Cybersecurity in Project Management

Doc. Control Number	Version
SNL-07	0.3

Document Reference

Item	Description
Title	Cybersecurity in Project Management
Department	Cybersecurity department
Version No	0.3
Status	Draft
Type	DOCX
Publish-Date	17 May 2024
Revision-Date	17 May 2025

Authors		
Name	Department	Signature/Date
Muhaned Kamal Ali	Cybersecurity - I. S Specialist	5/17/2024

Reviewed by		
Name	Department	Signature/Date
Yasir Awad	Head of Cyber Security Department	5/18/2024

Approved by		
Name	Department	Signature/Date
Abdullah Al Shuhail	V.P	5/18/2024

Control-Page

Document Amendment Record			
Version-No	Date	Prepared-by	Explanation
0.1	1 August 2022	Muhaned Ali	First Release
0.2	17 May 2023	Muhaned Ali	The policy has been updated.
0.3	17 May 2024	Muhaned Ali	The policy has been reviewed.

Contents

1. Purpose

It's important to integrate information security into project management because this provides the opportunity for SNLC to ensure that information security risks are identified, evaluated, and addressed as part of the project management.

2. Scope

This policy applies to all SNLC short, medium, and long-term projects as well as internal and external projects.

3. Policy

3.1 Cybersecurity requirements shall be integrated in every project and in each phase of the project.

3.2 Cybersecurity personnel shall be defined as part of the project team.

3.3 Cybersecurity objectives shall be included in the project objectives.

3.4 It is important to maintain an acceptable risk profile during a project when people, information assets, and situations may be changing.

3.5 The risk register should consider any changes that could affect information security at all stages of the project and within the deliverables.

3.6 All staff affected by project risks should be made aware of the associated controls, including when they are to be effective; regardless of whether they are part of the project team or not.

4. Guidelines

4.1 Include information security objectives in project objectives.

4.2 Determine roles and responsibilities associated with information security so that everybody knows and executes what is necessary.

4.3 Perform a risk assessment in an early stage of the project.

4.4 Carry out treatment of the identified risks and implement security measures.

4.5 Make the information security policy an indispensable part of all stages of the project.

4.6 Train the project team on information security policies and controls to increase awareness and competence so that you can reduce the occurrence of incidents and non-compliances.

4.7 Have confidentiality agreements with suppliers working on the project and inform them about relevant policies and procedures.

4.8 If the project is in collaboration with a vendor, configure scheduled access reviews with the vendor team.

4.9 Conduct reviews and audits to measure the effectiveness of implementation and analyze results.

4.10 Take corrective or improvement actions where needed.

4.11 At the closing phase of projects, save and store all data and documents with proper safeguards. Check the access rights of team members. When these activities are performed improperly, it can be a catalyst for unauthorized disclosure of sensitive and priceless business information.

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.