Mobile Device Security Standard

Version No	2.4
Document Type	Standard
Parent Document	Group Information and Cyber Security Policy
Parent Framework	Information & Cyber Security RTF
Document Approver Name	Jamie Cowan
Document Approver Job Title	Head, ICS Risk Framework & Governance
Document Owner Name	Ibrahim Gathungu
Document Owner Job Title	Director, ICS Standards
Document Contact Name	Anna Kowal-Hughes
Document Contact Job Title	Assoc Dir, ICS Standards
Business Scope	All Businesses
Function Role	All Functions
Geography Scope	Global
Effective Date	16-Dec-24
Approval Date	4-Dec-24
Next Review Date	30-Nov-26

Table of Contents

1 INTRODUCTION AND SCOPE 4
1.1 Risks 4
1.2 Scope 4
2 ROLES & RESPONSIBILITIES 5
3 STANDARD REQUIREMENTS 6
3.1 Control Area: Management of Mobile Devices 6
3.2 Control Area: Access Management 6
3.3 Control Area: Mobile Devices access to Group Network 6
3.4 Control Area: Secure Configuration of Laptops 7
3.5 Control Area: Configuration of Group Owned Smartphones and Tablets 7
3.6 Control Area: Secure Configuration of Portable Storage Devices 7
3.7 Control Area: Employee owned Mobile Devices used for business purpose (BYOD) 8
4 INFORMATION & SUPPORT 9
4.1 General Information and Support 9
4.2 Reporting Non-Compliance 9
4.3 Breach of this Standard 9
5 GLOSSARY 9
6 REGULATORY / INDUSTRY REFERENCES 9
7 Appendix A – Version Control Table 9

Version Control Table

Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
Anna Kowal-Hughes **[ICS Standards]**	Editorial changes: 1. Document template updated in line with Template for Group Standards, V 7.0 2. Document references updated 3. Roles references updated in line with the new org structure	Non-material	Jamie Cowan Head, ICS Risk Framework & Governance	2.4	04-Dec-24	16-Dec-24

1 INTRODUCTION AND SCOPE

This Information and Cyber Security Standard defines the minimum set of requirements for the selection, application and configuration of Mobile Devices and Portable Storage controls in the Group.

The objective of this Security Standard is to ensure that Mobile Devices and Portable Storage Devices do not compromise the security of Information stored on or processed by them and prevent unauthorised access to Information in the event they are lost or stolen.

Mobile Devices include, but are not limited to:

- Laptops
- Tablets
- Smartphones
- Wearable Technology

Portable Storage Devices ["PSDs"] include, but are not limited to:

- Digital Cameras
- Sound recorders
- Secure Digital ["SD"] Cards
- External Universal Serial Bus ["USB"] devices (stick)
- External Hard Disk Drives

1.1 Risks

Failure to adopt and implement this Information Security Standard may expose the Group to Risk which may result in:

- Financial Loss by External Attacker and/or Trusted Insider.
- Disclosure of Sensitive Information by External Attacker and/or Trusted Insider.
- Disruption of Business Operations by External Attacker and/or Trusted Insider.

1.2 Scope

This Standard must be read, and controls deployed in conjunction with all other ICS Standards.

The Standard is mandatory and applies to the Group businesses, functions, countries, and regions except where explicitly prohibited by local Law or Regulation [assessed as per section 4.2 Reporting Non-Compliance].

Note: *In case of any Country specific LRM requirement, the approach defined in ERMF (Chapter Eleven, Part B, section 4.2 "Country-level Host Regulatory Obligations") must be followed.*

The Standard covers all Group Information Assets which are processed and or used by the Group's Information Systems [wherever the term 'Systems' or 'Information System' is used in a control statement it refers to both Information System and Technology Infrastructure].

Where the Control Statements include Information Asset [IA] or Security-Business Impact Assessment [S-BIA] ratings, they are applicable only to those rated Systems. All other Control Statements apply to all Systems regardless of ratings and hosted environments [Production or Non-Production unless stated otherwise].

The Systems owned and or managed by the Third Parties [including Cloud Systems, Vendor Systems, Regulatory Systems, Self Service Terminal [SST] and similar], must additionally refer to

the ICS Standards for Security in Interactions with Third Parties and Secure Configuration Management.

Please note, any Systems which are deemed as 'Standalone Machines' must be assessed using the Security – Business Impact Assessment [S-BIA] and controls must be applied accordingly in line with applicable ICS Standards.

2 ROLES & RESPONSIBILITIES

Technology Infrastructure Owner
A named individual accountable for the protection of owned Technology Infrastructure and for compliance with applicable Control Statements.

People Leader
People Leaders must comply with the requirements and ensure that their Staff are made aware of their responsibilities in complying to this standard.

