**Bring Your Own Device (BYOD)Policy & Procedure**

**Version Control:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Document Name** | **Version** | **Approved By** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Contents

1. Purpose .................................................................................................................. 3

2. Document Control ................................................................................................. 3

2.1 Ownership ...................................................................................................... 3

2.2 Applicability .................................................................................................... 3

2.3 Maintenance …................................................................................................ 3

2.4 Document Roles and Responsibilities ............................................................. 3

3. Scope ...................................................................................................................... 4

4. Policy ...................................................................................................................... 4

5. Monitoring and Access .......................................................................................... 5

Purpose

The purpose of this policy is to establish security requirements to provide controlled access on employee- owned devices to SNS GROUP information resources, to prevent unauthorized access, disclosure, deletion, or modification and to ensure its continued availability as well as satisfy compliance with any relevant policies and regulatory requirements.

Document Control

Ownership

This information security Governance document is owned by the IT Manager – Corporate Governance, Risk, and information security.

Applicability

This Information Security Governance Framework is applicable to all the roles mentioned in the document and information security staff, suppliers and third parties who are directly or indirectly employed by SNS GROUP.

Maintenance

This document will be maintained by a Senior Information Security Consultant in a manner delegated by the document owner and will follow the Change Management Process as documented within - Change Management Process. This document will be reviewed regularly and at least annually.

Document Roles and Responsibilities

An effective Information Security Governance Framework is a living document should be updated and maintained as circumstances and business requirement change. Specific roles associated with the maintenance and management should be specified to ensure it remains up to date. The roles and responsibilities should be assigned, must be documented in Table 1: Document Roles and Responsibilities.

* Maintain Register: Ensures the document register is updated following changes
* Prepare/ Update/ Amend: Ensures the document is updated and amended as required
* Review: Reviews the document and agrees final version prior to approval process
* Endorse: Reviews the document and endorses prior to submission for approval
* Approve: Signs off on the document prior to publication.
* Publish: Ensures the document is appropriately circulated within the SNS GROUP

***Table 1: Document Roles and Responsibilities***

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
| Prepare/ |
| Maintain |
|  | Update/ | Review | Endorse | Approve | Publish |
| Register |
| Amend |
|  |  |  |  |
|  |
|  |
| Owner |  | YES |  |  |  |  |
| Information Security Manager |  |  | YES |  |  |  |
| Department head | YES |  | YES |  |  | YES |
| CEO |  |  |  | YES |  |  |
| BOD |  |  |  |  | YES |  |

Scope

This policy covers all the employees, contractors, suppliers, vendors, etc. who use their mobile devices and other devices to access SNS GROUP information resources. All relevant SNS GROUP policies should apply to all SNS GROUP employees.

Employee-owned Mobile Computing Device is any type of device that can be easily moved and has the capability of collecting, storing, transmitting, and processing electronic data or images e.g. tablets, smartphones, mobile phones, and laptops.

4. Policy

1. Business information shall be isolated from personal information by appropriate means (e.g. containerization or controls through mobile devices management solution).   
   Mobile devices shall only install applications from authorized sources.
2. Mobile device management (MDM) solutions shall be used for the administration of mobile devices to apply access controls to the device and business container and encryption mechanisms on the personal device (to ensure secure transmission and storage).
3. Remote data wiping software shall be used which has been approved and supplied by SNS GROUP to mitigate the risk if the device is lost, modified (jailbreaking), the employee terminates his or her employment, data, or policy breach is detected, and virus or security threat is detected.
4. Protection shall be in place to avoid the unauthorized access to, or disclosure of the information stored and processed by these facilities using appropriate and approved cryptographic techniques.
5. Devices without having standards configurations shall not be allowed to be connected to the SNS GROUP network.
6. SNS GROUP shall ensure that mobile computing devices are configured with approved and properly
7. updated software-based security mechanisms including anti-virus, anti-spyware, firewalls, etc. Users shall not bypass or disable these security mechanisms under any circumstances.
8. Strong password policies shall be adhered for all mobile computing devices depending on the
9. device.
10. Following training/awareness shall be provided to staff using mobile computing facilities to raise
11. awareness about the corresponding risks:
    1. Awareness session for Bring Your Own Device
    2. Awareness session for a Mobile Device Management Solution
    3. Awareness session for current risk trends for Mobile usage
12. SNS GROUP employees may use their mobile devices to access the defined company-owned resources
13. e.g., internet, e-mail, contracts, meeting reminders, calendars, etc.
14. SNS GROUP has provided a separate network facility for internet connectivity of personal mobile devices: any unauthorized connectivity of personal mobile devices with SNS GROUP internal network is strictly prohibited.
15. Any access to the internal network from personal devices should be controlled and restricted based
16. on the job requirements and must be monitored.
17. SNS GROUP reserves the right to disconnect devices or disable services without notification.
18. SNS GROUP confidential data, except communicated in emails, must never be stored on the mobile device
19. unless it has approval from the data owner and is being encrypted by strong encryption.
20. Users should not store emails older than one week on their mobile devices.
21. To prevent unauthorized access, devices shall be password protected.
22. The device must lock itself with a password or PIN if it’s idle for five minutes.
23. The employee and contractors are expected to always use his or her devices in an ethical manner and adhere to the SNS GROUP acceptable use policy as outlined.
24. Individuals who make use of BYOD must take responsibility for their own device and must ensure:

a. To familiarize themselves with their mobile devices and their security features so that they can ensure the safety of SNS GROUP information resources.

b. Invoke the relevant security features.

c. Maintain the device themselves ensuring it is regularly patched and upgraded.   
d. Prevent theft and loss of data.

e. Keep information confidential where appropriate.

f. Take responsibility for any software they download onto their device.

5. Monitoring and Access

SNS GROUP will not routinely monitor personal devices. However, it does reserve the right to:

1. Prevent access to a particular device from either the wired or wireless networks or both.
2. Prevent access to a particular system.
3. Take all necessary and appropriate steps to retrieve information owned by the SNS GROUP.