Group Information & Cyber Security Standard: Secure Handling of Production Data

Version No	1.0
SCB Rulebook Document Reference	09-STND-0001-23
Document Type	Standard
Parent Document	Group Information and Cyber Security Policy
Document Approver Name	Darren Argyle
Document Approver Job Title	Group Chief Information Security Risk Officer
Document Owner Name	Liz Banbury
Document Owner Job Title	Head of Information and Cyber Security Policy
Document Contact Name	Bali Chandramouli
Document Contact Job Title	Associate Vice President, CISRO
Business Scope	All Businesses
Function Role	All Functions
Geography Scope	Global
Status	Approved
Approval Date	15th December 2019
Effective Date	15th December 2019
Last Review Date	15th December 2019
Next Review Date	15th December 2020

Contents

Version Control Table

Version	Issue Date	Changes	Primary Reviewer	Secondary Reviewer	Approver
1.0	15th December 2019	Uplift of existing Production Data for Testing Guideline document to a Security Standard	CISRO Policy	Liz Banbury, Sean Coppinger, Draco Wong, Gary Teo, Shameek Kundu, Liu Xinhua, Philip Tan, Prometheus Yang, Sivaswamy Rathnabhan, Samuel Rajkumar, Ruth Standring, Vijay Jairaj, CISRO ISO All, Heads of Information and Cyber Security	Darren Argyle

1. INTRODUCTION AND PURPOSE

This Information Security Standard defines minimum control requirements for the secure handling of the Group's Information Assets ["IA"] when being used for testing purposes.

Testing should by default always take place in a non-Production environment using synthetic data in order to ensure that services are not interrupted, and that data is neither contaminated nor compromised.

However, there are specific and exceptional circumstances where the default cannot be adhered to:

1. Testing in a Production environment, usually User Verification Testing ["UVT"] for the Business / Information System Owner to verify that the Production environment is performing correctly.
2. Testing in a Production environment has been mandated by the Vulnerability Identification and Management Standard.
3. Production data is required to be used in a non-Production Environment for testing. Where this is the case key components of that data should always be masked or removed so that personal Information cannot be identified.

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.

Testing in Production, if required provides assurances to the Business that the Information Systems they rely on are functioning correctly and securely. Testing in Production does add an increased risk to the Production environment though as Production data could be contaminated and/or test activities could interfere with Production processes leading to unauthorized disclosure of Information.

Using Production data within a non-Production environment, if required provides assurance to the Business and to the Testing Managers that the Information System being tested is processing Information and functionality as intended. Using Production data in a test environment does add an increased risk of that data being compromised leading to unauthorized disclosure of Information.

1.2 Risks

The Secure Handling of Production Data Standard mandates that adequate controls are implemented to protect Information Assets extracted from Group's Production Information Systems.

Failure to adopt and implement this Information Security Standard may expose the Group's IAs to risks of Information disclosure, inaccurate or incomplete Information or disruption to business services due to unauthorised access which may result in:

- Loss of customer trust.
- Adverse publicity and reputational damage.
- Compromise of Group, Staff, Customer Information.
- Regulatory fines

1.2 Scope

This Security Standard is mandatory and applies to Group businesses and environments except where explicitly prohibited by local Law or Regulation [see section 4.2. Policy Non-Compliance].

The scope covers the Group IAs either extracted from the Group's Production Information Systems and Technology Infrastructure which are then used for testing within or outside the Group, including by the Third Parties and the use of data for testing within a Production and non-Production environment.

2. ROLES & RESPONSIBILITIES

Information Asset/System Owner

The Information Asset/System Owners are responsible for compliance with the control areas of this Information Security Standard which are applicable to them and accountable for ensuring that the Information Custodians do correctly apply the controls as set out in this Standard.

As first line role holders they must have in place a model for validation of control existence and effectiveness.

Information Custodians [T&I]

The Information Custodian is responsible for compliance with the control areas of this Information Security Standard which are applicable to them and for the correct selection and application of controls on their Information Systems and Technology Infrastructure.

As first line role holders, they must have in place a model for validation of control existence and effectiveness.

Staff

All Staff must ensure the Group Information Asset allowed for use in testing under their care are handled and protected in-line with the requirements of this Standard.