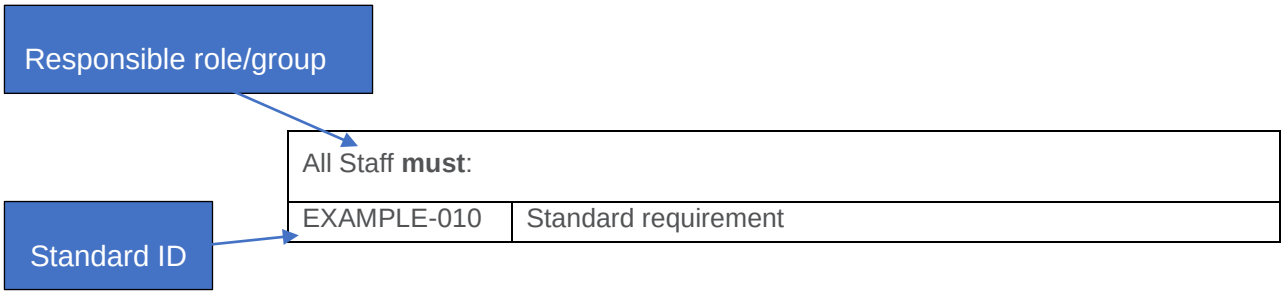
CISO ICS Standards & Controls
The CISO is the owner of this Information Security Standard and will ensure the document is updated to an agreed schedule.

***Note**: The Responsible role who 'must' execute against this standard can do so either directly or by delegation. Where this is the case and a delegate exercises the control, the named role remains accountable.*

All roles & responsibilities including their corelations within ICS risk management activities are defined in Chapter Eleven, Part B, section 2 "Three LoD Responsibility and Governance Committee Oversight" of the Enterprise Risk Management Framework.

3 STANDARD REQUIREMENTS

This section outlines minimum mandatory requirements that apply to this Standard. The requirements are set out in the following format:



3.1 Control Area: Management of Mobile Devices

Technology Infrastructure Owner **must**:	
MDS-030	Ensure that only Group approved Mobile Devices are permitted for Group's Information processing.
MDS-040	Ensure that the Mobile Device security policy settings cannot be modified by users.
MDS-050	Ensure that there are controls in place over software installed on Mobile Devices that are used to process Group's Information. *Note: Preventing unauthorised software from running for example by using application approved list or application execution tools that allow only specified, permitted applications to run or unapproved list that forbid specified application from running.*

3.2 Control Area: Access Management

Technology Infrastructure Owner **must**:	
MDS-080	Block access to Group Information from non-compliant Mobile Devices, such as when [but not limited to]: a) Mobile Device has not been connected to the central management server for a defined number of days [90 days]; b) Operating System is less than the Group defined version; c) Operating System has been tampered with; d) Security configuration is tampered with; e) Mobile Device is jailbroken or rooted [not applicable to laptops]; f) Anti-Malware is disabled [Laptops only]; g) Security profiles are removed; h) Is lost or stolen. *Note: For Laptops where technically feasible.*

3.3 Control Area: Mobile Devices access to Group Network

Technology Infrastructure Owner **must**:	
MDS-100	Ensure that Mobile Devices connecting to the Group network are installed with the encrypted security profile issued by Group which must have a profile unique to the user and the mobile device. The user must not be able to delete or edit this profile. [The Digital Certificate].

3.4 Control Area: Secure Configuration of Laptops

Technology Infrastructure Owner **must**:	
MDS-110	Ensure that Laptops protect the Confidentiality of stored Information by: a) Deploying file-based encryption software to safeguard files and folders by the user when required; b) Being centrally managed [unless specific approval is obtained]; c) Ensuring they are configured for software and firmware automatic updates from the Group's approved software and firmware update repository (this includes for example version updates but not Security Patches which are addressed in Vulnerability Identification and Management Standard); d) Disabling the auto-run feature. *[Reference Information Handling Standard, Information Classification Standard, Cryptography Standard, Identity and Access Management Standard, Secure Configuration Management Standard, Data Leakage Prevention Standard, Vulnerability Identification and Management Standard]*

3.5 Control Area: Configuration of Group Owned Smartphones and Tablets

Technology Infrastructure Owner **must**:	
MDS-130	Ensure that remote wipe is performed, and the security certificate must be revoked when the Mobile Device is: a) Lost or stolen; b) Sent to Third Party for repair; c) Jailbroken or rooted; d) Contains an application that is known to contain a security vulnerability (if not removed within a given timeframe after informing the user); e) A user has exceeded the maximum number of failed password attempts; f) Part of an employee exit clearance, transfer of service or termination process; g) Returned to Third Party; h) Sent to Third Party for destruction. *[Reference: Identity and Access Management Standard and Vulnerability Identification and Management Standard]*
MDS-140	Ensure that Group's Information and [Non-Group's] Personal Information are separated through containerisation.

