SNOWBE ONLINE SP18

System Development Lifecycle Policy

Danielle Williams

SP1 - Version # 1

DATE: December 21, 2024

Table of Contents

Purpose

The purpose of an SDLC methodology is to provide IT Project Managers with the tools to help ensure successful implementation of systems that satisfy SnowBe strategic and business objectives. The documentation provides a mechanism to ensure that executive leadership, functional managers and users sign-off on the requirements and implementation of the system. The process provides SnowBe Project Managers with the visibility of design, development, and implementation status needed to ensure delivery on time and within budget.

Scope

This Guideline applies to all major application projects, both new applications and upgrades of existing applications.

Definitions

NIST 800-160 v1 – documentation that establishes principals, concepts, and tasks for engineering secure systems.

Roles & Responsibilities

Project Manager – The project manager is responsible for overseeing the overall project from the analysis phase to the disposal phase. The PM is responsible for budgeting, planning, team coordination and communication as well as communicating project progress to the necessary parties.

Quality Assurance – Quality Assurance is responsible for testing developed systems during and after development. They are to report and errors or bugs to send the system back into the development phase.

Developers – Responsible for creating source code needed for system development.

Policy

This System Development Lifecycle(SDLC) policy aims to provide a framework for developing quality systems using an identifiable, measurable, and repeatable process based on activities from NIST 800-160 v1 Documentation and the nine phases of the SDLC. It will be used to establish a project management structure to ensure that each system development project is effectively managed throughout it's lifecycle. While not every project will require that the phases be subsequently executed and ay be tailored to accommodate the unique aspects of the project. While specific process and activities have been chosen with SnowBe's security and business needs in mind, project managers may chose the most appropriate tasks from each activity to meet project goals.

Analysis Phase

The analysis phase begins when management determines that it is necessary to enhance a business or security process through the application of information technology. To make this determination, management will perform the appropriate operational, economic, technical, and human factor feasibility studies. The following processes and tasks are recommended to meet these goals:

AQ-1 Prepare for the security aspects of the acquisition
SN-2 Define Stakeholder project needs
SN-3 Develop operational and other lifecycle concepts
SR-2 Define System Requirements
AR-3 Develop security models and security views of candidate architectures
SA-2 Perform the security aspects of the system anaylsis

Planning Phase

The planning phase will determine the projects operational and functional goals as well as user requirements. All of the necessary features, functions, and customizations for the system will be defined. Potential problems will be prematurely diagnose. Management will define security needs as well as a system to meet emerging needs or a new system if necessary. The following process and tasks are recommended to meet these goals:

AQ-1 Prepare for the security aspects of the acquisition
LM-1 Establish the security aspects of the process
LM-2 Assess the security aspects of the process
PM-1 Define and authorize the security aspects of projects
HR-1 identify systems security engineering skills
QM-1 Plan security quality management
KM-1 Plan Security Knowledge Management
PL-1 Define the security Aspects of the project
PL-2 Plan the security aspects of the projects and technical management
PA-1 Plan for the security aspects of project assessment and control
RM-1 Plan Security Risk Management
CM-1 Plan for the security aspects of configuration identification
IM-1 Prepare for the security aspects of information management
MS-1 Prepare for security measurement
QA-1 Prepare for security quality assurance
BA-1 Prepare for the security aspects of business or mission analysis
SN-1 Prepare for stakeholder protection needs and security requirements definition
SR-1 Prepare for system requirements definition
AR-1 Prepare for architecture definition from the security viewpoint
DE-1 Prepare for security design definition
DE-3 Assess the alternatives for obtaining security-relevant systems
SA-1 Prepare for the security aspects of system analysis
IP-1 Prepare for the security aspects of implementation
IN-1 Prepare for the security aspects of integration
VE-1 Prepare for the security aspects of verification
TR-1 Prepare for the security aspects of transition
VA-1 Prepare for the security aspects of Validation

OP-1 Prepare for secure operation
MA-1 Prepare for the security aspects of maintenance
DS-1 Prepare for the security aspects of disposal

Design Phase

The project team will develop a blueprint for the project in this phase. They will identify cost, necessary resources and timeframes necessary to complete the project. Details of the project features as well as user requirements will be both defined and designed in this phase. The development team will produce architect samples of the system. If any trainings are needed to complete the project, the team will design them, or find the appropriate materials necessary in this phase. Future maintenance will be determined as well as operation necessary to complete the system development. The following processes and tasks are recommended to meet these goals.

