. Training

Training will be coordinated when there are significant updates made to the change management process, major organization system changes that impact work flow or failed changes occur that require additional training and follow-up.

10. Updates

This policy is reviewed and updated annually, at a minimum. The Change Management Policy may be updated on an ongoing basis as roles and conditions change.

Appendix A: MACS Change Management Form

Change # (Help Desk Ticket):	
Change Title:	
Request Date:	
Priority:	
Impact:	
Change Owner:	
Sponsored By:	
Change Manager:	
Description of Change and Implementation Process:	
Reason for Change:	
Test Plan (Include Security testing):	
Roll Back Procedure:	
Existing Doc's need to be updated?	
Security, Risk Impact & Availability Assessment:	
Technical Review:	
Approval Status:	
Approved By:	

Change Schedule (Date and Time):	

First Reading: 2/12/2020

Adopted: 3/15/2020