Australian Shepherd Club of America, Inc.

Change Management Policy

Purpose:
The purpose of this Change Management Policy is to ensure that changes made to our organization's IT systems and services are effectively managed and controlled to minimize the risk of cybersecurity threats and vulnerabilities.

Scope:
This policy applies to all IT systems and services owned or operated by our organization.

Roles and Responsibilities:

a. Change Owner: The individual or team responsible for proposing and planning a change.
b. Change Approver: The individual or team responsible for approving or rejecting a change request.
c. Change Implementer: The individual or team responsible for implementing the change.
d. Change Reviewer: The individual or team responsible for reviewing and verifying the effectiveness of the change.

Change Management Process:

a. Request for Change: Any change to IT systems or services must be documented in a Change Request Form. The Change Owner is responsible for initiating and completing this form.
b. Change Approval: The Change Approver must review and approve the change request based on the impact analysis, risk assessment, and compliance requirements.
c. Change Implementation: The Change Implementer is responsible for implementing the change in a controlled and monitored manner.
d. Change Review: The Change Reviewer must review and verify the effectiveness of the change by performing a post-implementation review to ensure that it has met the desired outcome, has not introduced any new risks, and is compliant with all regulatory requirements.

Change Management Control:

a. Change Control Board: A Change Control Board (CCB) must be established to ensure that all changes are reviewed and approved by a group of subject matter experts, including representatives from the information security, compliance, and business areas.
b. Configuration Management: Changes made to IT systems or services must be tracked and documented in the Configuration Management Database (CMDB).
c. Testing and Validation: Changes must be tested and validated in a non-production environment before being implemented in production.
d. Rollback Plan: A rollback plan must be developed to revert to the previous state in case of any issues or failures during implementation.

Commented [ct1]: For now, this could be as simple as maintaining a change log in Excel.

e. Change Freeze: A change freeze period must be established to restrict changes during critical business periods or during emergency situations.

Compliance:
This policy is designed to comply with the NIST Cybersecurity Framework. All changes must be compliant with applicable laws, regulations, and industry standards.

Enforcement:
Any violation of this policy may result in disciplinary action, up to and including termination of employment, as well as legal action.

Review and Revision:
This policy must be reviewed and updated at least annually or when there are changes to our IT systems or services, regulatory requirements, or industry standards.

Revision History:

Date	Version	Summary of Changes	Approved By