Data Leakage Prevention

Version No	2.2
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	2.2	04-Dec-24	16-Dec-24

1. INTRODUCTION AND SCOPE

1.1 Purpose and Objectives

Data Leakage Prevention [DLP] is an approach to protect business sensitive Information from data breaches and other types of unwanted data disclosure. Key drivers for establishing DLP within Organisations include regulatory compliances, intellectual property protection and gaining additional visibility into data movement.

Everyday significant amounts of Information are used by businesses and functions that involve parties from both inside and outside the Group's network boundaries. Information can travel via a variety of paths and in many forms. For Example: e-mail messages; word processing documents; spreadsheets; database flat files and instant messaging.

For most Organisations globally, a significant amount of Information is classified as 'confidential', indicating that this Information needs to be protected from unauthorised access or exposure. Safeguards are deployed to protect this type of Information, however controls are often deployed inconsistently.

The result is that despite best efforts, Organisations around the globe are subject to continuous Information leaks. These leaks create significant risk to the Organisation, their customers and business partners with the potential to negatively impact their reputation, compliance with regulatory requirements and ability to do business.

The Group's Information is its most valuable asset after People. DLP solutions offer a multifaceted capability that provide a view of the location, flow, and usage of Group Information. These significantly increase the Group's ability to assess and manage the risks to its critical Information. Careful planning and preparation, communication and awareness training are paramount in deploying a successful DLP program.

To ensure its effectiveness and achieve its objectives, DLP must be delivered as a consistent programme, comprising of the below components:

1) Management – definition of the Group wide Strategy for sensitive data protection,
2) Discovery – identifying and categorising confidential (sensitive) data, location of the data and creating and maintaining data inventories,
3) Monitoring – tracing the routes and movements of the data, identifying data communication channels and flows, understanding sensitive data use context and patterns, identifying actual or attempted data misuse,
4) Protection – security policies and controls enforcement to prevent unauthorised access to data and data misuse.

This Information and Cyber Security Standard defines the minimum set of requirements for establishing and maintaining Data Leakage Prevention [DLP] in the Group by:

1) mandating Group-wide approach and strategy for DLP,
2) setting baseline requirements for the DLP approach and Strategy implementation,
3) defining required baseline configuration of Information Systems (including Application and Technology Infrastructure Components) to support Group DLP capabilities and objectives,
4) ensuring references to key processes (such as Security Logging & Monitoring, Training & Awareness, Security Incident & Response) are defined,
5) defining roles & responsibilities in the DLP area.

1.2 Risks

This Standard mandate that adequate DLP controls, are implemented to protect the Information Assets and Information Systems that comprise the Group's network.

Failure to adopt and implement this Information Security Standard may expose the Group to Risk which may result in:

- Disclosure of Sensitive Information by External Attacker and/or Trusted Insider

1.3 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, and countries/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 Information Assets, Information Systems and Technology Infrastructure that comprise the Group's network including components managed by Third Parties:

1) which are rated L4 & L5 ('Confidentiality' aspect),
2) which constitute communication channels/external gateways or identified data loss vectors,
3) which are identified by respective Owners and reported to DLP service as Assets where:
   a. potential impact propagation could take place, leading to L4[1] or L5[2] impact (i.e. target Asset is rated <L4 for 'Confidentiality', but the breach can lead to L4 or L5 damage),
   b. identified threat profile could expose the Asset to increased risk of data leakage or result in L4 or L5 impact propagation.

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 (in scope) regardless of the hosted environments [Production or Non-Production unless stated otherwise].

2. ROLES & RESPONSIBILITIES

Group Chief Information Security Office (Group CISO)

The Group CISO is accountable for establishing a Process(es) to ensure that the Group approach to Data Leakage Prevention is delivered in a consistent and comprehensive manner, across various technologies. In addition to that, CISO must appoint Process Owner(s) and ensure a model for Process effectiveness validations is in place.

