**Mobile Computing Policy**

**Security Classification: Restricted**

**Document Ref. ISMS12002**

**Version: 1.0**

**Draft 1**

**Document Author: Cybersecurity Unit**

**Document Owner: NCS-TMP**

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Change Number** | **Summary of Changes** |
| 1.0 | 30 Jan 24 | Draft 1 | Tailoring to NCS |
| 1.1 | Feb 24 | Draft 1 | IE Review |
| 1.2 | Feb 24 | Draft 1 | Legal Review |
| 1.3 |  | Draft 1 | Unit Sign-Off |
| 2.0 |  | Version 2 | Management Sign-off |

**Document Review**

|  |
| --- |
| **Date of Next Scheduled Review** |
| 29th January 2024 |

Distribution

|  |  |
| --- | --- |
| **Name** | **Title** |
| Bukola Omoniyi | Officer in Charge Project management |
| Abubakar Sadiq | Project Management |
| Oliver Nnona | Independent Expert |
| MJ Abubakar | Officer in Charge, Cybersecurity |
| Maduka Emelife | Independent Expert |
| Uche I Egolum | NCS Legal |

Approval

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Position** | **Signature** | **Date** |
|  |  |  |  |

**Contents**

[1 Introduction 6](#_Toc380568267)

[1.1 Risks Addressed 6](#_Toc380568268)

[1.2 Scope 6](#_Toc380568269)

[1.3 Related Documents 6](#_Toc380568270)

[1.4 Purpose 6](#_Toc380568271)

[2 Mobile Computing Policy 8](#_Toc380568272)

[2.1 General 8](#_Toc380568273)

[2.2 Physical Protection 8](#_Toc380568274)

[2.3 Access Controls 8](#_Toc380568275)

[2.4 Cryptographic Techniques 9](#_Toc380568276)

[2.5 Backups 9](#_Toc380568277)

[2.6 Virus Protection 9](#_Toc380568278)

[2.7 Network Connection 10](#_Toc380568279)

[2.8 Overlooking 10](#_Toc380568280)

# Introduction

## Risks Addressed

This document describes a control that was identified in [ISMS06004 Information Security Risk Treatment Plan](https://d.docs.live.net/69f2be528857fcc0/Documents/TMP/ISO%2027001%20Information%20security%20management%20systems/ISO-27001-2013-V5R1/06.%20Planning/ISMS06004%20Information%20Security%20Risk%20Treatment%20Plan.doc) to address the following risks:

|  |  |
| --- | --- |
| **Reference** | **Description of Risk** |
|  |  |
|  |  |
|  |  |

## Scope

This control applies to all systems, people and processes that constitute the PMO information systems, including management, employees, and other third parties who have access to PMO systems.

## Related Documents

The following policies and procedures are relevant to this document:

* [ISMS15001 Access Control Policy](https://d.docs.live.net/69f2be528857fcc0/Documents/TMP/ISO%2027001%20Information%20security%20management%20systems/ISO-27001-2013-V5R1/A9.%20Access%20control/ISMS15001%20Access%20Control%20Policy.doc)
* [ISMS12003 Remote working Policy](https://d.docs.live.net/69f2be528857fcc0/Documents/TMP/ISO%2027001%20Information%20security%20management%20systems/ISO-27001-2013-V5R1/A6.%20Organisation%20of%20information%20security/ISMS12003%20Teleworking%20Policy.doc)
* [ISMS15002 User Access Management Process](https://d.docs.live.net/69f2be528857fcc0/Documents/TMP/ISO%2027001%20Information%20security%20management%20systems/ISO-27001-2013-V5R1/A9.%20Access%20control/ISMS15002%20User%20Access%20Management%20Process.doc)
* [ISMS15003 Procedure for Remote Supplier Access to Systems](https://d.docs.live.net/69f2be528857fcc0/Documents/TMP/ISO%2027001%20Information%20security%20management%20systems/ISO-27001-2013-V5R1/A9.%20Access%20control/ISMS15003%20Procedure%20for%20Remote%20Supplier%20Access%20to%20Systems.doc)
* [ISMS15004 Procedure for the Reset of User Passwords](https://d.docs.live.net/69f2be528857fcc0/Documents/TMP/ISO%2027001%20Information%20security%20management%20systems/ISO-27001-2013-V5R1/A9.%20Access%20control/ISMS15004%20Procedure%20for%20the%20Reset%20of%20User%20Passwords.doc)
* [ISMS16001 Cryptographic Policy](https://d.docs.live.net/69f2be528857fcc0/Documents/TMP/ISO%2027001%20Information%20security%20management%20systems/ISO-27001-2013-V5R1/A10.%20Cryptography/ISMS16001%20Cryptographic%20Policy.doc)

