Information Classification Standard

Version No	2.5
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	Standard
Effective Date	12/16/2024
Approval Date	12/4/2024
Next Review Date	11/30/2026

Table of Contents

Version Control Table

Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
Anna Kowal-Hughes **[ICS Standards]**	Editorial and administrative changes made: 1. Roles references updated in line with the new org structure 2. Document template updated in line with Template for Group	Non-material	Jamie Cowan Head, ICS Risk Framework & Governance	2.5	04-Dec-24	16-Dec-24

Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
	Standards, V 7.0 3. Duplicate control ID INC-080 merged					

1 INTRODUCTION AND PURPOSE

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

Information Classification is the application of 'labels' to Information and Information Assets and Systems which allow the Group to identify its most important Information which, in turn determines which controls are deployed.

What is the difference between an 'Information Asset' and 'Information'?

An Information Asset is a type or category of Information that has a business value and uses a 'rating'.

[Reference: Table 6 - Information Asset Rating Definitions]

Information is the 'unstructured' data that the end user will create or process. For Example: a Word document, an Email or a PowerPoint presentation.

Within the Group we have 2 different methods of 'Classification':

1. A Classification system for the end-user handling of Information.
2. A Rating system for Information Assets and thereafter Information Systems based on the business value of the Information.

Information on its own is accorded a 'classification' based on levels of Confidentiality and Integrity to determine how to handle that Information accordingly.

a. Confidentiality Classifications are: Restricted, Confidential, Internal, Public
b. Integrity Classifications are: Highly Trusted, Trusted, Accurate, Uncontrolled

Note: For all end user requirements on how to classify and label the information (including: all types of electronic and non-electronic Information, for example: emails, files, paper documents), please refer to *Acceptable Use Standard* [Appendix 7.1 Table 1 – Confidentiality Classification Labels and 7.2 Table 2 – How to Classify the Information]

Information Assets are 'rated' by determining the impact of a loss of Confidentiality, Integrity and Availability of the Information using the Group Risk Assessment Matrix ["GRAM"] and considering the affected volume of records. The result will be transcribed as a rating for each of the three elements above (Confidentiality, Integrity and Availability) and provides a high watermark overall rating. These ratings are then used to determine the rating of the Information System using the Security-Business Impact Assessment ["S-BIA"] Methodology.

Note: *Availability is not included when considering controls for the secure handling of Information.*

For Example: Board Papers

As an Information Asset, they have a rating of '5'.

However, they may be classified as 'Internal' depending on the content and the impact of that content as per the GRAM.

The objective of rating an Information Asset is to determine the value of the Information to the business.

The objective of classifying Information is for the end user to understand how to securely handle the Information they deal with on a day-to-day basis to prevent unauthorised access or alteration to that Information.

The classification of Information is important as it forms the core foundation for determining the controls required to protect the Information at the right level. The classification not only ensures that we are providing the highest level of protection for the Information that needs protecting, but also ensures that resources are prioritised based on the classification level.

The level of classification applied to Information shows the potential consequences of that Information being disclosed, altered, or destroyed.

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

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

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 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.

Information Asset Owner
A named individual with accountability for the protection and permissible use of owned information Assets in Information Systems and Technology Infrastructure.

Business Function Head
The Business Function Head is responsible for identifying their Critical Information Systems and ensuring that Ownership is assigned to Information Systems prior to the System being deployed to Production.

Process Owner (PO)
POs (as defined by Enterprise Risk Management Framework) are Business or Function managers responsible for the end-to-end business or function processes as identified within the Group's Process Universe. They are responsible for identification and management of the end-to-end process as defined in the Group's Process Universe and associated risks, including ICS related activities as mandated by the Standard. The PO is responsible for ensuring the provision of quality, timely, and adequate data, and management information to measure appropriate coverage and performance of control points (and subsequent measurement) against ICS Policy and Standards.

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.

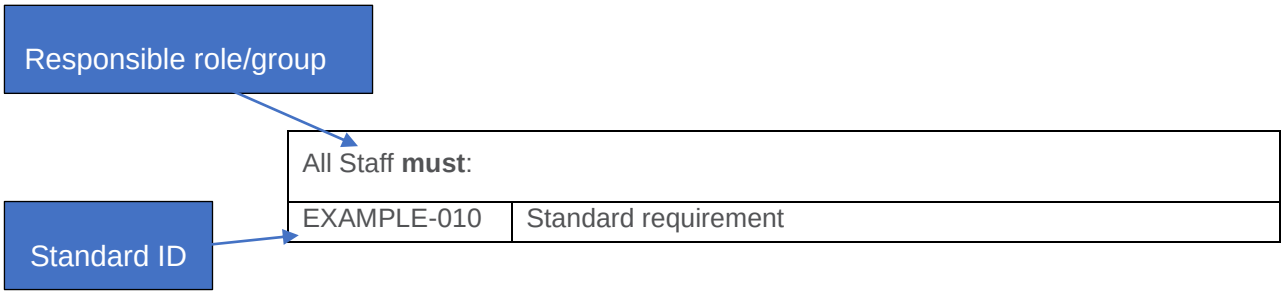
CISO ICS Standards & Controls
The CISO is the owner of this Information Security Standard and will ensure the document is updated to an agreed schedule.

***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: To Identify, Assign Ownership and Rate Information Assets

Business Function Head and/or Process Owner **must**:	
INC-010	Identify all Information Assets, aligned where possible to sub-domains of the Data Quality Management Framework [DQMF], and owned by Business Function. *[Reference: Defining Information Assets for Standard Chartered Methodology]*
INC-020	Assign an Information Asset Owner to each Information Asset.