[1] L4 refers to the GRAM level 4 impact, as assessed during impact assessment of Information Asset, Information System/Technology Infrastructure.

[2] L5 refers to the GRAM level 5 impact, as assessed during impact assessment of Information Asset, Information System/Technology Infrastructure.

Process Owner

Process Owner is accountable for defining and implementing an operational approach to Data Leakage Prevention in line with the Standard requirements. In addition, the PO is accountable for providing operational capability to support Information System/Technology Infrastructure/Application Owners to deliver required objectives of the Standard.

Information Asset Owner

Information Asset Owners are accountable for identifying and communicating specific DLP requirements for owned Information Asset(s), as well as consulting, if required, the DLP strategy for the Information Asset(s). The DLP requirements should be also communicated, together with the permissible use, to Information System Owners.

Information System Owner

Information System Owners are responsible for complying with the control areas of this Information Security Standard which are applicable to them to ensure that Data Leakage Prevention deployed to owned Information Systems is effective and aligned with the Group approach. They are also accountable for ensuring that the Technology Infrastructure Owners do correctly apply the controls as set out in this standard.

Technology Infrastructure Owner

Technology Infrastructure Owners are responsible for complying with the control areas of this Information Security Standard which are applicable to them to ensure that Data Leakage Prevention requirements for the owned Technology Infrastructure are met (by applying and maintaining respective configuration and operational procedures).

Application Owner

Application Owners are responsible for complying with the control areas of this Information Security Standard which are applicable to them to ensure that Data Leakage Prevention requirements are embedded or configured on the Application level (when applicable and required).

CISO ICS Standards & Controls

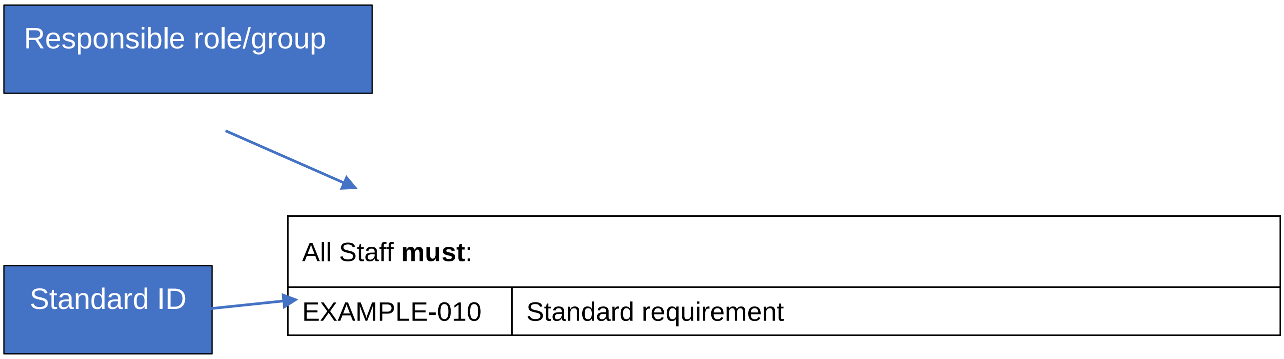
The CISO is the owner of this Information Security Standard and will ensure the document is updated to an agreed schedule.

Note: The Responsible role who ‘must’ execute against a standard can do so either directly or by delegation. Where this is the case and a delegate exercise the control, the named role remains accountable.

All roles & responsibilities including their correlations 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: Operational Approach Definition and Maintenance

3.1.1 Process Definition and Governance

Group CISO **must**:	
DLP-001	Establish an operational definition to the approach to ICS Data Leakage and Prevention by: 1) establishing Process(es) for Data Leakage Prevention, 2) appointing Process(es) Owner(s), 3) defining a model for Process effectiveness, oversight, and compliance validation. *[Reference: ERMF – Process Owner definition]*