LM-1 Establish the security aspects of the process
IF-1 Establish the secure Infrastructure
HR-2 Develop systems security engineering skills
CM-1 Plan for the security aspects of configuration identification
BA-2 Define the security aspects of the problem or opportunity space
BA-3 Characterize the security aspects of the solution space
SR-2 Define system security requirements
AR-2 Develop Security viewpoints of the architecture
AR-3 Develop security models and security views of candidate architectures
AR-4 Relate security views of the architecture to the design
AR-1 Prepare for architecture definition from the security viewpoint
DE-2 Establish security design characteristics and enablers for each element

Development Phase

In this phase of the lifecycle, the development team will develop the system. The developer will began to write and optimize code. The previous design is realized, any necessary components are purchased, programmed, developed, configured, tested, or otherwise constructed. The following processes and tasks are recommended to meet these goals.

AQ-2 Advertise the acquisition and select the supplier to conform with the security aspects of the acquisition
AQ-3 Establish and maintain the security aspects of agreements
SP-2 Respond to a solicitation
SP-3 Establish and maintain the security aspects of agreements
SP- 4 Execute the security agreements
LM- Improve the security aspects of the project
HR-2 Develop systems security engineering skills
QM-3 Perform security quality management corrective and preventative actions
PL-3 Activate the security aspects of the project
PA-3 Control the security aspects of the project
DM-3 Make and manage security decisions

RM-2 Manage the security aspects of the risk profile
RM-4 Treat security risks
CM-2 Perform the security aspects of configuration identification
CM-3 Perform the security configuration change management
IM-2 Perform the security aspects of information management
MS-2 Perform Security Management
QA-5 Treat security incidents and problems
SN-3 Develop the security aspects of operational and other lifecycle concepts
SR-2 Define system security requirements
AR-5 Select candidate architecture
VE-2 Perform security focused verification
OP-4 Support Security needs of customers

Testing Phase

In this phase the users will began to test the developed system in preparation of deployment. The QA team will be responsible for running test that identify problems in the design(bugs or errors) or areas for improvement. SnowBe development and security teams will also test and validate all security controls and secure software. The following processes and tasks are recommended to meet these goals.

AQ-3 Establish and maintain the security aspects of agreements
PA-2 Assess the security aspects of the project
QA-2 Perform product or service security evaluations
QA-3 Manage quality assurance security records and reports
SN-5 Analyze Stakeholder security requirements
SA-2 Perform the security aspects of system anaylsis
VE-2 Perform security focused verification
VA-2 Perform security-focused validation
VA-3 Manage results of security focused validation

Deployment Phase

The developed and tested system will be deployed to production in this phase. The following processes and tasks are recommended to meet these goals

AQ-5 Accept the product or service
SP-5 Deliver and support the security aspects of the product or service
IF-1 Establish the secure infrastructure
PM-1 Define and authorize the security aspects of projects
HR-3 Acquire and provide systems security engineering skills to projects
KM-2 Share security knowledge and skills throughout the organization
KM-3 Share security assets throughout the organization
KM-4 Manage security knowledge, skills, and knowledge assets
PL-3 Activate the security aspects of the project

PA-3 Control the security aspects of the project
CM-6 Perform the security aspects of release control
SN-4 Transform stakeholder protection needs into security requirements
IP-2 Perform the security aspects of implementation
IN-2 Perform the security aspects of integration
TR-2 Perform the security aspects of transition
OP-2 Perform Secure operation

Maintenance Phase

SnowBe believes that continuous maintenance is necessary to ensure optimal systems, and so any systems owned by SnowBe will undergo continuous enhancements and/or modifications. Any components, hardware or software that need to be replaced or updated should be managed in this phase. SnowBe's systems will be constantly monitored for performance metrics to ensure it is meeting initial goals defined in the analysis phase. The following processes and tasks are recommended to meet these goals.

