SNOWBE ONLINE Policy#01
System Development Life Cycle

Your name: Paola Baez Hernandez

< Policy#01 System Development Life Cycle **> - Version #01 DATE:**

05/29/2025

Table of Contents

Purpose

The purpose of this policy is to ensure that all systems and software development at SnowBe Online adheres to a secure, standardized, and repeatable lifecycle. It incorporates security best practices at each phase and aligns with NIST SP 800-160 to reduce any vulnerabilities, protect customer data, and also be a support for long-term business resilience and regulatory compliance.

Scope

This policy applies to all internal teams and third-party vendors involved in developing, maintaining, or enhancing SnowBe Online systems and applications, whether hosted on premises or in the cloud.

Definitions

SDLC (System Development Life Cycle): A framework that outlines each step involved in building and maintaining information systems.

Secure Coding: Programming practices that help prevent common vulnerabilities like injection, buffer overflows, and unauthorized access.

Threat Modeling: A security exercise performed during system design to identify possible attack scenarios and plan defenses.

Roles & Responsibilities

CISO: Oversees secure SDLC implementation and ensures alignment with regulatory and business goals.

Developers: Implement secure code practices and collaborate in reviews and threat modeling.

Project Managers: Ensure the project timelines and security checkpoints are followed during each of the SDLC phases.

QA Analysts: Test systems for security, usability, and performance before the release.

Security Team: Conduct risk assessments, evaluate architecture, and review test and deployment plans.

Policy

SnowBe Online mandates the use of a secure SDLC model for all system and software development projects:

1. **Planning & Requirements:** Identify technical, functional, and security needs early.
2. **Design:** Review architectural plans and conduct threat modeling.
3. **Development:** Adhere to secure coding standards and track changes in version control.
4. **Testing:** Perform static/dynamic analysis and security vulnerability scanning.
5. **Deployment:** Use structured change control, with rollback procedures if needed.
6. **Maintenance:** Monitor logs, track system health, and apply necessary patches or updates.

Exceptions/Exemptions

Any deviations from this policy must be submitted for review and approval by the IT Director or CISO. Documentation must include a business justification and mitigation plan.

● To ensure compliance with internal standards, exceptions or exemptions requests are handled through a specific procedure. These requests are reviewed, justified, and approved according to SnowBe Online's internal guidelines.
● The dropdown for submitting Exceptions/Exemptions requests can be found on the SnowBe Online associate portal webpage. Allowing staff members to easily request exceptions or exemptions from regular rules and processes, guaranteeing that any deviations are appropriately recorded and examined.
● The request form is available through the “Compliance Forms” tab, located at the top right of the page. This ensures consistency throughout the process; this centralized location makes it simple for employees to find, be able to view, and send requests.
● The form for requesting exceptions or exemptions is titled “Exceptions/Exemptions” within the drop-down window. This clearly labels the form for exception or exemption requests, ensuring that the process is straightforward, and users can identify the correct form to address their specific needs.
● Requests for exceptions or exemptions are made when deviations from standard procedures or policies are necessary due to specific circumstances, such as operational needs, technical constraints, or temporary situations. Any changes are carefully thought through and examined before they are accepted as a result of these requests.

Approval Hierarchy:

● IT: The IT Director or IT Manager will perform the initial review to ensure the requested exemption does not compromise SnowBe Online's security, infrastructure, or compliance.
● Management: Management will review the request to confirm alignment with business objectives and ensure that no critical operations are disrupted.
● Final Authority: The IT Director or IT Manager holds the final authority on all exceptions or exemptions, ensuring decisions align with SnowBe Online’s overall business strategy, security requirements, and compliance obligations.

Approval Notification: Once the request is submitted, the requester will receive an email notification indicating whether the request was approved or denied. The status of the request can also be tracked via the SnowBe Online associate portal webpage.

Enforcement

Failure to comply with this policy may result in access restrictions, retraining, or disciplinary measures depending on the situation. CISO, in consultation with HR and Management, will oversee enforcement.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
V .1.0	05/29/2025	Paola Baez		SNOWBE ONLINE Policy#01 System Development Life Cycle

Citations

https://www.nist.gov/

https://help.drata.com/en/articles/8002321-software-development-lifecycle-sdlc-policy-guidance