Process Owner **must**:	
DLP-002a	Define an operational approach to DLP by: 1) defining BAU and operational Process procedures by describing and documenting operational activities in the DLP area, 2) ensuring the precise and accurate Process documentation is maintained, 3) defining and documenting the scope of the DLP related activities in line with: a) the baseline requirements of the Standard; b) risk-based (threat-led approach); and c) identified (and prioritised) data loss vectors, 4) determining and documenting operational requirements and procedures for Information System/Technology Infrastructure/Application Owners (such as OS configuration guidelines, DLP agent installation manual, etc.) essential to ensure predefined compliance level (with the Standard requirements). *Note: The control statement requires PO to document the operational approach, i.e. Process as well as to provide all supplementary documentation required for the Process to operate affectively. The final scope and approach to the DLP activities is based on the baseline requirements of the Standard and risk-based approach, i.e. may be changing as driven by threat landscape and profile of the IT Asset in the Group.*

Process Owner **must**:	
DLP-002b	Ensure that the operational approach covers the essential DLP components: 1) Management (please refer to ‘Data Management’), 2) Discovery (please refer to Data Discovery), 3) Monitoring (please refer to Data Monitoring‘ 4) Protection (please refer to Data Protection); and covers data in-use (end-point), at-rest (storage) and in-transit (network). *[Reference: Control Area: DLP Key Components’;* Baseline DLP Requirements for Assets and Information*’]*
DLP-002c	Ensure that a risk-based approach to scoping and determining the DLP strategy considers: 1) monitored asset criticality (i.e. *Confidentiality* impact rating), 2) identified and applicable risk/threat factors, 3) identified data loss vectors, 4) baseline requirements of the Standard. *[Reference: Appendix* - Baseline DLP Requirements for Assets and Information*]*

3.1.2 Operational Capability Delivery

Process Owner **must**:	
DLP-003	Deliver operational capability to ensure DLP accountabilities of the Information System/Technology Infrastructure/Application Owners can be fulfilled by: 1) deploying and maintaining the BAU required to ensure consistent and compliant Process is present, 2) identifying, deploying, and maintaining resources required to support Process objectives (such as tooling, operational procedures, etc), 3) defining and communicating operational and configuration guidelines for various technologies available in the Group.
DLP-004	Ensure that a model for Process effectiveness and compliance with the Standard is present by: 1) documenting the DLP approach and strategy, 2) documenting and communicating operational procedures to impacted stakeholders, 3) defining Process effectiveness metrics, approach to issue identification and data quality checks, 4) determining escalation paths for issue management, 5) continuous improvement, 6) MI and reporting: a) the overall state of the DLP services, b) monitored hosts compliance, c) DLP issues, event, and incidents.
DLP-005	Periodically (at least annually) review and update the DLP strategy to ensure it supports Standard’s objectives delivery.

Process Owner **must**:	
DLP-006	Ensure that any tools deployed to support DLP purposes: 1) actively control monitored hosts compliance status, 2) ensures coverage of hosts in scope of the DLP approach and strategy, 3) enables remediation of issue identified by the DLP tool, 4) is integrated with applicable Group solutions (such as AD, SIEM, security monitoring tools, SCCM), 5) have access control and adhere to Group's Identity and Access Management Standard, 6) does not compromise host security by partnering with respective technology owner during DLP implementation, 7) supports predefined DLP rules and configuration enforcement, 8) is documented (architecture, configuration, data flows, services provided). *[Reference: Security Logging and Monitoring Standard, Identity and Access Management Standard]*

3.2 Control Area: DLP Key Components

3.2.1 Data Management

Process Owner **must**:	
DLP-007a	Ensure that the DLP strategy and operational approach is aligned with the Group approach to Information classification and handling. *[Reference: Information Classification Standard, Information Handling Standard]*
DLP-007b	Ensure that DLP process is aligned with and supports Incident Management and Response processes, i.e.: 1) any events or incidents identified in the DLP area are reported and handled in a timely manner, 2) applicable prima facie evidence is provided to support incident investigation process. *[Reference: Security Incident and Response Management Standard]*
DLP-007c	(On best effort basis) Report identified training and awareness needs (in DLP area) to respective Process Owner(s).

