Secure Decommissioning and Destruction

Version No	3.3
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

Version Control Table

Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
Anna Kowal-Hughes	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	3.3	04-Dec-24	16-Dec-24

1. INTRODUCTION AND SCOPE

This Security Standard, which is a part of the Group Information and Cyber Security Policy [GICSP] framework, defines the control requirements for the secure decommissioning of Group Information Systems and/or destruction of Group Information which exists within electronic storage media devices and in non-electronic [paper] formats.

Note: This standard must be followed in conjunction with the records retention and destruction requirements as set out in the Group Record Keeping Policy/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 in line with applicable ICS Standards.

2. ROLES & RESPONSIBILITIES

Technology Infrastructure Owners

A named individual accountable for the protection of owned Technology Infrastructure and for compliance with applicable Control Statements defined in this Standard.

Information System Owner

A named individual accountable for the protection of owned Information System and for compliance with applicable Control Statements defined in this Standard.

Process Owner

Process Owner i.e., Group Property for Physical Information, is accountable for the end-to-end management of owned process, associated risks and for compliance to the 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.

CISO ICS Standards & Controls

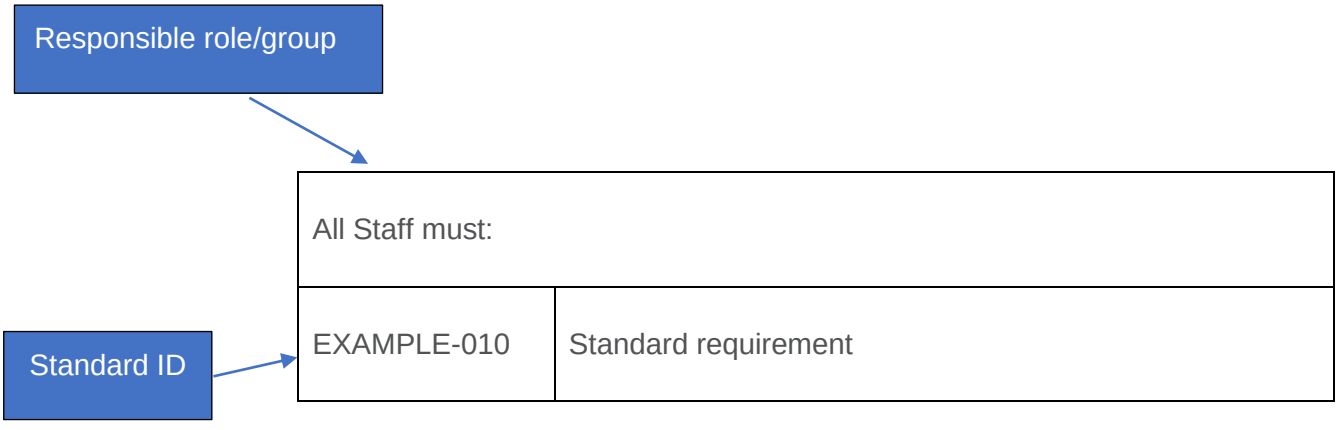
The CISO is the owner of this Security Standard and will ensure the document is updated to an agreed schedule.

***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: Secure Decommissioning and/or Destruction of Information Systems/Technology Infrastructure

Technology Infrastructure Owner **must**:	
SDD-010	Remove or ensure removal of all electronic storage media devices before the commencement of technology decommission/disposal. *For example: hard disks, Portable Storage Devices*
SDD-020	Ensure that Group Information within the electronic storage media devices is securely wiped before the electronic media device is reused, returned to Third Party, destroyed, or sent to the appropriate authority for repair, as appropriate.
SDD-030	Ensure that a data wiping/erasure technique process exists and the same is used guarantying that the Group Information is non-retrievable. *For example: Sanitization, Degaussing, Purging*
SDD-040	Obtain Group Information/Information Asset Owner approval when their Information/Data cannot be securely destroyed from storage media device & maintain approval records.
SDD-050	Allow destruction outside the Group premises only if it cannot be performed on the Group premises and validate if the destruction is equivalent to the requirements in this Standard.
SDD-060	Allow destruction by a Third Party [TP] where the TP has been assessed for security risks and the TP must provide a certificate of destruction signed by a valid authority (a named person holding authority to sign destruction certificates at TP place).
SDD-070	Provide and maintain an inventory of electronic storage media devices scheduled for destruction and its destruction status.
SDD-080	Maintain a record and evidence showing clear accountability for the completion of destruction activities.
SDD-090	Ensure that Group Information (including any Group configuration) is wiped from TP owned storage media devices before return to TP. If the effective disposal of data is not possible, the storage media devices must not be returned to TP.

