




Bring Your Own Device (BYOD) Policy


Doc. Control Number	Version
SNL-10	0.3



Document Reference

Item	Description
Title	Bring Your Own Device (BYOD) Policy
Department	Cybersecurity Department
Version No	0.3
Status	Draft
Type	DOCX
Publish-Date	5 March 2024
Revision-Date	5 March 2025

Authors		
Name	Department	Signature/Date
Muhaned Kamal Ali	Cybersecurity - I. S Specialist	5/3/2024 

Reviewed by		
Name	Department	Signature/Date
Yasir Awad	Cybersecurity -Manager	5/3/2024 

Approved by		
Name	Department	Signature/Date
Abdullah Al Shuhail	V.P	5/3/2024 

Control-Page

Document Amendment Record			
Version-No	Date	Prepared-by	Explanation
0.1	10 May 2022	Muhaned Ali	First Release
0.2	24 May 2023	Muhaned Ali	The Policy has been updated
0.3	5 March 2024	Muhaned Ali	Policy has been reviewed



Contents

1. Overview	4
2. Scope.....	4
3. Policy.....	4
4. Cyber Security Requirements for Personal Device (BYOD).....	4
5. Policy Compliance	5

1. Overview

Mobile computing is an increasing part of everyday life, as devices become smaller and more powerful the number of tasks that can be achieved away from the office grows. However, as the capabilities increase so do the risks. Security controls that have evolved to protect the static desktop environment are easily bypassed when using a mobile device outside of the confines of an office building.

Mobile devices include items such as:

- Laptops
- Notebooks
- Tablet devices
- Smartphones

2. Scope

This policy applies to all systems, people and processes that constitute the organization's information systems, including board members, directors, employees, suppliers and other third parties who have access to SNLC systems.

3. Policy

- 3.1 Data and information stored on personal devices (BYOD) must be protected by using appropriate security controls to restrict access to such information, and to prevent unauthorized personnel from accessing or viewing it.
- 3.2 Individuals must not use their own devices to hold and process company information unless they have submitted a request to do so.
- 3.3 The software of users' devices and mobile devices, including operating systems, programs, and applications, must be updated, and provided with the latest update and fix packages in accordance with the company's approved update and fix management policy.
- 3.4 Configuration and hardening of user devices and mobile devices must be applied in accordance with cybersecurity standards.
- 3.5 The storage media of users' devices and important and sensitive mobile devices that have advanced powers must be encrypted according to the company's approved encryption standard.
- 3.6 Users' devices, mobile devices, and personal devices (BYOD) with out-of-date or expired software (including operating systems, software, and applications) should not be allowed to connect to the SNLC network to prevent security threats arising from expired software that is not protected by update and hotfix packages.
- 3.7 Personal devices (BYOD) that are not equipped with the latest security software should be prevented from connecting to SNLC's network to avoid cyber risks leading to unauthorized access, malware entry, or data leakage.
- 3.8 The Personal Device Security Policy shall be reviewed, measured, and optimized annually, and changes documented and approved.

4. Cyber Security Requirements for Personal Device (BYOD)

- 4.1 Mobile devices, Personal devices must be managed centrally using the Mobile Device Management "MDM" system.
- 4.2 Data and information of SNLC stored on BYOD must be segregated and encrypted.
- 4.3 In case of the device being lost or stolen, the owner must inform the IT Support Desk as soon as possible, giving details of the circumstances of the loss and the sensitivity of the business information stored on it. SNLC reserves the right to remote wipe the device where possible

as a security precaution. This may involve the deletion of non-business data belonging to the device owner.

- 4.4 Securely delete the company's information after the completion of the associated job function and when the information is no longer necessary.
- 4.5 Upon leaving the company, the device owner must allow the device to be audited and all business-related data and applications removed.

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.