## Purpose

Mobile computing is an increasing part of everyday life, as devices become smaller and more powerful, the number of tasks that can be achieved 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.

Mobile devices include items such as:

* Laptop and notebook computers
* Tablets
* Smartphones
* Wearable devices

The purpose of this policy is to set out the controls that must be in place when using mobile devices. It is intended to mitigate the following risks:

* Loss or theft of mobile devices, including the data on them.
* Compromise of classified information through observation by unauthorized persons.
* Introduction of malware to the network
* Loss of reputation

It is important that the controls set out in this policy are observed at all times in the use and handling of mobile devices.

# Mobile Computing Policy

## General

* Only mobile devices provided by the Nigeria Customs Service or the Project Management Office (PMO) should be used to hold or process classified information on behalf of the Nigeria Customs Service (NCS).
* Users must not use their personal devices for operational purposes.
* If users are required to make use of mobile equipment, they will be provided with an appropriate device(s) which will be configured to comply with the Service’s policies.
* Support will be provided by the Cybersecurity Unit who may at times need access to the device for problem resolution and maintenance purposes.

## Physical Protection

* Users must ensure that the device is transported in a protective case when possible and is not exposed to situations in which it may become damaged.
* Do not leave the device unattended in public view, such as in the back of a car or in a meeting room or hotel lobby.
* Do not remove any identifying marks on the device such as a Service asset tag or serial number.
* Ensure that the device is locked away when being stored and that the key is not easily accessible.
* Faults with the device must be logged with the ICT-Modernisation Unit.
* Do not add peripheral hardware to the device without the approval from the ICT-Modernisation Unit.
* The Office of the ACG ICT-Modernisation must be consulted before the device is taken out of the country.

## Access Controls

* Users will not hold classified information on the device unless this has been authorized and appropriate controls (e.g. encryption) put in place
* Do not keep access tokens, Personal Identification Numbers or other security items on the device.
* Ensure that the device screen locks after a short period of not being used and requires an access code or password to unlock it.
* Passwords used should be strong and difficult to guess.
* No unsecured logons (i.e., those that do not require a password should be set up on the device.
* The device is for operational use only; it must not be shared with family or friends or used for personal activities.
* User may be asked to return the device to the Service at any time for inspection and audit.
* Users must not install any unauthorised software on the device without consulting the ICT-Modernisation Unit first.
* Users must not change the configuration or setup of the device without consulting the ICT-Modernisation Unit first.

## Cryptographic Techniques

* Where possible, the device will be secured so that all the data on it is encrypted and so is only accessible if the password is known.
* If the device is supplied with encryption, do not disable it.

## Backups

* Changes to files held on the device may not be backed up on a regular basis if it is not connected to the corporate network for a period of time. Try to schedule some time in to achieve this on a regular basis.
* Do not make unencrypted backups of classified information.

## Malware Protection

* Where applicable, malware protection will be installed on the device by the Service.
* Ensure that the device is connected to the corporate network on a regular basis to allow the malware signatures to be updated.
* Do not disable malware protection on the device.

## Network Connection

* The device should not be connected to non-corporate networks such as wireless or the Internet unless a VPN (Virtual Private Network) is used.

## Overlooking

* When in public places, ensure that you site the device such that unauthorised people cannot view (or take photographs or video of) the screen.