Secure Handling of Production Data Standard

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-Apr-27

Table of Contents

1. INTRODUCTION AND SCOPE 4

1.1 Risks 4

1.2 Scope 4

2. ROLES & RESPONSIBILITIES 5

3. STANDARD REQUIREMENTS 6

3.1 Control Area: Operational Design and Approach 6

3.2 Control Area: Owner Authorisation and Handling 6

4. INFORMATION & SUPPORT 7

4.1 General Information and Support 7

4.2 Reporting Non-Compliance 7

4.3 Breach of this Standard 8

5. GLOSSARY 8

6. REGULATORY/INDUSTRY REFERENCES 8

7. Appendix A – Version Control Table 8

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. Correction of the document version 4. 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

Testing which involves Group data has a potential for misuse, unauthorised data disclosure and loss of data leading to possible negative impact to the Group in front of regulators, its stakeholders, and customers.

This Information and Cyber Security ("ICS") Standard defines minimum requirements for the secure handling of Group's Production Data when being used in testing.

Testing, by default to take place in a Non-Production environment using Synthetic Data in order to ensure the Confidentiality of Production Data remain protected.

This Standard applies only to a situation where Group's real/raw Production Data to be used in testing.

Examples of when it may be appropriate to use Production data in testing

1. Providing Production support for error fixing.
2. Volume Testing where it is not practical to produce the correct spread and mix of test data required to generate accurate test results.
3. Parallel Testing to compare the output of the new system against a live system.
4. Stress Testing where it is not practical to produce the correct spread and mix of test data required to generate accurate test results.
5. Data Conversion Testing.

Using actual or raw Production Data in testing provides confidence to Business that the Information System being tested is processing Information and functionality as intended. On the other side, using Production Data in testing does add an increased risk of that data being exposed to possible data leakage or unauthorized disclosure of Group Information.

Note: This Standard shall be read in conjunction with the Group Data Management Policy framework on GovPoint.

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

Process Owner (PO)

Process Owner i.e., Framework to Enable Data eXtraction [FEDX] process, 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.

Information Asset Owner

Information Asset Owners are accountable for granting permissible use of owned IA, i.e., approving the use of owned IA for testing on the Information Systems and Technology Infrastructure.

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.

CISO ICS Standards & Control

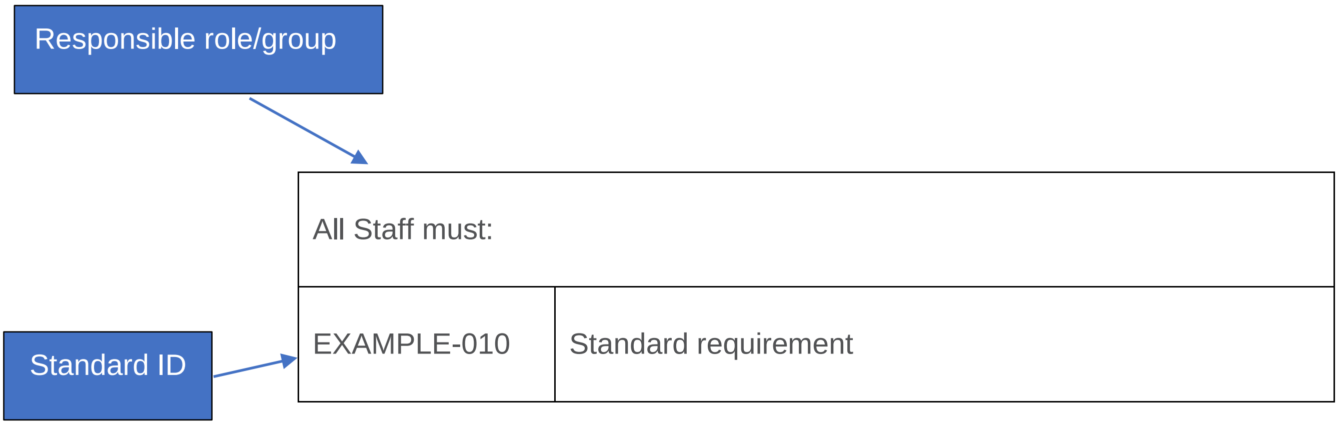
The CISO is the owner of this Security Standard and will ensure the document is updated to an agreed schedule.

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: Operational Design and Approach

Process Owner **must**:	
SPD-010	Establish an operational process for extraction of data from production Systems and rollout the process for Group wide adoption. The process, at the minimum, to ensure: a) a request submission method is available, b) the method obliges requestor to include the purpose for Production Data need in testing, c) the method requires Start date of testing and an End date[1], d) the requests having an accountable individual for all activities related to testing, e) the requests are approved by right owners of requested data and for the requested purpose before extraction; and f) a help guide is available for to extract & maintain Confidentiality of Production Data throughout its usage in testing.
SPD-020	Establish a governance model that: a) allows having a visibility on the Group's adoption of the process and variations to the process. b) measures the process effectiveness and compliance to this Standard; and c) verifies the erasure of Production Data used in testing after its End Date & Owner notified.