3.6 Control Area: Secure Configuration of Portable Storage Devices

Technology Infrastructure Owner **must**:	
MDS-150	Protect Portable Storage Devices by using: a) Access restrictions (For Example: whether the user is authorised to read, write or format the device); b) Encryption techniques wherever applicable (using Group's approved cryptographic algorithms).

Technology Infrastructure Owner **must**:	
	For Example: using encryption software installed on the device or using file-encryption software on the computing device to which the Portable Storage Device connects when storing Group's Information. *[Reference: ICS Information Classification Standard, ICS Information Handling Standard, ICS Cryptography Standard]*

3.7 Control Area: Employee owned Mobile Devices used for business purpose (BYOD)

Technology Infrastructure Owner **must**:	
MDS-180	Define a formal documented process for managing the usage of employee owned Mobile Devices for business purposes.
MDS-190	Define and obtain employee sign-off of Terms of Use before allowing access to Group's Information from employee owned Mobile Devices.
MDS-200	Ensure that the Terms of Use considers relevant privacy legislation and defines the circumstances in which the Group reserves the right to: a) Confiscate, audit or inspect employee owned Mobile Devices; b) Manage the employee owned Mobile Device and application running on it; c) Enforce technical security controls such as access control, malware protection and encryption; d) Monitor, access, manage, recover or delete Group and personal applications and data on employee owned Mobile Device; e) Remotely delete all Group Information in the event of a security incident, if the Staff leaves the organisation or the Mobile Device is lost or stolen.
MDS-210	Ensure that technical security controls that are applicable to Group provided IT equipment are implemented on employee owned Mobile Devices that have access to Group's Information or Information Systems.

4 INFORMATION & SUPPORT

4.1 General Information and Support

For queries relating to this Security Standard please contact the ICS Standards team via: *ICSStandards*

4.2 Reporting Non-Compliance

As a general guideline, any non-compliance against the Applications and underlying Technology Infrastructure in CMDB should follow the ICS Non-Compliance Register (ICS NCR) process. Further assessment of these non-compliance should follow the issue management process, i.e. iTrack for issues with remediation plan or ICS Dispensation when there is an explicit decision not to remediate the issue.

4.3 Breach of this Standard

- Failure to comply with this Standard may result in formal action under the Group Disciplinary Standard, that for serious breaches could include termination of employment.
- Any actual or suspected breaches must be reported immediately to your People Leader or to your Compliance representative from the Group.
- All breaches of this Standard must be reported to the Document Owner of the Standard.

5 GLOSSARY

The ICS Standards Glossary has been defined and is available via the *GovPoint* – see the *Technology Glossary* via the *GovPoint Glossary* reference.

6 REGULATORY / INDUSTRY REFERENCES

All Regulatory/Industry References are available via the *ICS Master Control List* document published on: *Control Framework Library*

7 Appendix A – Version Control Table

Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
CISRO ICS Policy	Annual review includes: 1. Migrated existing standard to ERM standard template. 2. The existing Mobile Devices Standard document has been uplifted into this standard. 3. Consultation feedback, corrections incorporated	Material	Liz Banbury [delegate of Group CISRO]	1.0	3-Oct-19	3-Oct-19

Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
CISRO ICS Policy	Consultation feedback, corrections incorporated.	Material	Liz Banbury [delegate of Group CISRO]	2.0	15-Jan-21	1-May-21
CISRO ICS Policy	Annual review: Risks alignment to RTF.	Non-material	Samantha Finan, Global Head, ICS Policy, Standards and Reporting	2.1	15-Dec-21	1-Jan-22
CISRO ICS Policy	MDS-050 editorial change in line with ICSCR-3Mar2022-1 (inclusive terminology)	Non-material	Paul Hoare Head, ICS Policy and Best Practice	2.2	8-Mar-23	
CISRO ICS Policy	Editorial and administrative change 1. MDS-220; MDS-230;MDS-240;MDS-250;MDS-260;MDS-270;MDS-280;MDS-290 Control Removed (In line with ICSCR-18Feb2022-1 as these are covered now under Acceptable Use Standard (AUS))	Non-material	Paul Hoare Head, ICS Policy and Best Practice	2.3	13-Oct-23	1-Nov-23
Anna Kowal-Hughes **[ICs Standards]**	Editorial changes: 1. Document template updated in line with Template for Group Standards, V 7.0	Non-material	Jamie Cowan Hean, ICS Risk Framework & Governance	2.4	04-Dec-24	16-Dec-24

Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
	2. Document references updated 3. Roles references updated in line with the new org structure					