SNOWBE ONLINE SD-1 System Development Life Cycle Policy

Ray Yancey

<SDLC> - Version 1.0

DATE: 12/19/25

Table of Contents

Purpose

The purpose of the Secure Systems Development Lifecycle (SSDLC) policy is to define the security requirements and tasks that must be considered and addressed within every system, project or application that is created or updated to address a business need in SnowBe Online. SnowBe's systems and applications may change over time to adjust to ever changing business, regulatory and statutory requirements. Security is a requirement that must be included within every phase of SnowBe's systems development life cycle.

Scope

This policy document applies to all SnowBe Online programs with an information technology component. SnowBe's managerial staff as well as its contracted or hourly employees are responsible for ensuring that the systems development and management approach described in the document is practiced on a day-to-day basis. Because there may be external Federal agencies (i.e., Government Accountability Office, Office of Management and Budget, etc.) who may request investment information at a moment's notice, SnowBe Online's upper-level management, must be prepared to provide SDLC documentation or deliverables. This can only be achieved by following the best practice of utilizing an SDLC and documenting the SDLC deliverables.

Definitions

CIO – Chief Information Officer
IRB – Investment Review Board
KPI – Key Performance Indicator
Procurements – Things obtained or "procured" by SnowBe Online
(SDLC) – System Development Life Cycle

Roles & Responsibilities

(CIO)

- Assigning the Technical Project Manager to the IT project.
- Jointly responsible with SnowBe Online's Associate Directors, Heads of Offices and Senior Executives for selecting, assessing and managing information technologies
- Reviewing and approving all information technology-related procurement plans and strategies
- Approving all IT-related procurements
- Advising SnowBe Online's CEO and Stakeholders on the selection, management and use of information technology, and on risks related to the management of IT
- Advising the agency head on budgetary implications of information technology decisions as the Chair of the Investment Review Board (IRB);
- Advising the agency head on whether to continue, modify or terminate an IT investment
- Designating CIO staff to be on the Integrated Project Team for the program or project
- Designate CIO staff to be dedicated technical advisors on IT projects if funded by the program office or by the project

(Project Manager):

- Lead end-to-end project planning, execution, and delivery for cybersecurity software initiatives.
- Define project scope, objectives, and deliverables aligned with security requirements and stakeholder expectations.
- Track KPIs such as velocity, sprint completion rates, defect trends, and security test results.
- Oversee secure SDLC (Software Development Life Cycle) practices, such as code reviews and security testing.
- Advocate for security-first development practices and developer security training.

(Compliance/Audit Teams)

- Review public content regularly to confirm it does not include nonpublic data.
- Document findings and initiate immediate removal of exposed information.
- Draft and enforce agreements such as Non-Disclosure Agreements (NDAs) and data sharing contracts.
- Provides guidance on regulatory requirements affecting information sharing.

Policy

SnowBe Online's Software Development team, is responsible for developing, maintaining, and participating in a Systems Development Life Cycle (SDLC) for SnowBe Online system development projects. All entities at SnowBe Online, that are engaged in systems or software development activities, must follow SnowBe Online's SDLC. SnowBe's SDLC is defined as follows:

- All software developed in-house which runs on production systems must be developed according to the SnowBe Online's SDLC Standards. At a minimum, this software development plan should address the areas of preliminary analysis or feasibility study; risk identification and mitigation; systems analysis; general design; detail design; development; quality assurance and acceptance testing; implementation; and post-implementation maintenance and review. This methodology ensures that the software will be adequately documented and tested before it is used in conjunction with critical and/or sensitive SnowBe Online user information.
- All development work shall exhibit a separation between production, development, and test environments, and at a minimum have at least a defined separation between the development/test and production environments unless prohibited by licensing restrictions or an exception is made. These separation distinctions allow better management and security for the production systems, while allowing greater flexibility in the pre-production environments.
- Where these separation distinctions in environments have been established, development, and QA/test staff must not be permitted access to production systems unless absolutely required by their respective job duties/descriptions.
- All application/program access paths utilized in development or testing, other than the formal user access paths, must be deleted or disabled before software is moved into production.
- Documentation must be kept and updated during all phases of development from the initiation phase through implementation and ongoing maintenance phases. Additionally, security considerations should be noted and addressed through all phases.
- All software and web applications that create, manage, use, or transmit Level I information, must be developed and maintained solely by SnowBe Online's Information Technology team. Other development work involving Level II and Level III information

may be done outside of SnowBe IT provided SnowBe Online's Systems Development Life Cycle (SDLC) Standards are followed

Exceptions/Exemptions

Exceptions will be reviewed by the IT Director under the guidance of the Custodians. To request an exception, submit an Information Security Exception request to the Information Security Department. The request should clearly state what policy, control, or requirement the exception applies to, as well as the reason for the request and any mitigating measures to address associated risks. All exceptions will be formally documented and reviewed on a periodic basis to ensure continued appropriateness.

Enforcement

SnowBe Online will take appropriate remedial action, which may include, but is not limited to, verbal or written warnings, suspension, or termination of employment. SnowBe Online will also report to law enforcement, if appropriate.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
1.0	12/19/2025	Ray Yancey	Prof. Stone	System Development Life Cycle Policy

Citations

https://services.ku.edu/TDClient/818/Portal/KB/ArticleDet?ID=21409

https://www.opm.gov/about-us/open-government/digital-government-strategy/fitara/opm-system-development-life-cycle-policy-and-standards.pdf