Information System Owner and/or Technology Infrastructure Owner **must**:	
SDD-101	Ensure their Information are securely disposed of and/or destroyed.

3.2 Control Area: Secure Destruction of Portable Media Devices

Technology Infrastructure Owner **must**:	
SDD-110	Destroy optical media (e.g., CDs and DVDs) and magnetic tapes via shredding using a commercial optical disk grinding device or optical disk media shredders. *Note: For secure erasure of data within and destruction of electronic media devices, refer to Control SDD-020 – SDD-090.*

3.3 Control Area: Secure Destruction of Physical Information

Process Owner **must**:	
SDD-140	Ensure that secure disposal devices (for example confidential waste bins, shredders) are provided for the disposal/destruction of Group Information (paper).
SDD-150	Ensure confidential waste bins are locked and the key is managed in a secure manner.
SDD-160	Ensure confidential waste bins are emptied by authorised personnel on a regular basis.
SDD-170	Ensure that the handover of paper waste to the authorised personnel is recorded.
SDD-180	Ensure that only TPs which have been assessed for security risks can handle Group paper waste.
SDD-190	Ensure the authorised TP/personnel maintain the security of the Group paper waste throughout handling and until securely destroyed.
SDD-200	Ensure any destruction by an authorised Third-Party follow the destruction requirements equivalent to the requirements in this Standard and be validated by the Technology Infrastructure Owner.

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
CISO Policy	Uplifted controls from existing standards. Changes made based on feedback.		Gareth Carrigan, Global Head, ICS Governance, Policy and Risk	1.0 [29-Mar-19]	29-Mar-19	29-Mar-19
Yogesh Kumar Venkatesan	To align with recent Org change, reference to CISO amended to CISRO accordingly within the document.	Non-material	Liz Banbury, Head, ICS Policy	1.1 [30-Dec-19]	30-Dec-19	30-Dec-19
CISRO Policy	Annual Review – The following statements have been amended. **Duplicates Removed** – SDD-100 **Minor –** SDD-030, SDD-040, SDD-090, SDD-110 **Administrative –** SDD-010, SDD-170, SDD-190, SDD-120, SDD-020, SDD-130, SDD-140, SDD-160, SDD-200 **New – SDD-101**		Liz Banbury, Head, ICS Policy	2.0 [29-Apr-20]	16-Apr-20	16-Apr-20
CISRO Policy	Annual Review – Alignment of Scope, Risks, Roles & Responsibilities with correct functions. Amended statements: **Administrative, Editorial:** SDD-050, SDD-070-090, SDD-200	Non-material	Liz Banbury, Head, ICS Policy	2.1 [20-May-21]	08-Jun-21	01-Jul-21
CISRO ICS Policy	1. Document template updated (in line with the ERM template). 2. Risks section realigned with ICS RTF v4.0.		Samantha Finan, Global Head, ICS Policy, Standards and Reporting	3.0 [22-June-2022]	22-Jun-22	01-Jul-22

	3. Amended SDD-040 w.r.t ICSCR-11Oct2021-1					
CISRO ICS Policy	1. Template update to ERM Standard template v5.6. 2. Updated Group Record Management Policy/Standard to Group Record Keeping Policy/Standard.	Non-material	Paul Hoare Head, ICS Policy and Best Practice	3.1 [11-July-2023]	11-Jul-23	
CISRO ICS Policy	1. Changes made w.r.t ICS Policy Changes Requests: ICSCR-18Feb2022-1 – Removed as covered in Acceptable Use Standard – SDD-220, SDD-120, SDD-130, SDD-230, SDD-240. 2. People Manager to People Leader	Non-material	Paul Hoare, Head, ICS Policy and Best Practices	3.2 [13-Nov-23]	13-Nov-23	14-Nov-23
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	Jame Cowan Head, ICS Risk Framework & Governance	3.3	04-Dec-24	16-Dec-24