Information Handling Standard

Version No	3.0
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	20-Dec-24
Approval Date	6-Dec-24
Next Review Date	30-Nov-27

Table of Contents

Version Control Table

Document Author Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
Katarzyna Wencka **[ICS Standards]**	Editorial changes: 1. Document template updated in line with Template	Material	Jamie Cowan Head, ICS Risk Framework	3.0	06-Dec-24	20-Dec-24

	for Group Standards, V 7.0 2. Document references updated 3. Roles references updated in line with the new org structure Changes to ICS controls: 1. Table in section 7.1.2 “Electronic Information protection” updated in line with ICSCR-10Jun24-1 (i.e. BYOK/HYOK approach exception for SaaS, as per point 10 added)		& Governance			

1 INTRODUCTION AND PURPOSE

This Information Security Standard defines control requirements for all Information and Information Systems within the Group.

Information Handling is the creation, acquisition, sending, receiving, storing, processing and destruction of all Information whether it is in physical or electronic format. It is handled by people, Information Systems, processes and suppliers and controls must be applied accordingly to each.

Note: This Standard must be followed in conjunction with all applicable ICS Standards, including the following:

- Information Classification Standard,
- Unstructured Data Storage Standard,
- Acceptable Use Standard.

Note: *For all end user requirements on Handling Non-Electronic and Electronic Information, please refer to Acceptable Use Standard.*

1.1 Risks

The Standard mandates that adequate controls are implemented to ensure that all Information, Information Assets and Information Systems are appropriately handled.

Failure to adopt and implement this Security Standard may expose Group Information Assets and Information Systems 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.

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 System [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 as per the 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.

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

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

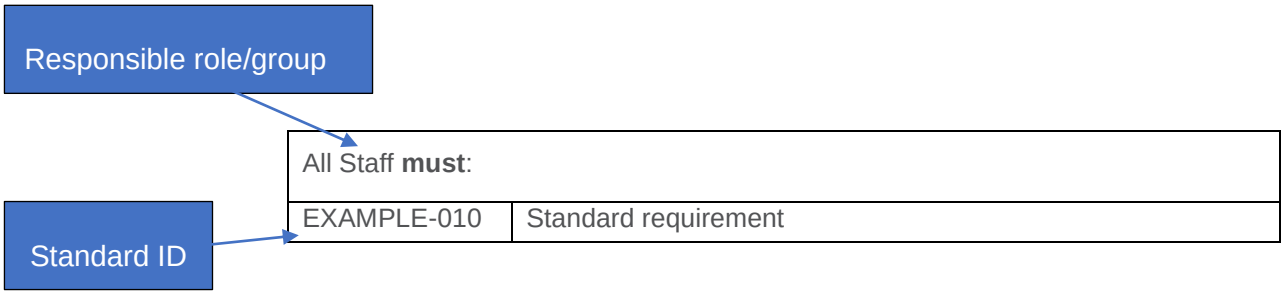
CISO ICS Standards & Controls
The CISO is the owner of this Information Security Standard and will ensure the document is updated to an agreed schedule.

***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: Protecting Information in Information Systems

Information System / Technology Infrastructure Owner **must**:	
INH-010	Identify and document the security controls required by the Information Security Standards to protect Information Assets and Information handled within owned Information Systems and Technology Infrastructure. *[Reference: Table 'Electronic structured data protection' in section 7.1.2 [INH-AP-020] Electronic Information protection.]* *[Reference: INC-025, INC-026]* *[Note: If electronic data (that represents Information Asset or Information) in an Information System/Technology Infrastructure is not protected with 1st or baseline options recommended in Table 'Electronic structured data protection' in section 7.1.2 [INH-AP-020] Electronic Information protection, then the dispensation process must be followed in line with section 4.2 of this Standard..]*
INH-025	Implement identified security controls to protect Information Assets and Information handled within Information Systems and Technology Infrastructure. *[Reference: INH-010]*

3.2 Control Area: Protecting Information Systems

Information System / Technology Infrastructure Owner **must**:	
INH-030	Use effective integrity checking mechanisms to ensure that integrity of Group Software and Firmware in Information Systems and Technology Infrastructure is preserved.
INH-040	Use effective integrity checking mechanisms to ensure that integrity of Group electronic data (this covers Information and Information Assets) in Information Systems and Technology Infrastructure is preserved.

3.3 Control Area: Protecting Information Handled by People and Processes

3.3.1 Protecting Electronic Information: Sending and Receiving

Information System / Technology Infrastructure Owner **must**:	
INH-210	Enhance the security of email messages through implementation of hashing or encryption. *[Reference: Tables: 7.1.1 [INH-AP-010] Electronic Information protection requirements; 7.1.2 [INH-AP-020] Electronic Information protection; 7.3 Handling Non-Electronic and Electronic Information in Acceptable Use Standard].*

Information System / Technology Infrastructure Owner **must**:	
INH-215	Include legally required disclaimers in email messages.
INH-230	Use digital signatures for the following: • to assure that email message (and data contained within it) have not been altered in transit since it was signed; • to assure Non-repudiation of email messages (that the sender - not an imposter - signed the contents of the email message).
INH-250	Prevent automatic auto-forwarding to external email addresses.
INH-260	Prevent the use of distribution lists for sending emails externally and in sending emails internally from an external source.