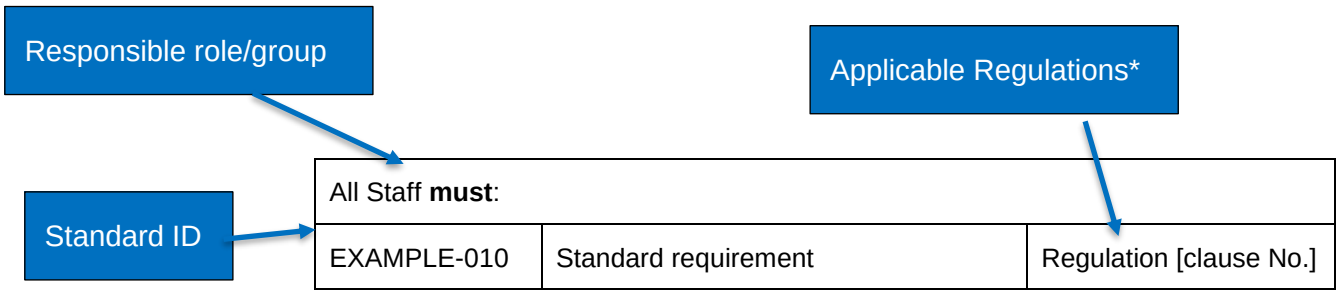
Group Chief Information Security Risk Office [CISRO]

The Group CISRO is the owner of this Security Standard and will ensure the document is updated to an agreed schedule. As second line role holders, the Group CISRO will perform effectiveness reviews to monitor first line compliance with this Security Standard.

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 exercises the control, the named role remains accountable.

3. STANDARD REQUIREMENTS

This section outlines minimum mandatory Secure Handling of Production Data requirements that are set out in the following format:



*Applicable regulations are shown to outline the impact of non-compliance

3.1. Control Area: Securing Test Data in Production

Production Test Manager **must**:		
SPD-010	Ensure that Approval has been obtained from the Information System Owner prior to migrating test data, creating testing accounts or carrying out any testing activities in Production. The Approval must contain acknowledgement of the following: a) What test data is being used; b) Owner of the test data; c) Start and end dates of testing; d) How the test data will be securely migrated into Production; e) Controls in place to ensure that test data do not contaminate Production data; f) By when and by whom all test data will be removed from Production. *Note: If unmasked data is required a separate Approval with the Business justification is required*.	
SPD-020	Label all test data and test accounts in Production so that they are clearly identified	
SPD-030	Remove all test data and test accounts from Production by or before the expiry date of the approved testing period and notify the Information Asset Owner.	
SPD-040	Maintain a register of all the test data and test accounts in the Production environments which includes the following: a) What test data is being used; b) Owner of the test data; c) Start and end dates of testing; d) How the data will be securely migrated into Production; e) Controls in place to ensure that test data does not contaminate Production data; f) By when and by whom all test data will be removed from Production.	

Information System Owner **must**:		
SPD-050	Review and Approve all requests for testing prior to the migration of any test data and the creation of any test accounts in the Production environment. The Approval must contain acknowledgement of the following: g) What test data is being used; h) Owner of the test data; i) Start and end dates of testing; j) How the data will be securely migrated into Production; k) Controls in place to ensure that test data does not contaminate Production data; l) By when and by whom all test data will be removed from Production.	
SPD-060	Review the Production environments at least every twelve months to ensure no test data or test accounts exist outside approved periods.	
SPD-070	Ensure that all test data and test accounts are removed from Production by or before the expiry date of the approved testing period so that Production is not interfered with.	

3.2 Control Area: Securing Production Data in non-Production Environments

Test Manager/Data Requestor **must**:		
SPD-080	Ensure that Approval has been obtained from the Information System Owner prior to migrating Production data or carrying out any testing activities using Production data. The Approval must contain acknowledgement of the following: a) A valid business case and justification for using Production data; b) Start and end dates of testing; c) How the data will be securely extracted and migrated into the non-Production environment; d) Controls in place to ensure that the Production data is masked to secure any Personally Identifiable Information;	

	e) The number and roles of the persons who will have access to the Production data; f) Assurance that those with access are Group on-boarded and/or have the appropriate contracts and non-disclosure agreement [“NDA”] in place [in the case of Third-Party access]; g) That the transfer of any personal data cross-border is not prohibited; h) By when and by whom all test data will be removed from non-Production. *Note: If unmasked data is required the business case must have a clear rationale as to why live personal data is required*.	
SPD-090	Label all Production data so that it is clearly identified and not transferred back to Production.	
SPD-100	Ensure that data is masked or removed to preserve the confidentiality of all Personally Identifiable Information [“PII”], if appropriate. *Note: Data masking must be carried out at source and not after the data transfer.*	
SPD-110	Verify the Production data before and after the data masking exercise to ensure its validity and accuracy.	
SPD-120	Remove all Production data from the test environment by or before the expiry date of the approved testing period and notify the Information System Owner.	

Information System Owner **must**:		
SPD-130	Review the business case and justification for the use of Production data and approve ONLY when the controls and risks have been fully understood.	
SPD-140	Review the business case and justification for the use of unmasked Production data and approve ONLY when the controls and risks have been fully understood	
SPD-150	Ensure that the Test Manager has taken all reasonable steps to protect the Production data in migration to the test environment.	