Information Asset Owner and/or Information System Owner and/or Technology Infrastructure Owner **must**:	
INC-025	Together determine how Information Asset is represented by electronic data in various fields/attributes (in Information Systems and Technology Infrastructure) to enable data protection mechanisms, to 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 electronic data alone does not constitute any impact if comprised).
INC-026	Ensure that Information System is documented, and the documentation accuracy is maintained. The documentation must include (but is not limited to): a) Information System architecture with security architecture layer included b) Data model and data workflows for the (key) data sets processed by the Information System (with reference to the parent Information Asset where applicable) *c)* Information System interfaces and communication channels (other Information System/Technology Infrastructure connectivity and open system services)
INC-027	Perform assessment of business and regulatory requirements related to electronic data protection in owned Information Systems/Technology Infrastructure, that processes Information Assets/Information.

Information Asset Owner **must**:	
INC-040	Evaluate the impact of Confidentiality, Integrity, and Availability loss on owned Information Assets.

Information Asset Owner **must**:	
INC-050	Rate owned Information Assets for loss of Confidentiality, Integrity and Availability based on evaluated impact. *[Reference: INC-040]*
INC-060	Record all Information Assets (including all mandatory details) in Group owned Information Asset Register.
INC-070	Review that all mandatory details and CIA ratings of all owned Information Assets, recorded in Group owned Information Asset Register, are up to date. *[Reference: Defining Information Assets for Standard Chartered]*

Group OTCR **must**:	
INC-080	Govern and maintain the Information Asset Framework and S-BIA Framework.

3.2 Control Area: To Identify, Assign Ownership and Rate Information Systems and Technology Infrastructure

Business Function Head and/or Process Owner **must**:	
INC-090	Identify all Information Systems and Technology Infrastructure owned by Business Function.
INC-100	Assign an Information System Owner to each Information System and Technology Infrastructure Owner to each Technology Infrastructure.

Information System Owner **must**:	
INC-120	Identify all Information Assets handled by owned Information Systems and record this Information in a Group owned IT Asset and Configuration Management Register. *[Reference: Defining Information Assets for Standard Chartered]*
INC-130	Rate Information Systems through employment of the Group S-BIA methodology. *Note: Technology Infrastructure should be S-BIA rated in line with requirements defined in referenced Methodology.* *[Reference: Security Business Impact Assessment (S-BIA) Methodology]*

Information System Owner and/or Technology Infrastructure Owner **must**:	
INC-110	Review annually that all mandatory details and S-BIA ratings of all owned Information Systems and Technology Infrastructure, recorded in Group owned IT Asset and Configuration Management Register, are up to date. *[Reference: Security Business Impact Assessment (S-BIA) Methodology]*
INC-140	Record all Information Systems and Technology Infrastructure (including all mandatory details) in a Group owned IT Asset and Configuration Management Register and maintain it.

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 Classification Labels

For document and information classification labels and approach, refer to the Acceptable Use Standard.

7.2 Information Asset Rating Definitions

Please refer to *Information Asset Methodology*

Appendix A - Version Control Table

Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
CISRO ICS Policy	New Standard		Darren Argyle	1.0		
CISRO ICS Policy	1. Updated the definitions of Confidential and Internal labels under Section 6.2.1 Table 1 as approved in ICS Change Request Forum – ICSCR-10Jul2020-1 2. For alignment with updated definitions, the table 6.2.3 is updated for Internal classification label by removing 'and not intended for external use or for customers?'		Liz Banbury [delegate of Group CISRO]	1.1	14-Nov-19	18-Nov-19
CISRO ICS Policy	Annual Review		Liz Banbury, Global Head, ICS Policy and Risk	2.0	15-Jan-21	1-May-21
CISRO ICS Policy	Annual Review; Control Update: INC-025, INC-026 New Control: INC-027		Samantha Finan, Global Head, ICS Policy, Standards and Reporting	2.1	15-Dec-21	1-Jan-22
CISRO ICS Policy	Appendix, 7.1 Table 1 - Confidentiality Classification Labels, Confidentiality Labels: Internal modified in line with ICSCR-31May2022-1 Document template uplifted		Paul Hoare Head, ICS Policy and Best Practice	2.2		

Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
CISRO ICS Policy	Human error correction: removed control INC-190 re-added.		Paul Hoare Head, ICS Policy and Best Practice	2.3		
CISRO ICS Policy	Editorial and Administrative Changes made 1. Removed Control – INC-170; INC-190 in line with ICSCR-18Feb2022-1 as these are covered under Acceptable Use Standard 2. Removed table from Appendix [ICSCR-18Feb2022-1] : 7.1 Table 1 - Confidentiality Classification Labels; 7.2 Table 2 – Integrity Classification Labels; 7.3 Table 3 – How to Classify the Confidentiality of Information; 7.4 Table 4 – How to Classify the Integrity of Information 3. Document template aligned with the Template for the Group Standards v5.6 4. Role references updated (Group CISRO		Paul Hoare Head, ICS Policy and Best Practice	2.4	18-Oct-23	12-Nov-23

Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
	and People Leander)					
Anna Kowal-Hughes **[ICS Standards]**	Editorial and administrative changes made: 1. Roles references updated in line with the new org structure 2. Document template updated in line with Template for Group Standards, V 7.0 3. Duplicate control ID INC-080 merged	Non-material	Jamie Cowan ICS Risk Framework & Governance	2.5	04-Dec-24	16-Dec-24