3.2 Control Area: Owner Authorisation and Handling

Information Asset Owner **must**:	
SPD-030	Approve requests for owned IA by ensuring: a) the request having an accountable individual for all activities relate to testing,

[1] By the End Date the Production Data used in testing to be erased.

	b) the request having a purpose and it is approved only for requested purpose, c) the request having a Start and End Date & includes plan for erasure by End Date, d) a risk-based decision is made; where necessary consult relevant risk experts (e.g., the ICS, Privacy, Compliance, Legal), e) the approval is not permanent (e.g., approval becomes invalid when IA ownership changes).
SPD-040	Disallow use of following in testing due to potential regulatory, compliance impact: a) Personal Data [also referred as Personally Identifiable Information (PII) in certain Countries/Regions], b) Client impacting Information, c) Live Primary Account Number [PAN - PCI-DSS v3.2.1 prohibits using in testing]. *Note: the IA Owner shall consider allowing the above listed a & b if the test environment is S-BIA rated and ICS controls are applied in conjunction to the rating.*
SPD-050	Approve a Third Party engagement in testing by ensuring: a) the Third Party Security Assessment [TPSA] is completed, b) there is a Confidentiality agreement in place, c) the Group Data to be returned or secure destroyed at the end of engagement. *[Reference: ICS Standard Security in Interactions with Third Parties [STP].]*

Information System Owner and/or Technology Infrastructure Owner **must**:	
SPD-060	Allow Production Data extraction by ensuring: a) a formal request is received, and only Owner approved data are provided, b) data extraction follows the help guide by the Process w.r.t SPD-010; and c) an audit trail is available for all requests.
SPD-070	Ensure owned test environment is S-BIA rated, in correlation to the Production Data getting migrated to and ICS controls are applied corresponding to its rating. *[Note: The S-BIA rating of test/non-Production environment to follow the Group's S-BIA Methodology. As per the S-BIA Methodology, the Production S-BIA rating applies to all environments. If the test/non-Production environment impact is expected to be different, then an independent assessment to be conducted].*
SPD-080	Ensure owned test environment are erased for Production Data after completion of testing.

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*

7. Appendix A – Version Control Table

Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
CISRO ICS Policy	Uplift of existing Production Data for Testing Guideline document to a Security Standard	Material	Darren Argyle	1.0 [15-Dec-19]	15-Dec-19	15-Dec-19
CISRO ICS Policy	Annual Review – Alignment of Scope, Risks, Roles & Responsibilities with correct functions. Amended statements: Administrative, Editorial: SPD-010-070 (roles alignment), SPD-130, SPD-150 Administrative, Removed: SPD-090, SPD-110, SPD-140	Non-material	Liz Banbury [delegate of Group CISRO]	1.1 [20-May-21]	8-Jun-21	1-Jul-21

CISRO ICS Policy	This refresh includes the following enhancements: 1. Document template updated (in line with the ERM template). 2. Risks section realigned with ICS RTF v4.0. 3. Introduced the Process Owner [PO] role that governs & manages the Group's Framework to Enable Data eXtraction [FEDX] process and proposed the PO role with high level responsibilities. 4. Information Asset Owner [IAO] approval to ensure an accountable individual for all testing related activities, requests having specific purpose, includes data erasure plan by Test end date & not to provide permanent approvals [e.g., IAO changes]. 5. IAO is guided with what types of real/raw Production Data to be avoided in testing. This avoids potential regulatory impact. However, the IAO shall take a risk-based decision if test environment is S-BIA rated and ICS controls applied accordingly. 6. Incorporated minimum control requirements in a	Material	Samantha Finan, Global Head, ICS Policy, Standards and Reporting	2.0 [22-Jun-22]	22-Jun-22	1-Jul-22

	Third-Party engagement for testing. 7. Information System/Technology Infrastructure Owner to ensure owned test environment is S-BIA rated & applied with ICS controls commensurate to its S-BIA rating for secure handling of Production Data in testing. 8. Production Data to be erased from test environment after test completion to avoid any data leakage exposure to unauthorized users. 9. Consolidated existing use cases, hence the proposed Standard has become environment independent for testing Production Data. 10. Replaced Riskpod references with Group ERM's GovPoint.					
CISRO ICS Policy	1. Template update to ERM Standard template v5.6 2. Included the first 2 ICS risk sub-types in line with the ICS RTF v5.0 3. Changes made w.r.t ICS Policy Change Requests – SPD-070-ICSCR-20Sep2022-1 (Clarification of S-BIA for Testing Environments).	Non-material	Paul Hoare Head, ICS Policy and Best Practice	2.1 [09-Mar-23]	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 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