3.3 Control Area: IAs in Proof of Concepts ["POC"]

Information Asset Owner **must**:		
SPD-160	Re-rate the IAs to be deployed for the POC based on the context and use of that IA within the POC. IAs rated 5 or 4 must not be allowed in any POC.	
SPD-170	Ensure the POCs are legally governed. *Note: Legal governing is to ensure the IAs shared for a POC are used only for intended purpose and they are securely managed throughout the test timeframe. The IAs must be destroyed securely as per Group's ICS Standard requirements or equivalent.*	
SPD-180	Ensure IAs rated 3 to 1 are masked before being used within a POC.	
SPD-190	Ensure that IAs rated 3 to 1 for Confidentiality and Integrity are protected before sharing [For Example: External Sharing].	

4. INFORMATION & SUPPORT

General Information and Support

- For queries relating to this Security Standard please contact the CISRO Policy team via: CISRO-ICSPolicy

Reporting Non-Compliance

- A dispensation must be obtained if any of the requirements mandated in this Standard cannot be met. Where a security requirement is necessary to meet a regulatory, legal or mandatory requirement compliance cannot be waived. Dispensation request to be submitted to dispensations, ICS.

Breach of this Standard

- Failure to comply with this Standard may result in formal action under the Group HR Disciplinary Policy, that could for serious breaches include termination of employment.
- Any actual or suspected breaches must be reported immediately to your People Manager or to your Compliance representative.
- All breaches of the policy and or it's associated standards will be escalated to the Policy Owner.

5. GLOSSARY

Term	Definition
Data Masking	*The process of concealing real Information via methods such as obfuscation, de-identification or scrambling to hide the original data so that it is not in clear text.*
Group	*Standard Chartered PLC, together with its subsidiaries and subsidiary undertakings.*
Information Asset	*Information defined into a class e.g. Client Information which has value to the bank.*
Information Asset Owner	*A named individual with accountability for the protection and permissible use of a set of information.*
Information Asset /System Owner Delegate/ Information Custodian Delegate	*A named individual with delegated authority to perform the activities associated with and allocated to the Names Roles.*
Information System	*A system represents a collection of technology that performs a discrete function based on information resources organized for collection, processing, maintenance, use, sharing, dissemination or disposition of information, which are delivered as a service to end users. A system is a set of interacting or interdependent components forming an integrated whole.*
Information System Owners	*A named individual with accountability for the existence and permissible use of a system.*
PII	*Personally, Identifiable Information is all Information determined by the Privacy Policy as that which could link an individual to their account and transaction data.*
Information Custodian	*A named individual, typically within the Technology & Innovation [T&I] function, responsible for providing secure processing of information to the level specified by the Information Asset or System Owner.*
non-Production Environment	*Development, test or other environment which is separated from the Production environment and where testing, development activities are conducted before moving settings and setups to the production environment. Otherwise known as Test Environments.*
Production Environment	*A real-time setting where programs are run and hardware setups are installed and relied on for organisational or commercial daily operations.*
Production Data	*This is all data [Information] that originates from a Production Environment.*
Production Test Manager	*Anyone conducting testing and managing the conducting of testing in a Production Information System [Environment].*
Proof of Concept ["POC"]	*A Proof of Concept is the evidence, typically deriving from an experiment or pilot project, which demonstrates that a design concept or business proposal is feasible. The systems or tools used in a Proof of Concept are typically incomplete and governed seperately from those systems deployed via a managed non-Production environment.*
Staff	*All persons employed by or working for the Group including contractors, consultants and secondees.*
Synthetic Data	*Synthetic data is Information that's artificially manufactured rather than generated by real-world events. Synthetic data is created algorithmically, and it is used as a stand-in for test datasets of production or operational data, to validate mathematical models and, increasingly, to train machine learning models.*
Technology Infrastructure	*Collection of hardware and software which provides the infrastructure upon which Information and Information Systems [For Example: Applications] are processed and run. [For Example: Networks, Firewalls, Servers [Operating systems and Databases] etc.]*
Test environment	*Development, test or other environment which is separated from the Production environment and where testing, development activities are conducted before moving settings and setups to the production environment. Otherwise known as non-Production Environments.*

User	*A member of Staff who is authorised to use Group Information Assets, Information Systems and Technology Infrastructure.*
UVT	*User Verification Testing is testing carried out by the Business User in a Production environment to verify that the Production environment is performing correctly.*
Vendors	*An external Organisation the Group has a commercial arrangement with for the provision of Goods and / or Services.*

6. APPENDIX

Regulatory/Industry References:

[REGULATOR NAME]	REGULATOR DOCUMENT	SECTION/Version