3.2.2 Data Discovery

Process Owner **must**:	
DLP-008a	Define and deploy data discovery capabilities, which: 1) use the Group approach to Information classification for determining sensitive data repositories and identification patterns, i.e.: a) determine the sensitivity of the Information based on the Information Asset Register and corresponding 'Confidentiality' rating, b) address the Information Asset representation in terms of sensitive data fields, patterns, and attributes, as defined by Information Asset / Application / Information System / Technology Infrastructure Owner, c) ensure the Information Assets rated L5 and L4 for Confidentiality are in scope of the data discovery approach,

Process Owner **must**:	
	d) optionally, include the L1-L3 *Confidentiality* rated Information Assets, based on identified DLP related risk/threat profile. 2) uses Group Information Systems and Technology Infrastructure (asset) repositories to determine the scope and applicability the data discovery scans, 3) locate sensitive data at-rest, and (if required) notify the accountable parties to remediate, 4) notify respective Information System/Information Asset Owners to undertake data clean ups and removal if they deem the data is no longer required. *[Reference: Information Classification Standard, DLP-008c, DLP-271]*
DLP-008b	Perform periodic data discovery scans for data in rest, in line with predefined DLP approach and Strategy, in order to initiate and support activities required to record, secure and relocate the data (as performed by accountable parties). *Note: The actual scope of the data discovery scans (i.e. categories of Assets covered) is determined by the Strategy.*

Application Owner or Information System Owner or Technology Infrastructure Owner **must**:	
DLP-008c	Report to Process Owner the data representation for L4 and L5 ('Confidentiality' rated) Information Assets in Information Systems or Technology Infrastructure, which are rated L4 or L5 ('Confidentiality' aspect) and ensure applicable DLP controls that are defined by Group has been implemented.

3.2.3 Data Monitoring

Process Owner **must**:	
DLP-009a	Define data use and flows monitoring approach to monitor the data in transit and in use to detect potential data misuse or unauthorised transfers.
DLP-009b	Ensure that the monitoring approach considers: 1) identified data loss vectors, in line with the predefined Strategy and approach, 2) asset exposure to DLP threats and risks, as per Strategy, 3) monitored data sensitivity, as per its *Confidentiality* classification, 4) data content and known or identified data flow/use anomalies, 5) baseline requirements, as listed in Appendix – section 0 " 6) Baseline DLP Requirements for Assets and Information". *Note: Data content analysis can be based, for example, on: rules and regular expression to identify data attributes/specifics, exact data matching / fingerprinting, statistical / dictionary analysis of the content, sensitive data categories matching.*
DLP-009c	Ensure that monitoring capabilities (as mandated in DLP-009b) are deployed either independently within the DLP Process or embedded in Security Logging and Monitoring Process. *[Reference: Security Logging and Monitoring Standard]* *Note: the DLP related monitoring may be delivered withing the DLP Process or embedded in the SLM Process – as long as the control objectives are met, the implementation aspects are fully under PO discretion.*
DLP-009d	Ensure that any events or incidents identified are handled and managed in a timely manner, in line with the applicable Group Process(es).

Process Owner **must**:	
	Note: The events or incident should be either handed over to Group Incident Management Process or managed in line with the documented and predefined approach within the DLP Process capabilities.
DLP-009e	Ensure that DLP monitoring and auditing events are: 1) received, complete and retained in a central repository, 2) protected from tampering and disclosure, 3) archived in line with required retention requirements (as per Group Records Management Standard), 4) available to authorised stakeholders to discharge their responsibilities, and 5) maintain key attributes, such as: a) Event type and ID (if available) b) Event source c) User Identifier (if applicable) d) Date and time stamp e) Host Identifier (if applicable) f) Event description g) Event severity h) Task category i) Log type/name (if applicable).

