Data Storage and Backup

Version No	3.1 (Draft)
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	Arti Singh
Document Contact Job Title	Assoc. Director, ICS Standards
Business Scope	All Businesses
Function Role	All Functions
Geography Scope	Global
Approval Date	4-Dec-24
Effective Date	16-Dec-24
Next Review Date	30-Jun-27

Table of Contents

1. INTRODUCTION AND PURPOSE 4

1.1 Risks 4

1.2 Scope 4

2. ROLES & RESPONSIBILITIES 5

3. STANDARD REQUIREMENTS 6

3.1 Control Area: Storage Devices 6

3.1.1 Storage Area Network (SAN) Requirements 6

3.1.2 Network Attached Storage (NAS) Requirements 6

3.2 Control Area: Backups 6

3.2.1 Data to Backup 6

3.2.2 Securing of Backup 7

3.2.3 Scheduling 7

3.2.4 Restoration Testing 7

4. INFORMATION & SUPPORT 7

4.1 General Information and Support 7

4.2 Reporting Non-Compliance 8

4.3 Breach of this Standard 8

5. GLOSSARY 8

6. REGULATORY / INDUSTRY REFERENCES 8

Appendix A – Version Control Table 8

Version Control Table

Document Author Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
Arti Singh [ICS Standards]	Administrative changes introduced to update document template, references, roles and ownership.	Non-material	Jamie Cowan Head, ICS Risk Framework & Governance	1.1	04-Dec-24	16-Dec-24

1. INTRODUCTION AND PURPOSE

This Information Security Standard defines control requirements to be adhered during the selection, implementation and operation of Data Storage and Backup devices used to store the Group Information.

With the ever-increasing use of network computing and the subsequent increase in amount of data processed by the Group, it is vital to store and manage the data in an efficient and secure manner. Therefore, Storage and Backup devices must be securely configured to protect Group Information at all times, and backups must be taken in a manner which will enable continuity and recovery of business in case of any emergency.

Note: This standard must be followed in conjunction with the records retention and destruction requirements as set out in the Group Records Management Policy and Standard.

1.1 Risks

This Data Storage and Backup Standard mandates that adequate controls are implemented to protect the Group's Information in Storage and Backup devices.

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. Policy 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 in line with applicable ICS controls defined in ICS Standards

2. ROLES & RESPONSIBILITIES

All Staff

All Staff are responsible for the safety of Group Technology Assets under their care, the security of Group Information allowed for accessing via the Technology Assets and for compliance with the 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.

Technology Infrastructure Owner

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

People Manager

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

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

CISO ICS Standards & Controls

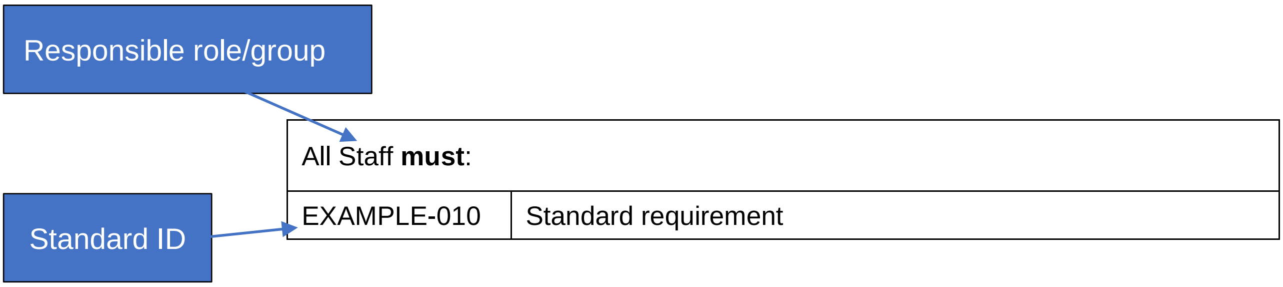
The CISO is the owner of this Security Standard and will ensure the document is updated to an agreed schedule.

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:



Responsible role/group

Standard ID

All Staff **must**:	
EXAMPLE-010	Standard requirement

3.1 Control Area: Storage Devices

3.1.1 Storage Area Network (SAN) Requirements

Technology Infrastructure Owner **must**:	
DSB-160	Ensure masked Logical Unit Number [LUN] is configured on the SAN Storage Arrays.
DSB-170	Ensure Fibre channel zonings are configured.

3.1.2 Network Attached Storage (NAS) Requirements

Technology Infrastructure Owner **must**:	
DSB-190	Ensure that data segmentation is configured on the NAS. *[For example: usage of Storage Virtual Machine/Tenants for data services.]*
DSB-210	Ensure NAS Network File System [NFS] is configured to only accept requests from authorised devices.
DSB-220	Ensure NAS Common Internet File System [CIFS] / Server Message Block [SMB] share permissions do not allow “Open” or “Everyone” access to a NAS share.

3.2 Control Area: Backups

3.2.1 Data to Backup

Information System Owner **must**:	
DSB-230	Ensure a data backup schedule is implemented in line with specific data availability, retention, and recovery requirements for the Information Systems.

	Reference: Technology Resilience Management Standard /Process

Process Owner [Backup] **must**:	
DSB-240	Ensure the Backups taken are clearly labelled along with the source System detail from where the backup was taken.

3.2.2 Securing of Backup

Process Owner [Backup] **must**:	
DSB-250	Implement physical and environmental protection mechanisms to secure on-site and off-site Backups. *[Reference: Data Centre Facility Management under Group Information Technology (IT) Policy]*
DSB-260	Ensure access protection to the Backup Infrastructure against any unauthorised tampering or changes to data (including but not limited to destructive ransomware attacks) is in place.
DSB-265	Ensure immutable mechanisms are implemented for critical assets including Systems S-BIA rated 5 (Availability) with data backup requirements.
DSB-266	Ensure isolation mechanisms are implemented for Storage and Backup Infrastructure.
DSB-270	Implement controls to handle, transport and store Backup media as per manufacturer specifications to protect from loss, damage, and unauthorised access.
DSB-300	Ensure the key and the encryption algorithm for backup encryption are managed in line with ICS Standard – Cryptography**.**

3.2.3 Scheduling

Process Owner [Backup] **must**:	
DSB-320	Ensure the Backup schedule is documented and maintained.

3.2.4 Restoration Testing

Information System Owner **must**:	
DSB-330	Ensure Backup and Restore Capability is in place for Information and Information Systems S-BIA rated 3-5 and that testing, and validation is in line with IT Resilience Standards. *[Reference: Technology Resilience Management Standard]*

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 Manager 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.*

Appendix A – Version Control Table

Document Author Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
CISO ICS Policy	Annual review includes: 1. Migrated existing standard to ERM standard template. 2. The existing Storage HLSTS and Backup Information Security Standard documents have been consolidated in this standard.	-	Gareth Carrigan, Global Head, ICS Governance, Policy and Risk.	1.0	15-May-19	22-May-19

Document Author Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
	Consultation feedback, corrections incorporated.					
Yogesh Kumar Venkatesan	To align with recent Org change, reference to CISO amended to CISRO accordingly within the document.		Liz Banbury, Head, ICS Policy.	1.1	30-Dec-19	05-Jan-20
CISRO ICS Policy	Annual Review - The following statements have been amended. **Duplicates Removed:** DSB-010, DSB-020, DSB-030, DSB-040, DSB-050, DSB-060, DSB-070, DSB-080, DSB-090, DSB-100, DSB-110, DSB-120, DSB-130, DSB-140, DSB-150, DSB-180, DSB-200, DSB-290. **Minor:** DSB-260 **Administrative**: DSB-230, DSB-240, DSB-280, DSB-330		Liz Banbury, Global Head, ICS Policy and Risk.	2.0	29-Apr-20	06-May-20
CISRO ICS Policy	Annual Review – Alignment of Risks, Scope, Roles & Responsibilities with correct functions; Updated paragraph 4. Amended statements: **Administrative, Editorial:** DSB-270, DSB-300 **Administrative, Removal:** DSB-280, DSB-310 Minor: DSB-330		Liz Banbury [delegate of Group CISRO]	2.1	23-Mar-21	29-Mar-21
CISRO ICS Policy	Based on Change Requests and additional standard review: **New:** DSB-265, DSB-266 **Updated:** DSB-230, DSB-260	Material	Samantha Finan, Global Head, ICS Policy, Standards and Reporting	3.0	22-Jun-22	29-Jun-22