Payment Card Data Management

Version No	3.1
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
Effective Date	16-Dec-24
Approval Date	4-Dec-24
Next Review Date	30-Jan-2027

Table of Contents

Version Control Table

Document Author Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
Arti Singh Standards]	1.) Administrative changes introduced to update document template, references, roles and ownership. 2.) Duplicate ID PCD-120 under Data Protection changed to PCD-116	Non-material	Jamie Cowan Head, ICS Risk Framework & Governance	3.1	04-Dec-24	16-Dec-24

1 INTRODUCTION AND PURPOSE

This Information Security Standard defines control requirements for the Information Systems and Technology Infrastructure which processes Account Data.

Account Data Management is the identifying and protecting of Account Data regardless of whether you are an issuer, acquirer or merchant and includes the processing of Group data by Third Parties.

Account Data is found on both Credit Cards and Debit Cards whether they are Group issued cards or other company-issued cards.

Account Data is:

Account Data	
Cardholder Data includes:	Sensitive Authentication Data includes:
• Primary Account Number [PAN] • Cardholder Name • Service Code • Expiration Date	• Full Track Data (magnetic-stripe data or equivalent on a chip) • Card verification code • PINs/PIN block

Account Data is important data and therefore often a target for activities involved in financial fraud. Group is both an issuer and acquiring bank and therefore it is imperative that stringent security controls are put in place. Security controls which are not adequately mandated or deployed would allow vulnerabilities within Payment Card Systems which could be exploited by criminals.

1.1 Risks

The standard mandates that adequate controls are deployed to protect the Account Data while it is being processed.

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, 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 Group Information Assets which are processed and or used by the Group's Information System [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 Asset Owner

A named individual with accountability for the protection and permissible use of owned Information Assets in Information Systems and Technology Infrastructure.

Information System Owner

A named individual accountable for the protection of the owned Information System and compliance with applicable Control Statements.

Technology Infrastructure Owner

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

Process Owners (PO)

The PO to embed applicable requirements of this Standard within their process and within any suppliers, joint ventures and outsourced/off-shored activities for which they are responsible for.

The PO is responsible ensuring quality, timeliness and adequacy of provided data, and management information to measure appropriate coverage and performance of control points (and subsequent measurement) against ICS Policy and Standards.

In addition to that PO is accountable for providing operational capability to support Information Asset/System/Technology Infrastructure Owners to deliver required objectives of the Standard.

Group Chief Information Security Office (Group CISO)

The Group CISO is responsible for:

- Complying with the control areas of this Information Security Standard which are applicable to them.

- Ensuring the CISO Awareness team provide the Group with the appropriate awareness and training tools (messaging, content, strategy and governance and training support).
- Notifying OTCR as and when they become aware of any regulations relevant to ICS issued by non-financial services regulatory authorities;
- Identifying the relevant Process Owners responsible for implementing the regulation in their processes and informing OTCR;
- Implementing ICS Policy and Standards;
- Ensuring mechanisms are in place to demonstrate that necessary documentation and audit trail concerning implementation of ICS LRM requirements are maintained;
- Completing attestations to relevant regulatory authorities to confirm compliance to the relevant regulations; and
- Tracking remediation of gaps identified from LRM attestations in line with remediation programmes.
- As first line role holders, the Group CISO will additionally perform effectiveness reviews to monitor first line compliance with this Information Security Standard.

CISO ICS Standards & Controls

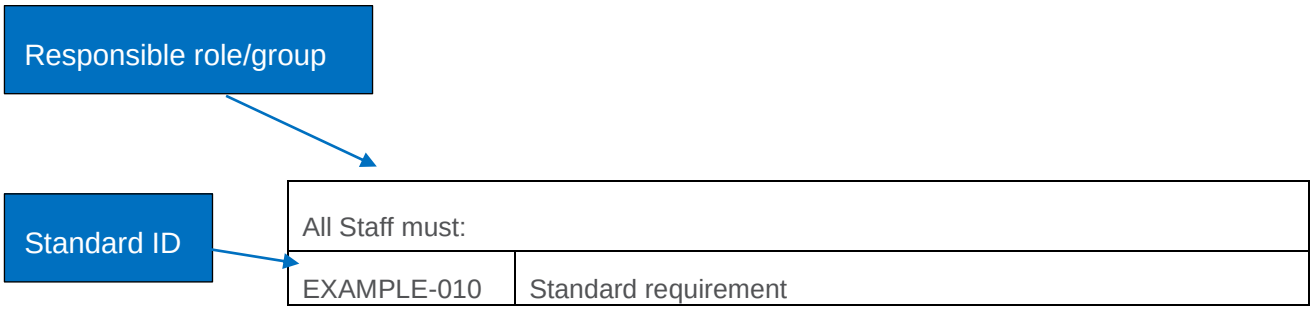
The CISO is the owner of this Security Standard and will ensure the document is updated to an agreed schedule.

