SNOWBE ONLINE

Policy# SDLC 01

Secure Development Life Cycle

Chris Stevens

Secure Development Life Cycle (SDLC)

Version # 1.0

DATE: 10-28-2025

Secure Development Life Cycle (SDLC) – V 1.0
Status: ✠ Working Draft ☐ Approved ☐ Adopted
Document owner: Chris Stevens
DATE: 10-28-2025

Table of Contents

Purpose

The purpose of this System Development Life Cycle (SDLC) Policy is to establish a standardized framework for the design, development, implementation, and maintenance of all information systems and applications at SnowBe Online. This policy ensures that security and data privacy are integrated into every stage of the system lifecycle, from initial concept to retirement. By following this policy, we'll ensure that our systems, including the AWS-hosted website, internal servers, and company-wide applications, are secure, reliable, and compliant with all legal and regulatory requirements, such as PCI compliance.

Scope

This policy applies to all SnowBe Online employees, contractors, and third-party vendors involved in the development, modification, or deployment of software, systems, and applications. This includes, but is not limited to, the e-commerce website on the AWS platform, on-premise servers (for access management, storage, etc.), and all related applications.

Definitions

System Development Life Cycle (SDLC)
A structured process for planning, creating, testing, and deploying an information system.

Secure Coding
The practice of writing code that is resistant to security vulnerabilities and exploits.

Vulnerability Scan
An automated test of a system's security to identify potential weaknesses.

Penetration Testing
An authorized simulated cyberattack on a system to identify exploitable security vulnerabilities.

Production Environment
The live, operational environment where an application or system is used by end-users or customers.

Roles & Responsibilities

IT Director/Manager
Responsible for overseeing the entire SDLC process and ensuring that all policies and procedures are followed.

Developers
Responsible for writing secure code and adhering to the defined SDLC process.

QA/Testers
Responsible for testing systems for functionality and security vulnerabilities before deployment.

System Administrators
Responsible for deploying, maintaining, and securing systems in the production environment.

Information Security Office
Responsible for conducting security reviews and approving systems before they move to production.

Policy

All system and application development at SnowBe Online must follow a documented SDLC process that integrates security from the earliest stages.

Requirements Gathering
All project requirements must include a security review to identify and address potential risks. This is especially critical for systems handling sensitive data like customer credit card and personal information.

Design and Architecture
System designs must incorporate security controls, such as secure data storage (for credit cards and customer information) and access controls.

Development
Developers must use secure coding practices and avoid common vulnerabilities. All code must be reviewed by a peer before it can be committed.

Testing

a. Vulnerability Scanning
Before deployment to the production environment, all new or updated systems must undergo a vulnerability scan.

b. Penetration Testing
High-risk systems, such as the e-commerce website, must be subjected to a penetration test.

Deployment
All changes to the production environment must be approved and documented. A rollback plan must be in place to handle deployment failures.

Maintenance
All systems must be regularly patched and updated with the latest security fixes, including the WordPress shopping cart, Windows servers, and network device firmware.

End of Life
When a system or application is retired, all sensitive data must be securely erased and all access to the system must be revoked. This includes customer data and purchase history stored on the website database.

Exceptions/Exemptions

Exceptions to this plan must be approved by the Information Security Office, under the guidance of SnowBe's IT Director and/or IT Manager. All exceptions will be formally documented. Plan exceptions will be reviewed on a periodic basis for appropriateness. Please note that while requesting exceptions or exemptions has been made available to you, it does not guarantee approval.

SnowBe Online recognizes that, under certain circumstances, deviations from this Acceptable Use Policy may be necessary to support specific business needs or technical requirements. Exceptions or exemptions to this policy may be granted under the following conditions:

Risk Acceptance
In some rare cases, a business case for non-compliance can be established. In all such cases, the non-compliance situation must be approved in advance through a risk acceptance process. This process requires a risk acceptance memo signed by a department manager and reviewed by IT Enterprise Security and IT Information Systems and approved by the IT Director and/or IT Management. Further details on the risk acceptance process can be obtained through the Enterprise IT Security Department.

Pre-Approval Required
All exceptions must be formally requested in writing and approved by the IT department and an authorized member of management. The request must clearly state the business justification, duration, and potential risks of the exception.

Documentation and Review
Approved exceptions will be documented and maintained by the IT department. All exceptions are subject to periodic review to ensure they remain valid and do not introduce unacceptable risks.

Temporary and Specific
Exceptions are granted on a temporary basis for clearly defined scopes and timeframes. They do not constitute a permanent change to the policy.

No Unauthorized Exceptions
Any deviation from this policy without documented approval is considered a violation and may result in disciplinary action, including suspension of access privileges.

Compliance Priority
Exceptions will not be approved if they compromise SnowBe Online's compliance with legal, regulatory, or security requirements.

Enforcement

Enforcement
SnowBe Online takes the enforcement of this (Policy name) seriously to protect its systems, data, and customers.

Violations of this policy, whether intentional or accidental, may result in disciplinary action, up to and including termination of employment, contract cancellation, and/or legal action.

The penalties will include the following components:

Monitoring and Auditing
SnowBe Online reserves the right to monitor, log, and audit all system and network activity to ensure compliance with this policy. Users should have no expectation of privacy when using company-owned systems or accessing company data.

Incident Investigation
Suspected policy violations will be investigated promptly by the IT department, Human Resources, and other relevant stakeholders. Users are expected to cooperate fully during any investigation.

Corrective Action
If a violation is confirmed, corrective actions will be taken based on the severity and nature of the breach. This may include revocation of access, mandatory training, written warnings, or other disciplinary measures as outlined in the employee handbook.

Legal Consequences
Activities that are illegal under local, state, or federal law may be reported to the appropriate authorities. This includes unauthorized access, data breaches, or misuse of customer financial information.

Appeals Process
Individuals who believe they were unfairly penalized for a policy violation may appeal the decision to management or HR following internal dispute resolution procedures.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
1.0	10-28-2025	Chris Stevens	CEO	Secure Development Life Cycle (SDLC)

Citations

The University of Kansas
https://services.ku.edu/TDClient/818/Portal/KB/ArticleDet?ID=21409
Purpose, Scope, Policy, Roles & Responsibilities

Bowie State University
https://www.bowiestate.edu/files/resources/information-security-public.pdf
Exceptions/Exemptions

ChatGPT
https://chatgpt.com/c/681bc793-d1dc-800b-a676-cb7b3cf2678d
Exceptions/Exemptions, but as a group we revised the verbiage.

Policy Template
https://www.sans.org/information-security-policy/
Exceptions/Exemptions