3.2.4 Data Protection

Process Owner **must**:	
DLP-010a	Define and enforce (where applicable and technically feasible) DLP policies and data protection mechanisms to proactively prevent sensitive data from leaving the Group's IT environment. *Note: Enforcement of the data protection may be executed as centrally enforced configuration policy (such as AD GPO, dedicated agent delivered, etc.) or by defining and publishing configuration guidelines for specific technologies or platforms, to be then implemented by accountable stakeholders.* *[Reference: DLP-270]*
DLP-010b	Ensure that the data protection approach and enforcement consider (where applicable): 1) identified and prioritised data loss vectors, as defined in the Strategy 2) asset exposure to DLP identified threats and risks, as per the Strategy, 3) sensitivity of the data in question as per its *Confidentiality* rating, 4) data content and data use context, 5) baseline requirements, as listed in Appendix – section 0 " 6) Baseline DLP Requirements for Assets and Information". *Note: Data protection policies can be delivered as enforced IT Asset configuration (for example through dedicated DLP agent) or pre-defined configuration guidelines, mandatory for implementation. This is applicable to data at rest, in motion and in use. Data protection does not only limit to automatic mechanisms deployed to IT assets, but also covers Group level rules and guidelines enforcement, such as printing policy, email use policy, etc.*
DLP-011	Ensure that any actual breach or attempt to breach the data protection policy is reported and handled in line with the Group Incident Response and Management Standard.

3.3 Control Area: Key Implementation Aspects

Process Owner **must**:	
DLP-200	Deliver and maintain (DLP related) operational and configuration guidelines for technology and products used in the Bank (in scope of the DLP approach and strategy).
DLP-210	Ensure that the guidelines: 1) consume baseline requirements of the Standard (including baseline requirements for data in use, transit and at rest – as listed in the section 0 " 2) Baseline DLP Requirements for Assets and Information"), 3) include (optional) enhanced controls (together with the guideline for their applicability), 4) do not interfere with the hosts operational capacity, 5) are aligned with vendor specification and recommendations (where technically feasible), 6) are embedded in the standard technology build (if feasible), 7) include required network/communication configuration and compatibility list/issues, 8) are tested before communicated for deployment. In addition to the above, technical, or operational procedures, must be shared to ensure maintenance and oversights over required DLP configuration.
DLP-220	Define and support enhanced DLP approach or requirements (if required) based on: 1) criticality of the IT Assets ('*Confidentiality*' impact rating, as defined through the S-BIA), 2) architecture, DLP threat exposure and threat intelligence, 3) specific business or technology context of Information System (or Technology Infrastructure) operations, as determined by System Owner, 4) IA specific needs, if determined by Information Asset Owner.

Information Asset Owner **must**:	
DLP-230	Identify Information Asset specific DLP requirements, share them with Process Owner and immediately report to Process Owner any changes to the requirements. *Example: specific regulatory or business context requirements*
DLP-240	Consult the DLP strategy and approach for Owned Information Asset (if requested by Process Owner) and take timely action to respond to Process Owner when there is anomaly identified and reported.

Information System Owner **must**:	
DLP-250	Identify Information System specific DLP requirements and report them to Process Owner. *Example: specific regulatory or business context requirements*
DLP-260	Oversee and maintain the compliance of the owned Information System with the DLP requirements (as defined and communicated by the Process Owner) by: 1) regular review of DLP standard requirements pertaining to owned Information System and processed Information Asset(s), 2) adopting and adhering to DLP solution as appropriately recommended by DLP Process Owner,

	3) continuously monitoring deployed DLP solutions to ensure that their effectiveness is not compromised due to technology or architecture changes, 4) ensuring that data representation of processed Information Asset(s) processed, is onboarded to DLP solution (if required) to avoid potential data leakage, 5) taking timely action and respond to DLP Process Owner when there is anomaly identified and reported, 6) taking timely action, as requested by Process Owner, to ensure sensitive data is relocated or removed (when required).

