



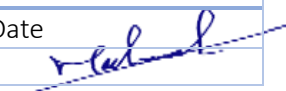
# Secure Software Development

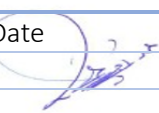
Doc. Control Number	Version
SNL-23	0.2



## Document Reference

Item	Description
Title	Secure Software Development
Department	Cybersecurity department
Version No	0.2
Status	Draft
Type	DOCX
Publish-Date	6 August 2024
Revision-Date	6 August 2025

Authors		
Name	Department	Signature/Date
Muhaned Kamal Ali	Cybersecurity - I. S Specialist	8/6/2024 

Reviewed by		
Name	Department	Signature/Date
Yasir Awad	Head of Cyber Security Department	8/6/2022 

Approved by		
Name	Department	Signature/Date
Abdullah Al Shuhail	V.P	8/6/2022 

## Control-Page

Document Amendment Record			
Version-No	Date	Prepared-by	Explanation
0.1	10 August 2023	Muhaned Ali	First Release
0.2	6 August 2024	Muhaned Ali	The policy has been reviewed



## Contents

1. Purpose .....	4
2. Scope.....	4
3. Standards .....	4
4. Roles and Responsibilities.....	5
5. Policy Compliance .....	5

## 1. Purpose

The purpose of this standard is to provide cybersecurity requirements based on best practices and standards related to software and application development and protection from internal and external threats in SNLC to reduce cyber risks and protect them from internal and external threats by focusing on the primary objectives of protection: confidentiality, integrity, and availability of information.

## 2. Scope

This standard covers all SNLC's software, application, information, and technology development activities, projects, and practices, and is applicable to all SNLC personnel.

## 3. Standards

1 Secure Code Development	
Objective	Provide cybersecurity requirements to ensure the protection of software and application development activities and cybersecurity controls to protect the software being developed.
The potential risks	Insecure application development can create vulnerabilities that can be exploited to threaten the confidentiality, integrity, and availability of SNLC data, and affect its workflow.
Required procedures	
1-1	A Secure Software Development Life Cycle (SSDLC) process shall be developed and implemented.
1-2	A DevSecOps methodology and process shall be developed and adopted.
1-3	Cybersecurity requirements shall be provided in the initial phases of software development and incorporated into the SSDLC process.
1-4	Cybersecurity testing shall be conducted in the testing phases of software development and incorporated into the SSDLC process.
1-5	A secure environment shall be designed and configured for development, testing, and quality assurance purposes.
1-6	Mitigations to the Open Web Application Security Project (OWASP) Top 10 Application Security Risks shall be implemented for critical systems and applications.
2 Source Code Repository	
Objective	Provide cybersecurity controls to ensure source code, libraries, and source code repository are protected.
The potential risks	If source code and libraries are not adequately protected, SNLC source code can be compromised, tampered with, or unauthorized access.
Required procedures	
2-1	A secure source code repository that has authentication, version control and logging enabled shall be used.
2-2	Deny access to source code and source code repository for anyone except application developers and owners.
2-3	A unified version control numbering scheme shall be used to reflect when updated versions of the software are installed.
3 Secure Code Review and Testing	
Objective	Provide assurance regarding the application of cybersecurity controls to secure application development and detection of software vulnerabilities, vulnerabilities, and problems.

The potential risks	SNLC can be exposed to significant security risks If source code and code development activities are not regularly tested and reviewed for vulnerabilities, misconfigurations, and vulnerabilities, SNLC can be exposed to significant security risks.
<b>Required procedures</b>	
3-1	A secure code review process shall be conducted regularly for internally developed web applications.
3-2	Static and dynamic analysis tools shall be applied to verify that secure coding practices are being adhered to for internally developed software.
3-3	Conduct a secure code review process regularly for all applications developed by third parties specifically for SNLC.
3-4	Security controls of new internally developed applications shall be reviewed and approved prior to application deployment into the production environment.
3-5	Cybersecurity compliance testing shall be conducted for software against SNLC's cybersecurity policies and standards prior to deployment into a production environment.

#### 4. Roles and Responsibilities

- 4.1 The sponsor and owner of the policy document: Head of Cyber Security Department.
- 4.2 Policy reviews and update: Cyber Security Department.
- 4.3 Policy implementation: IT Department

#### 5. Policy Compliance

##### 5.1 Compliance Measurement

The Infosec team will verify compliance with this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

##### 5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

##### 5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.