SNOWBE ONLINE Policy

Software Development Life Cycle Policy

Group: Group 2

Names: Jeremy Sarduy, Eddy Cruz, David Perez Puello, Vanessa Campbell, Travis Ferrufino

Software Development Life Cycle

Policy Standard - Version # 1

DATE: 7/28/2024

Table of Contents

Purpose

The purpose of this policy is to establish a comprehensive framework for development, implementation, and maintenance of information systems within Snowbe. This policy aims to ensure that security measures are integrated throughout the System Development Life Cycle (SDLC), protecting both company data and systems.

Scope

The scope of this policy applies to all employees, contractors, and third-party vendors involved in the development, implementation, and maintenance of Snow information systems.

Definitions

System Development Life Cycle (SDLC)

- Process used by Snowbe to design, develop, test, and deploy systems and applications, ensuring that they meet business and security requirements provided by the company.

Security Requirements

- Specific measures and controls implemented during the SDLC phases to protect the system and its data from unauthorized access, modification, or destruction.

Risk Assessment

- The process of identifying, evaluating, and mitigating risks to Snowbe and their information systems.

Roles & Responsibilities

Chief Information Security Officer (CISO)

- Develop and maintain this policy.
- Ensure the policy aligns with the industry's best practices and regulatory requirements.
- Provide oversight and support for the implementation of the policy.

It Security Team

- Implement and enforce security controls throughout the SDLC.
- Conduct regular secure assessments and audits to ensure viability and check for potential vulnerabilities.
- Provide training and resources to ensure compliance with this policy.

Project Managers

- Ensure that projects adhere to this policy and all policies and procedures within the SDLC.
- Coordinate with the IT Security Team to address security requirements and risks.

Developers

- Implement secure coding practices and adhere to security requirements during the entire development

process.

- Participate in security training and awareness programs.
- Follow industry best practices and stay up to date with regulatory requirements.

Policy

General Guidelines

Planning Phase

- Define the project scope, objectives, and security requirements
- Conduct a risk assessment to identify security risks that would potentially present themselves throughout the life cycle of the project.
- Develop a project plan that includes security considerations and resource allocation.

Analysis Phase

- Gather detailed security requirements based on business needs and regulatory requirements from all stakeholders involved.
- Analyze potential security risks and vulnerabilities.

Design Phase

- Create a secure system architecture and design for concept and production.
- Incorporate security controls and measures, such as encryption, access controls, and secure data storage.

Implementation Phase

- Develop the system according to secure coding standards and stakeholder relationships throughout the phase.
- Perform regular code reviews and security testing, including vulnerability/risk assessments and penetration testing.

Testing Phase

- Conduct testing for functionality, performance, and security to ensure all systems are production ready before deployment.
- Address and resolve all identified vulnerabilities before deployment.

Deployment Phase

- Post systems into production in a secure manner, ensuring all security controls are in place.
- Conduct any final risk assessments and ensure compliance with security policies implemented by Snowbe.

Maintenance Phase

- Monitor the system for security incidents and vulnerabilities.
- Apply security patches and updates as needed.
- Conduct regular security audits and reviews within the system.

Security Documentation

- Maintain detailed documentation of all security requirements, assessments, design requests and decisions, and testing results for production.

Exceptions/Exemptions

Emergency Access:

- In cases of urgent Snowbe needs requiring deviation from the SDLC policy, a formal risk assessment and approval process must be followed.
- Legacy Systems
  - Any systems that cannot fully comply with the SDLC policy will undergo a risk assessment and obtain approval to exceptions and standards to begin to bring legacy systems into the policy framework.

Enforcement

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment. Contractors and any third-party vendors found in violation of this policy may face contract termination and legal action.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
1	7/28/2024	Group 2		Software Development Life Cycle