Technology Infrastructure Owner **must**:	
DLP-270	Ensure the required configuration and operations (as shared by Process Owner) are deployed and maintained effectively for owned Technology Infrastructure to meet the DLP requirements.
DLP-271	Oversee and maintain the compliance of the owned Technology Infrastructure with the DLP requirements (as defined and communicated by the Process Owner) by: 1) regular review of DLP standard requirements pertaining to owned Technology Infrastructure and processed Information Asset(s), 2) adopting and adhering to DLP solution as appropriately recommended by DLP Process Owner, 3) continuously monitoring deployed DLP solutions to ensure that their effectiveness is not compromised due to technology or architecture changes, 4) ensuring that data representation of processed Information Asset(s) processed, is onboarded to DLP solution (if required) to avoid potential data leakage, 5) taking timely action and respond to DLP Process Owner when there is anomaly identified and reported, 6) taking timely action, as requested by Process Owner, to ensure sensitive data is relocated or removed (when required).
DLP-280	Allocate sufficient Technology Infrastructure capacity (storage and computing power) for DLP related configuration or services (in line with Process Owner configuration guideline(s)).
DLP-290	Ensure that technology and products onboarded provides required ability to ensure compliance with Group's approach to logging and monitoring (non-functional requirements).
DLP-300	Identify technology or use specific DLP needs and report them to the Process Owner.
DLP-310	Report to Process Owner any issues or problems identified, that can impact hosts DLP capability.

Application Owner **must**:	
DLP-320	Ensure the required configuration and operations (as shared by Process Owner) are embedded, deployed, and maintained effectively on the Application level to meet the DLP requirements.
DLP-330	Ensure onboarded Applications comply with the Group's approach to DLP (non-functional requirements).
DLP-340	Inform the Process Owner about specific DLP requirements for the Application (if any).
DLP-350	Report to the Process Owner any issues or problems identified that can impact the Application DLP capability.

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 Definition of Information Asset and S-BIA

Topic	Document	Reference
Defining Information Assets for Standard Chartered and determining the method for its classification.	Information Assets Methodology	CISRO ICS Policy SP
Impact Assessment Methodology for Information Systems and underlying Technology infrastructure	Security BIA Methodology	CISRO ICS Policy SP

7.2 Baseline DLP Requirements for Assets and Information[3]

Reference	DLP at Rest [Storage]	DLP in Transit [Network]	DLP in Use [End-points]
Information Assets	Information Assets (and the data representing the IA) stored within the Group (including 3rd party hosted Technology Infrastructure) encryption[4] (Group approved encryption solutions), in line with classification and handling requirements (as defined in Information Handling Standard). *For Example: Network File Shares [NFS], Storage Area Networks [SAN], SharePoint sites and Databases.*	Encryption[5] of the IA (and their data representation) while in motion internally and externally, in line with Information Classification & Information Handling Standards requirements.	Identification of the sensitive information location (data discovery scans) for IA (and their representation) rated L4 or L5 for the '*Confidentiality*'. Security assessment of the (identified) sensitive data location (i.e. whether the location fulfils the security requirements aligned with Information classification). The assessment is considered as verification of the declared Information System/Technology Infrastructure classification with identified data sensitivity. Initiation of Information relocation or removal (if required).
IT Assets	Full disk encryption[6] on Group issued or Group approved Mobile Devices and portable storage devices, in line with Information Handling Standard. DLP services deployment on Group issued or Group approved Mobiles Devices.	Protection of the Group Information by preventing the transmission of such Information which are at risk of disclosure (for example – by applying network segmentation, Web application firewalls, internet browser proxies, DLP network scanners which can detect/block/prevent	Data discovery scans to locate sensitive Information (IA and their representation rated L4 or L5 for 'Confidentiality') on the end-user Infrastructure. USB ports (or any such removal media interfaces) blocking by default on laptops, desktops, servers, workstations unless authorised for use by exception process. Initiation of semi-annual reviews of the user access

[3] The accountability for the actions is as per the Standard control statements. The baseline requirements list the minimum-security measures required to provide data protection mechanisms for data in use, at rest and in transit. The mechanisms must be considered in the DLP strategy, in line with the protected Information classification and then either enforced as mandatory configuration centrally or by creating configuration guidelines for Asset Owners to implement.