3.3.2 Protecting Electronic Information: Storing and Processing

Information System / Technology Infrastructure Owner **must**:	
INH-320	Protect Group Information (in form of electronic data) in line with Tables: Electronic Information protection, Electronic Information protection requirements, Types of protection for electronic data states. *[Reference: Cryptography Standard]*

3.3.3 Protecting Electronic Information: Instant and Collaborative Messaging

Information System / Technology Infrastructure Owner **must**:	
INH-420	Enhance the security of instant messaging applications by a) Preventing use of public instant messaging applications that Staff are not authorized to use and are not Group approved; b) Disabling unauthorised features such as file sharing, audio and video files; c) Directing messages through a content filter; d) Using encryption; e) Enable malware scanning. *[Reference: Tables: 7.1.1 [INH-AP-010] Electronic Information* protection requirements*; 7.1.2 [INH-AP-020] Electronic* Information protection*; 7.3 Handling Non-Electronic and Electronic Information in Acceptable Use Standard].*
INH-430	Ensure the protection of instant messaging infrastructure by a) Employing a standard client configuration for the instant messaging applications; b) Hardening instant messaging servers; c) Configuring firewalls to block unauthorized instant messaging traffic.

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

7.1 Tables: Electronic Information Handling

Note: *For the security controls and requirements for the end user information handling activities, refer to the Acceptable Use Standard.*

7.1.1 [INH-AP-010] Electronic Information protection requirements

Electronic Information protection requirements

Information System Confidentiality Impact Rating ('C' value of the S-BIA rating)	Electronic data state			
	At Rest***	In Transit Internal	In Transit External*	In Use
5**	Must	Must	Must	based on regulatory requirements or ICS risk
4**	Must	Must	Must	
3**	Must	based on regulatory requirements or ICS risk	Must	
2**	based on regulatory requirements or ICS risk		Must	
1**			based on regulatory requirements or ICS risk	
IT Equipment	Must	N/A (please refer to impact rating)	N/A (please refer to impact rating)	N/A (please refer to impact rating)

* All transfers to Cloud are treated as "In Transfer External"
** As Information Asset is represented by electronic data in various fields/attributes, then data protection mechanisms can be applied selectively to respective data fields/attributes if only these fields/attributes drive criticality rating of the Information Asset (i.e. the rest of the Information Asset and its data alone does not constitute any impact if comprised).
*** If electronic data is stored in cloud then native encryption provided by CSP (KMS) must be used.

7.1.2 [INH-AP-020] Electronic Information protection

Electronic structured data protection

Information System Confidentiality Rating ('C' value of the S-BIA rating)	Encryption				Tokenisation (reversible)	Hashing	Masking	Anonymisation (irreversible)	Key Management for encryption (exceptions apply – see below in point 10)
	Application	Database	File System	Storage					
5	1st option	2nd option (baseline)	2nd option (baseline)	3rd option	1st option	1st option* only for passwords	1st option for production data used in test environments PII (baseline)/based on regulatory requirements or ICS risk (critical data elements)	Based on regulatory requirements or ICS risk (in case of Non-Production processing)	SCB - HYOK/BYOK
4	1st option*	1st option (baseline)	1st option (baseline)	2nd option	1st option				SCB - HYOK/BYOK
3	based on regulatory requirements or ICS risk	based on regulatory requirements or ICS risk	based on regulatory requirements or ICS risk	1st option	based on regulatory requirements or ICS risk				SCB - HYOK/BYOK
2	based on regulatory requirements or ICS risk	based on regulatory requirements or ICS risk	based on regulatory requirements or ICS risk	based on regulatory requirements or ICS risk	based on regulatory requirements or ICS risk				based on regulatory requirements or ICS risk
1	based on regulatory requirements or ICS risk	based on regulatory requirements or ICS risk	based on regulatory requirements or ICS risk	based on regulatory requirements or ICS risk	based on regulatory requirements or ICS risk				based on regulatory requirements or ICS risk