AQ-4 Monitor the security aspects of agreements
IF-2 Maintain the security infrastructure
KM-4 Manage security Knowledge, skills, and knowledge assets
DM-3 Make and manage security decisions
RM-2 Manage the security aspects of the risk profile
Rm-5 Monitor Security risk
CM-4 Perform the security configuration status accounting
QA-4 Manage quality assurance security records and reports
BA-5 Manage the security aspects of business or mission analysis
SN-6 Manage stakeholder protection needs and security requirements definition
SR-4 Manage security requirements
AR-6 Manage the security view of the selected architecture
DE-4 Manage the security design
SA-3 Manage the security aspects of system analysis
IP-3 Manage results of the security aspects of implementation
IN-3 Manage results of the security aspects of integration
VE-3 Manage results of security focused verification
TE-3 Manage results of the security aspects of transition
VA-3 Manage results of security-focused validation
OP-3 Manage results of secure operation
MA-4 Manage results of the security aspects of maintenance and logistics

Evaluation Phase

During this phase of the development lifecycle, the project management team will determine if the system meets the initial requirements and objectives. If any changes are needed, project management should follow SnowBe's Change Control Management Policy(SP17). The following processes and tasks are recommended to meet these goals.

LM-2 Assess the security aspects of the process
PM-2 Evaluate the security aspects of the portfolio projects
QM-2 Assess security quality management
PA-2 Assess the security aspects of the project
DM-2 Analyze the security aspects of decision information
RM-3 Analyze security risk
CM-5 Perform configuration evaluation
BA-4 Evaluate and select solution classes
SN-5 Analyze stakeholder security requirements
SR-3Analyze system security in system requirements
IP-3 Manage results of the security aspects of implementation
IN-3 Manage results of the security aspects of integration
VE-3 Manage results of security focused verification
TE-3 manage results of the security aspects of transition
VA-3 Manage results of security-focused validation
OP-3 Manage results of secure operation

Disposal Phase

This is the final phase of the SDLC and involves discarding system information, hardware and software. SnowBe must adhere to specific regulations regarding the strage and disposal of certain data. To adhere to these regulations in this phase, the development team will appropriately move, archive, or discard, or destroy data. The following processes and tasks are recommended to meet these goals.

PM-3 Terminate Projects
DS-2 Perform the security aspects of disposal
DS-3 Finalize the security aspects of disposal

Exceptions/Exemptions

Any exceptions or exemptions to the security policies, standards, and procedures outlined in this plan must be documented via email and approved by the Network Administrator and the relevant department manager. Exceptions will be granted on a case-by-case basis and will be subject to periodic review and re-evaluation.

Enforcement

Any exceptions or exemptions to the security policies, standards, and procedures outlined in this plan must adhere to the following criteria;

- All requests must be documented in detail, including the specific reasons for the exception, potential risks involved, and any compensating controls implemented to mitigate those risks.
- Approval must be obtained from the Network Administrator and the relevant department manager, with final oversight and approval by the Director or Manager of Information Technology.

- All exceptions will be granted on a case-by-case basis, documented in a centralized exception tracking system, and reviewed at least quarterly by the Incident Response Team (IRT) to assess any changes in risk or compliance requirements.
- Exceptions that pose significant risks or affect regulatory compliance must be reported to the Compliance Officer for additional review.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
1	12/21/2024	Danielle Williams		Added policy purpose, scope, definitions, roles and responsibilities, policy, exception/exemptions, as well as enforcement policy.

Citations

Michigan tech - https://www.mtu.edu/it/security/policies-procedures-guidelines/information-security-program/system-development-lifecycle/

Full sail lecture slides - https://online.fullsail.edu/class_sections/161943/modules/800867/activities/4602566

NIST 800-160 documentation - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1.pdf