

SNOWBE ONLINE

System Development Life Cycle (SDLC)

Your name: James Ingram, Thomas Trippe, John Bays, Jose Rosario

<TEMPLATE> - Version 1

#DATE:3-26-2025

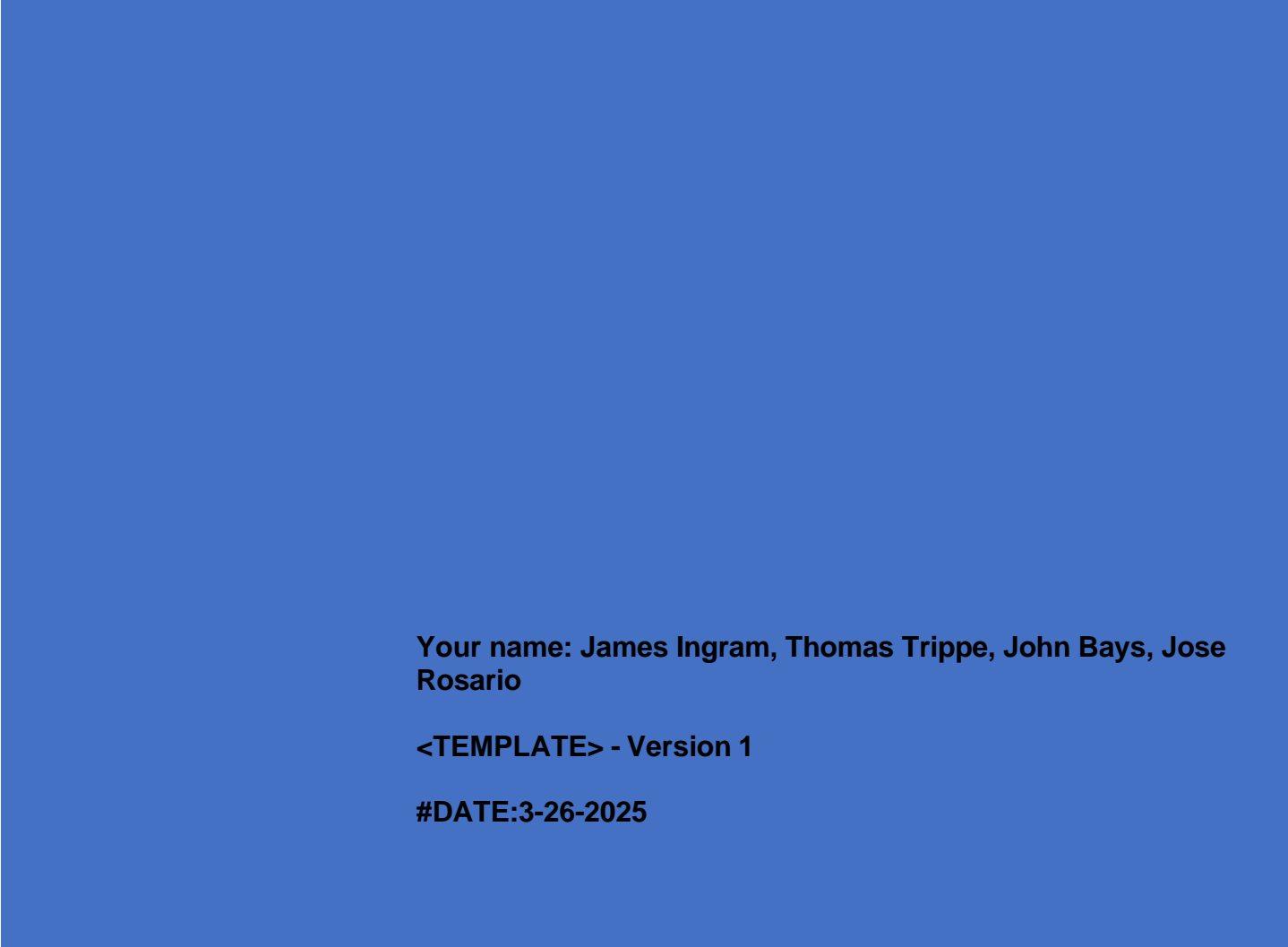


Table of Contents

PURPOSE2

SCOPE2

DEFINITIONS2

ROLES & RESPONSIBILITIES2

POLICY.....2

EXCEPTIONS/EXEMPTIONS3

ENFORCEMENT3

VERSION HISTORY TABLE3

CITATIONS.....4

Purpose

The purpose of this policy is to establish standard procedures for the development and management of systems at SnowBe, ensuring that security and risk management are integral to the system development life cycle.

Scope

This policy applies to all employees, contractors, and third-party service providers involved in the development, acquisition, maintenance, or management of systems used within SnowBe.

Definitions

System Development Life Cycle (SDLC): A structured process that outlines the steps involved in developing, deploying, and maintaining systems within an organization.

Risk Assessment: The process of identifying, evaluating, and prioritizing risks associated with potential threats to system security.

Roles & Responsibilities

Project Managers: Oversee the SDLC process and ensure adherence to this policy.

Developers: Responsible for building systems according to the project's specifications and conducting security testing.

Quality Assurance Team: Conduct thorough testing, including security assessments, to ensure system integrity.

Chief Information Security Officer (CISO): Approves any deviations from this policy and ensures compliance with security standards.

Policy

All systems developed, maintained, or acquired by SnowBe must adhere to the following SDLC phases:

1. **Planning:** Identify business requirements and assess risks.
2. **Analysis:** Gather detailed requirements and define security needs.
3. **Design:** Create system architecture, integrating security features.
4. **Development:** Build the system, focusing on security testing.
5. **Testing:** Perform thorough testing and vulnerability assessments.

- 6. Implementation: Deploy the system and ensure user training.
- 7. Maintenance: Update systems regularly and document all changes.

Exceptions/Exemptions

Requests for exceptions or exemptions to this policy must be documented and submitted to the CISO for approval, outlining the specific rationale and risks associated.

Enforcement

Violations of this policy may result in disciplinary actions, including termination or legal consequences. Compliance will be monitored continuously.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
1	03-26-2025	James Ingram		Initial Policy Creation

<Template Policy> – V 1.0

Status: ☒ Working Draft ☐ Approved ☐ Adopted

Document owner:

DATE

Citations

National Institute of Standards and Technology (NIST) guidelines.
ISO/IEC 27001 Information security management systems.