Procedure for Managing Lost or Stolen Devices

Doc. Control Number	Version
SNL-42	0.2

Document Reference

Item	Description
Title	Procedure for Managing Lost or Stolen Devices
Department	Cybersecurity department
Version No	0.2
Status	Draft
Type	DOCX
Publish-Date	23 May 2024
Revision-Date	23 May 2025

Authors		
Name	Department	Signature/Date
Muhaned Kamal Ali	Cybersecurity - I. S Specialist	5/23/2024

Reviewed by		
Name	Department	Signature/Date
Yasir Awad	Head of Cyber Security Department	5/23/2024

Approved by		
Name	Department	Signature/Date
Abdullah Al Shuhail	V.P	5/23/2024

Control-Page

Document Amendment Record			
Version-No	Date	Prepared-by	Explanation
0.1	23 May 2023	Muhaned Ali	First Release
0.2	23 May 2024	Muhaned Ali	The document has been reviewed

Contents

1. Overview

Mobile devices are a key part of our ability to process information in a flexible, location-independent way. But the level of access available to such devices also represents a significant risk to the company if they are misplaced or stolen.

Appropriate access control and, in many cases encryption, must be in place so that the risk of unauthorized access to lost or stolen devices is reduced. However, the additional steps described in this procedure will lessen the risk still further, whilst allowing the possibility of recovering the device in some circumstances.

The document Information Security Incident Response Procedure sets out a process of containment, eradication, recovery, and notification with respect to information security incidents, which may apply to the incidents covered by this procedure, depending on the severity and information involved. This procedure may form part of the containment and eradication steps of that process.

Note - This procedure may remove all data on the device including contacts and emails. In most cases this information will have been backed up as part of SNLC procedures and these backups will be used to set up a replacement device with the same configuration as before.

2. Scope

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

3. Procedure for managing lost or stolen devices.

- Prerequisites

  Before starting the procedure, the following prerequisites must be in place:

  - The device has been formally reported as lost or stolen by the owner and a service desk incident record has been created.
  - There is no reasonable prospect of recovery by the owner.
  - The permission of the owner of the device has been obtained to wipe the contents of it.
  - Relevant procedures for responding to information security incidents involving potential data loss have been engaged and followed.

- Timing and scheduling

  This procedure should be carried out as soon as it is decided that the device is lost and cannot be recovered.

- Procedure steps

  1- Obtain full details of the device in question so that it can be accurately identified. Depending on the device, this may consist of:
     - Device name
     - Serial number
     - Telephone number
     - IMEI number
     - MAC address

  2- Identify the appropriate Mobile Device Management (MDM) system used to manage the device.

  3- Log on to the MDM system and locate the device within it.

  4- If appropriate and available, use location-tracking facilities and the ability to play a sound to locate the device.

5- If appropriate and available, use Lost Mode (or similar) to put a message on the device with a number to call to arrange for return of the device. It may be necessary to consult the relevant incident manager to check that this is advisable in the specific circumstances.
6- If the device is successfully recovered, a decision will be made by the incident manager about whether the device should be wiped anyway as a security precaution. This will depend on a judgement of the circumstances of the device's recovery (e.g., if it was found by the device owner at home or handed in to a by a stranger).
7- If the device can't be recovered, then select the appropriate device within the MDM system and click on "Erase device" (or equivalent e.g., Wipe) to delete all data on it.
8- Confirm that the operation has been completed successfully.
9- If the operation does not complete successfully and the device has not been erased (perhaps because it is switched off or there is no network connection to it), report this fact to the service desk and discuss next steps, which may include retrying on subsequent days until successful. It is important that an unsuccessful wipe is reported, as this may affect the legislative notifications required for the incident.

- Error handling
  The following common errors may occur during this procedure:

STAGE OF PROCEDURE	ERROR	POSSIBLE CAUSE	RECOMMENDED ACTION
Logging on to MDM system	Unable to log on	There are several relevant systems – make sure you are on the right one	Move to correct system

- Support and escalation
  If an error occurs which cannot be corrected using this procedure, support should be obtained using the following information:

SUPPORT PERSON	ROLE	EMAIL	HOURS AVAILABLE
Eng.Mohaned Ibrahim	IT Team	mid@saudinetlink.com	8am to 5pm on business days

- Auditing and logging
  When this procedure is run it should be recorded as a security incident on the service desk system (if not already recorded) and available logs of activity on the MDM system should be preserved.
- Monitoring
  Monitor the messages received as part of the procedure to ensure that the erase has been successful.