Australian Shepherd Club of America, Inc.

Software Development Life Cycle (SDLC) Policy

Purpose:
The purpose of this Software Development Life Cycle (SDLC) Policy is to ensure that all software developed or acquired by our organization is designed, built, tested, and deployed in a secure and consistent manner to minimize the risk of cybersecurity threats and vulnerabilities.

Scope:
This policy applies to all software developed or acquired by our organization, including custom-developed software, commercial off-the-shelf (COTS) software, and open-source software.

Roles and Responsibilities:

a. Software Development Team: The individuals or team responsible for designing, developing, testing, and deploying software.
b. Information Security Team: The individuals or team responsible for ensuring the security of the software development process and the software itself.
c. Project Manager: The individual responsible for overseeing and managing the software development project.

SDLC Process:

a. Planning: The software development team must develop a project plan that includes requirements, design specifications, and timelines.
b. Analysis: The software development team must analyze the requirements and identify potential security risks and threats.
c. Design: The software development team must design the software to meet the requirements and address the identified security risks and threats.
d. Implementation: The software development team must implement the software according to the design specifications, following secure coding practices and using approved development tools and methodologies.
e. Testing: The software development team must test the software to ensure it functions correctly and is secure against known vulnerabilities and threats.
f. Deployment: The software development team must deploy the software to the production environment following a controlled and monitored process.
g. Maintenance: The software development team must maintain the software by addressing any reported defects, vulnerabilities, or security incidents.

SDLC Control:

a. Change Management: Changes to software must follow the Change Management Policy.
b. Security Testing: All software must undergo security testing before deployment.
c. Vulnerability Scanning: All software must undergo vulnerability scanning before deployment and periodically during operation.

d. Code Review: All software code must undergo a peer review process to identify any potential vulnerabilities or defects.
e. Secure Coding: All software code must follow secure coding practices and standards.
f. Documentation: All software must be fully documented, including design specifications, testing procedures, and maintenance procedures.
g. Compliance: All software must be compliant with applicable laws, regulations, and industry standards.

Compliance:
This policy is designed to comply with the NIST Cybersecurity Framework. All software 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 software development process, regulatory requirements, or industry standards.

Revision History:

Date	Version	Summary of Changes	Approved By