SNOWBE ONLINE

Policy DEV-01

Systems Development Life Cycle Policy

Daphnie Bruno

DEV-01 - Version # 1.0

March 24 2025

Table of Contents

Purpose

The purpose of the Systems Development Life Cycle (SDLC) Policy is to describe the requirements for developing and/or implementing new software and systems at SnowBe Online and to ensure that all development work is compliant as it relates to any and all regulatory, statutory, federal, and /or state guidelines.

Scope

SnowBe Online employees (faculty, staff), students, and other covered individuals (e.g., vendors, independent contractors, etc.) that perform any type of software or systems development work under the auspices of SnowBe Online.

In the event a SnowBe Online Department or Unit chooses to seek an exemption for reasons such as inability to meet specific points, tasks, or subtasks within the SDLC Policy or Standards, a SDLC Review Committee, comprised of representatives from across campus as designated by Information Technology, will convene in order to assess the specific merits of the exemption request(s) while still adhering to the main principles behind the SDLC Policy and Standards.

Definitions

- **SnowBe Online affiliates**: are the people and organizations associated with SnowBe Online through some form of formalized agreement.
- **Level I information**: is SnowBe Online Information with a high risk of significant financial loss, legal liability, public distrust, or harm if this data is disclosed.
- **Level II information**: is SnowBe Online Information with a moderate requirement for Confidentiality and/or moderate or limited risk of financial loss, legal liability, public distrust, or harm if this data is disclosed.
- **Level III information**: is SnowBe Online Information with a low requirement for Confidentiality [information is public] and/or low or insignificant risk of financial loss, legal liability, public distrust or harm if this data is disclosed.

Roles & Responsibilities

Chief Information Officer (CIO):

- Approves the policy and grants exceptions.
- Final authority for SDLC compliance.

Chief Information Security Office (CISO)

- Responsible for developing, maintaining, and enforcing the SDLC.
- Ensures SDLC alignment with information security policies.

SDLC Review Committee:

- Reviews and approves exception requests.
- Ensures that exemptions do not undermine SDLC standards.

Development Team (Dev Team):

- Must follow SDLC standards in their work.
- Responsible for separating environments and proper documentation.

Security Team / IT Security Staff:

- Reviews and implements secure practices in each SDLC phase.
- Ensures Level I data is only handled by KU IT staff.

Employees (General Faculty, Staff, Students):

- Must comply with the policy when engaging in system or software development.
- Subject to disciplinary action if non-compliant.

Policy

SnowBe Online Information Technology is responsible for developing, maintaining, and participating in a Systems Development Life Cycle (SDLC) for SnowBe Online system development projects. All entities at SnowBe engaged in systems or software development activities must follow the SnowBe Online SDLC. This SDLC is detailed in the SnowBe Online Systems Development Life Cycle (SDLC) Standards document.

Additionally, the following apply:

- All software developed in-house which runs on production systems must be developed according to the SnowBe Online SDLC Standards. At a minimum, a 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 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, as defined by the SnowBe Online Data Classification and Handling Policy, must be developed and maintained solely by SnowBe Online Information Technology. Other development work involving Level II and Level III information may be done outside of SnowBe IT, provided the SnowBe Systems Development Life Cycle (SDLC) Standards are followed.

Exceptions/Exemptions

Any exceptions to this policy must be documented and approved by the Chief Information Security Officer (CISO). Exceptions may be granted only for business-critical needs where compliance with this policy would significantly hinder operational performance, provided there is an alternative security mitigation in place.

Enforcement

Violations of this Security Maturity Policy will result in disciplinary actions, which may include but are not limited to verbal or written warnings, suspension, termination of employment, or legal action, depending on the severity of the violation.

- Faculty and staff who violate this SnowBe Online policy may be subject to disciplinary action for misconduct and/or performance based on the administrative process appropriate to their employment.
- Faculty and staff may also be subject to the discontinuance of specified information technology services based on policy violations.

Regular audits and monitoring will be conducted to ensure compliance, and employees are encouraged to report any suspected security incidents or policy breaches to the IT Security team immediately. IT audits will be conducted monthly at the discretion of the IT manager. The senior IT Manager will summarize the audit findings monthly and present them to the CISO.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
1.0	March 24, 2025	Daphnie Bruno		Created SDLC Policy Document

Citations

- Grammarly, Inc. (n.d.). *Grammarly: Free writing assistant*. Retrieved from https://www.grammarly.com Used to correct grammar errors and spelling errors.
- **NIST**: National Institute of Standards and Technology. (n.d.). *NIST Cybersecurity Framework*. Retrieved from https://www.nist.gov/cyberframework
- Systems Development Life Cycle (SDLC) Policy – University of Kansas: