Unstructured Data Storage Standard

Version No	2.3
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-27

Table of Contents

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	2.3	04-Dec-24	16-Dec-24

1 INTRODUCTION AND PURPOSE

This Information Security Standard defines control requirements for Unstructured Data Storage.

Unstructured Data Storage is the storage of Information [or Data] where the location and naming of files is determined manually.

Unstructured Data is a term used to define Information [or Data] that is extracted from Applications/Information Systems or created as files (using Word, Power Point, Excel files, log files or using any similar tools/applications (For Example: Outlook) for further use or that is generated through ad hoc use of computers (such as in spreadsheets, emails, written reports).

Unstructured Data is typically generated and processed by the End User.

Examples of Unstructured Data:

1. End User files stored in shared file directories
2. End User files stored in Network Attached Storage [NAS]
3. Information [or Data] and End User files stored in SharePoint sites and Intranet sites
4. Collaboration tools such as Confluence and JIRA
5. Emails stored in shared email folders

Access controls shall be implemented on the individual Storage Elements [file folders, SharePoint sites, the Bridge site] and the Storage Element Owner is responsible for managing access to these places, whereas access to the Unstructured Data Storage is managed by the Technology Infrastructure Owner and accountability sits with the Information System Owner.

A Storage Element is the 'container' for Unstructured Data which is subject to access controls with individually assigned owners.

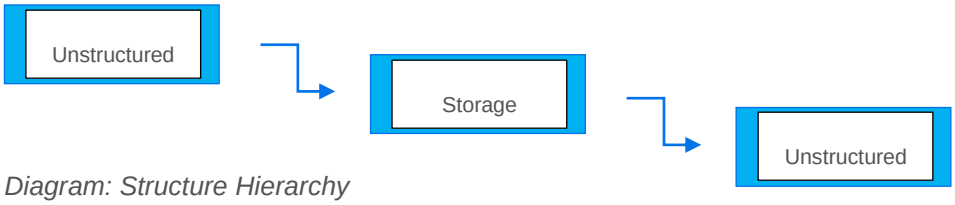


Diagram: Structure Hierarchy

The management of Unstructured Data Storage and Storage Elements is important as it enables the Storage Element Owner to manage access to their Unstructured Data. This reduces the likelihood of unauthorized access and therefore the risk of disclosure or modification of that Data.

Note: This standard must be followed in conjunction with the following:

- Information Security Standard: Information Classification
- Information Security Standard: Information Handling

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 Self-Service Terminals.

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 controls defined in ICS Standards.

2 ROLES & RESPONSIBILITIES

Information System Owner

Information System Owners are responsible for complying with the control areas of this Information Security Standard which are applicable to them and for the protection of Standalone Machines as part of their overall information asset portfolio. They are also accountable for ensuring that the Technology Infrastructure Owners correctly apply the controls as set out in this Standard. As first line role holders they must also have in place a model for validation of control existence and effectiveness.

Technology Infrastructure Owner

Technology Infrastructure Owners are responsible for complying with the control areas of this Information Security Standard which are applicable to them and must ensure that Information processed by the Standalone Machines under their custody are adequately secured. As first line role holders they must also have in place a model for validation of control existence and effectiveness.

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.

Storage Element Owner

A named individual who is in charge of and/or has elevated entitlements to the given Storage Element and its assets.

CISO ICS Standards & Controls

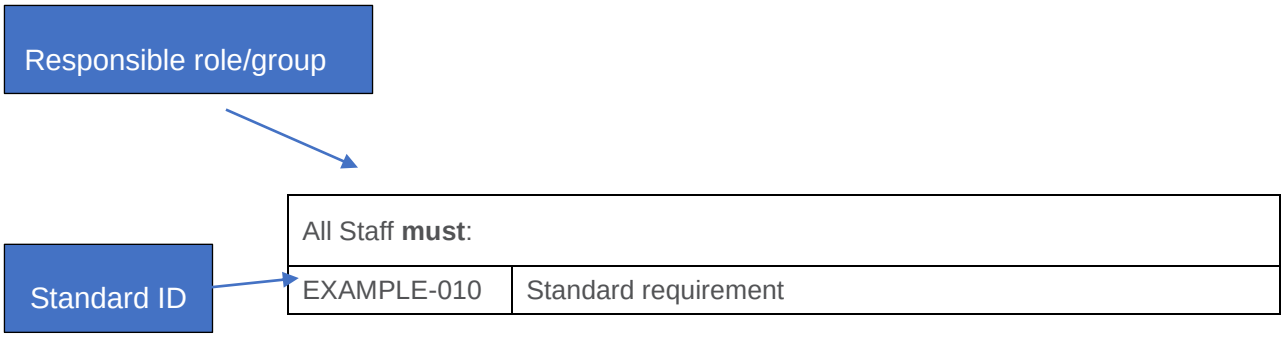
The CISO is the owner of this Security Standard and will ensure the document is updated to an agreed schedule.

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: Security by Design

Information System Owner and/or Technology Infrastructure Owner **must**:	
UDS-010	Design and maintain a documented process for Storage Element Owners to ensure they are aware of their roles and responsibilities which include: a) Access provisioning and de-provisioning; b) Access and content review. *[Reference: Identity and Access Management Standard]*
UDS-020	Design and maintain a documented process for Storage Element Owners to ensure Unstructured Data, that is no longer required, is removed.

3.2 Control Area: Access to Unstructured Data Sources

Business Function Head **must**:	
UDS-030	Identify appropriate Storage Elements for the storing of Unstructured Data and assign a Storage Element Owner to each.

Storage Element Owner **must**:	
UDS-050	Ensure that all access requests are reviewed and based on review approved or rejected.
UDS-060	Document Storage Element control requirements which must follow Identity and Access Management Standard.
UDS-070	Ensure that all access requests and approvals/rejections are documented or recorded and retained. *[Reference: Identity and Access Management Standard]*
UDS-080	Assign access to Unstructured Data within the Storage Element using Security Groups according to the process for approving and granting access.
UDS-090	Remove access to Unstructured Data within Storage Elements according to the process for reviewing and revoking access.

Storage Element Owner **must**:	
UDS-100	Initiate Access Reviews every 6 months in accordance with the User Access Certification [UAC] and Manager Access Review [MAR] processes and provide People Managers with the required reports. Note: For all self-managed Storage Elements their Owner must complete all UAC and MAR every 6 months to ensure that: a) Staff having access to Storage Element is an active employee; b) Staff's entitlements are validated; c) SoD and 'Least Privilege' principles are applied; d) any Staff's entitlements, that are no longer required (as a result of mover/leaver process), are removed; e) Dormant Accounts are identified and removed if no longer needed; f) Evidence that the UAC and MAR are completed on time is retained. *Note: Identification of 'Dormant Accounts' is based on IAM-720 & 730.* *[Reference: IAM-860]*
UDS-120	Delete the Storage Element when it is no longer required or no longer contains Unstructured Data.

4 INFORMATION & SUPPORT

4.1 General Information and Support

For queries relating to this Security Standard please contact the CISRO Policy 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	New Standard	Material	Darren Argyle	1.0	2-Dec-19	
CISRO ICS Policy	Amended to UDS-160 as approved in the ICS Change Request [CR] Forum - ICSCR-3Jul2020-1		Liz Banbury [delegate of Group CISRO]	1.1	4-Sep-20	
CISRO ICS Policy	Annual Review	Material	Liz Banbury [delegate of Group CISRO]	2.0	15-Jan-21	
CISRO ICS Policy	Annual review		Samantha Finan, Global Head, ICS Policy, Standards and Reporting	2.1	15-Dec-21	1-Jan-22
CISRO ICS Policy	Editorial and administrative changes introduced: 1) UDS-150 removed in line with the ICSCR-18Feb2022-1 (control removed as covered in the Acceptable Use Standard)	Non-material	Paul Hoare Head, ICS Policy and Best Practice	2.2	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 2. Document references updated	Non-material	Jamie Cowan Head ICS Risk Framework & Governance	2.3	04-Dec-24	16-Dec-24

	3. Roles references updated in line with the new org structure					