[4] Encryption is considered as one of the DLP mechanisms, but the accountability for the implementation of applicable encryption requirements is outside the DLP PO scope, as defined in relevant ICS Standards.

[5] See above

[6] Encryption is considered as one of the DLP mechanisms, but the accountability for the implementation of applicable encryption requirements is outside the DLP PO scope, as defined in relevant ICS Standards.

Reference	**DLP at Rest** [Storage]	**DLP in Transit** [Network]	**DLP in Use** [End-points]
		suspected leakage of sensitive information,).	granted to portable storage devices use. DLP service deployment[7] to printers or other printing services to ensure business access limitations enforcement and monitoring processed Information for potential misuse and disclosure. Restrict/control movement of and downloading of sensitive data to removable media or other drives.
Communication channels		Group communication channels (email, corporate chat, internet access and other network channels) monitoring[8] for unauthorized data access and disclosure. Unapproved communication channels and services blocking[9] to prevent malicious or unintentional data disclosure.	Enforcement formal policies for the Group communications channel acceptable use. Enforcement of formal policy for end-user Information labelling/classification. User activity monitoring in terms of identified data loss vectors use (such as portable storage devices use, access to sensitive data, etc.)

[7] The deployment is considered either as implementation of dedicated DLP agents, central configuration enforcement (for example through GPO) or delivery of specific configuration guidelines for Technology Infrastructure Owners to implement.

[8] The monitoring can be either delivered operationally as a part of the DLP Process activities or by other Processes or activities, based on the DLP PO requirements or guidelines for secure configuration

[9] Blocking of unwanted or unauthorized activities may be delivered as a part of the DLP Process activities or by other Processes or operations, based on the DLP PO requirements or guidelines for secure configuration.

8. Appendix A – Version Control Table

Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
CISRO Policy	Annual review includes: 1. Migrated existing standard to ERM standard template. 2. The existing Data Leakage Protection Standard document has been uplifted into this standard. 3. Consultation feedback, corrections incorporated.		Liz Banbury	1.0 [02-Oct-19]	2-Oct-19	2-Oct-19
CISRO Policy	The following have been updated: - Scope to include Technology Infrastructure. - Standard Ids DLP-010, DLP-030, DLP-070, DLP-080, DLP-110, DLP-120, DLP-130, DLP-140, DLP-190 and Section 6.2 added.		Liz Banbury	1.1 [05-Dec-19]	4-Dec-19	4-Dec-19
CISRO Policy	The following have been updated: 1. Editorial changes: Document template uplift (in line with new ERM requirements); glossary and regulatory references updated; section 7.1 – references updated		Samantha Finan, Global Head, ICS Policy, Standards and Reporting	2.0 [14-Dec-21]	14-Dec-21	1-Jan-22

	Applicability/scope updated 2. Controls for DLP in use/transit/at rest – moved to the table in the Appendix section (DLP-110 to 190) 3. Information Custodian role removed, new roles introduced: Process Owner, Technology Infrastructure Owner, All Staff, People Manager Scope & applicability changes 4. New controls introduced: DLP-001 to DLP-009, DLP-011; DLP-200 to 360 5. Controls replaced: DLP-010 to 030; DLP-050 to 100 6. Controls removed: DLP-040 7. Alignment in line with RTF v4.0					
CISRO ICS Policy	**1.** Template updated to ERM Standard template v5.6 2. Changes made w.r.t ICS Policy Changes Requests: ICSCR-18Feb2022-1 – Removed as covered in Acceptable		Paul Hoare, Head, ICS Policy and Best Practice	2.1 [13-Nov-2023]	13-Nov-23	14-Nov-23

	Use Standard – DLP-360, DLP-370. 3. People Manager to People Leader.					
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	2.2	04-Dec-14	16-Dec-24