1. The first option in the table is the preferred method of encryption for the given SBIA rating and encryption at a lower layer is to be considered only if this is not possible.
2. The baseline encryption is the minimum acceptable layer at with data should be encrypted for a given SBIA rating. If the baseline standard is met, there is no requirement of a dispensation.
3. If Database level encryption cannot be implemented for technical reasons, Storage level encryption with a minimum compensating control of Database Activity Monitoring can be implemented without a separate dispensation. Reasons why DB encryption cannot be implemented for the specific application need to be endorsed by the CISO.
4. Tokenization is considered to be equivalent to Application level encryption excepting for elements that cannot be tokenized (PIN, CVV, Blob etc).
5. If data is encrypted at a higher layer, encrypting at a lower layer is optional, provided all data elements contributing to the confidentiality rating are encrypted.
6. Regulatory requirements prescribing encryption/tokenization at a higher layer would take precedence over these recommendations based on SBIA ratings.
7. As Information Asset is represented by electronic data in various fields/attributes, then data protection mechanisms can be applied selectively to respective data fields/attributes if only these fields/attributes drive criticality rating of the Information Asset (i.e. the rest of the Information Asset and its data alone does not constitute any impact if comprised).
8. Data masking works by shielding confidential data, such as credit card information, Social Security numbers, names, addresses, and phone numbers, from unintended exposure to reduce the risk of data breaches.
9. If electronic data is stored in cloud, then native encryption provided by Cloud Service Provided ("CSP") (KMS) could be used.
10. HYOK/BYOK approach is not applicable for SaaS deployments. However, in such cases additional controls apply:
    a. cryptographic keys must be stored and processed in line with the requirement defined in the CRY-030,

b. the effectiveness of the CSP control environment is confirmed by industry recognised cyber security certification(s), for example SOC 2 Type II, ISO 27001.

Appendix A – Version Control Table

Document Author Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
CISRO ICS Policy	New Standard	Material	Darren Argyle	1.0	14-Nov-19	18-Nov-19
CISRO ICS Policy	1. Glossary updated for definition of Non-Public Information as approved in ICS Change Request [CR] Forum - ICSCR-21Feb2020-1 2. Updated Section 6.2.2 for Confidential Information requirements as approved in ICS CR Forum - ICSCR-31Mar2020-1	Material	Liz Banbury [delegate of Group CISRO]	1.1	17-Jun-20	17-Jun-20
CISRO ICS Policy	Updated INH-070 by including People Manager for authorising requests for sending Non-Public Information external. This has been approved in ICS Change Request Forum - ICSCR-10Jul2020-1	Material	Liz Banbury [delegate of Group CISRO]	1.2	11-Aug-20	11-Aug-20
CISRO ICS Policy	Annual Review	Material	Liz Banbury [delegate of Group CISRO]	2.0	15-Jan-21	01-May-21
CISRO ICS Policy	Editorial changes: document template update 1. INH-010 updated & INH-025 added in line with CSCR-14Apr2021-1; ICSCR-	Material	Samantha Finan, Global Head, ICS Policy, Standards and Reporting	2.1	14-Dec-21	01-Jan-22

Document Author Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
	4Mar2021-2; ICSCR-7Apr2021-1 2. Handling of printed information (send outside the Group & restricted) amended in table 7.1.1 in line with ICSCR-24Jun2021-1 3. Storage and handling outside Group premises for Confidential and Restricted uplifted in table 7.1.1 in line with ICSCR-1Jun2021-1 4. 7.1.3 Table updated in line with ICSCR-14Apr2021-1 / ICSCR-4Mar2021-2 / ICSCR-7Apr2021-1 5. 7.1.4 Table updated in line with ICSCR-13Feb2021-1					
CISRO ICS Policy	1. Document template uplifted 2. References of INH-140 corrected (admin) 3. reference to S-BIA Confidentiality rating in sections 7.1.2 & 7.1.3 updated in line with	Non-material	Paul Hoare Head, ICS Policy and Best Practice	2.2	08-Mar-23	22-Mar-23

Document Author Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
	ICSCR-26Sep2022-1					
CISRO ICS Policy	Editorial and Administrative changes made: 1. Removed Control - INH-060; INH-070; INH-075; INH-080; INH-090; INH-100; INH-120; INH-130; INH-140; INH-150; INH-160; INH-170; INH-180; iNH-190; INH-200; INH-280; INH-290; INH-300; INH-310; INH-330; INH-340; INH-365; INH-380; iNH-390; INH-410; INH-440; INH-490; iNH-500; INH-510; INH-520; INH-530; INH-540 [in line with ICSCR-18Feb2022-1 as these are covered under Acceptable Use Standard] 2. Removed Table from Appendix : 7.1.1 Non-Electronic	Non-material	Paul Hoare Head, ICS Policy and Best Practice	2.3	19-Oct-23	14-Nov-23

Document Author Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
	Information; 7.1.4 Electronic data handling (All Staff only) [in line with ICSCR-18Feb2022-1 as these are covered under Acceptable Use Standard] 3. Document references updated 4. Roles references updated					
Katarzyna Wencka **[OTCR ICS Policy]**	Editorial changes: 1. Document template updated in line with Template for Group Standards, V 6.0 2. Document references updated 3. Roles references updated in line with the new OTCR structure Changes to ICS controls: Table in section 7.1.2 “Electronic Information protection” updated in line with ICSCR-10Jun24-1 (i.e. BYOK/HYOK approach exception for	Material	Jamie Cowan Head, ICS Risk Framework & Governance	3.0	06-Dec-24	20-Dec-24

Document Author Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
	SaaS, as per point 10 added)					