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: Risk Assessment

Group CISO **must:**	
PCD-010	Establish a risk assessment process, which includes targeted risk analyses and perform a control effectiveness assessment at least every twelve months and upon significant changes to the Cardholder Data Environment. *[Reference: Information and Cyber Security Risk Management Standard]*
PCD-015	Define the scope of assessment for each PCI-DSS regulated market ('market entity').

3.2 Control Area: Architecture

Information Asset Owner **must**:	
PCD-020	Define and maintain a description of the Cardholder Data Environment which shows all the Payment Card Data flows across the systems and networks, which must be reviewed at least every twelve months and upon significant changes to the Cardholder Data Environment. *Note: Payment card data can be found in any location e.g. systems, shared folders, SharePoint sites, EUC, RPA, in-country as well as within our third-party environments.*
PCD-030	Maintain an inventory of system components that support the Cardholder Data Environment and review it at least every twelve months and upon significant changes to the Cardholder Data Environment. *[Reference: Information and Cyber Security Risk Management Standard]*

3.3 Control Area: Data Protection

Information System and/or Technology Infrastructure Owner **must**:	
PCD-040	Keep Payment Card Data storage to a minimum by implementing data retention and disposal policies that include the following: • Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements; • Specific retention requirements for Payment Card data; • Processes for secure deletion of data when no longer needed; • A quarterly process for identifying and securely deleting stored Payment Card data that exceeds defined retention; • Processes for controlling access to the shared folders where Payment Card data is stored. *[Reference: Secure Decommissioning and Destruction Standard]* *[Reference: Unstructured Data Storage Standard]*
PCD-050	Not store neither sensitive authorization data, nor full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere, CVC, CVV, three- four-digit numbers printed on either side of a payment card, PIN, etc.) after authorization, even if encrypted. *Note: In the case of issuers and companies that support issuing services, it is permitted to store the authentication data if there is a valid business justification and the data is securely stored.*
PCD-090	Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN.
PCD-100	Never use PAN as a Customer Reference Number or any type of Customer Identifier [e.g. user ID].
PCD-110	Render PAN unreadable anywhere it is stored by use of approved hashing and encryption methods. *[Reference: Cryptography Standard]*
PCD-116	Deploy a change- and tamper- detection mechanism to detect unauthorized modification to the HTTP headers and the contents of payment pages as received by the consumer browser and execute response activities to the ICS incidents identified. *[Reference: Security Incident and Response Management Standard, Security Logging and Monitoring Standard]*

3.4 Control Area: Encryption

Technology Infrastructure Owner **must**:	
PCD-120	Document and implement processes to protect keys used to secure stored Payment Card Data against disclosure and misuse. *[Reference: Cryptography Standard]*
PCD-130	Ensure that Payment Card Data is protected during transmission over open and public networks using approved encryption methods. *[Reference: ICS Standard Information Handling]* *[Reference: Cryptography Standard]*
PCD-140	Ensure wireless networks transmitting Payment Card Data or connected to the Cardholder Data Environment deploy approved encryption methods for authentication and transmission. *[Reference Cryptography Standard]*
PCD-150	Never send unprotected Live PANs by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat). *[Reference Information Handling Standard]*

3.5 Control Area: Media Handling

Technology Infrastructure Owner **must**:	
PCD-160	The Payment Card Data stored in the media must be encrypted. The physical movement of the media must be via secured courier or using other delivery method that can be accurately tracked.

3.6 Control Area: Security Awareness

Process Owner **must**:	
PCD-170	Maintain a list of service providers who process Payment Card Data on behalf of the Group including a description of the service provided.

Information Asset Owner **must**:	
PCD-180	Review a list of service providers who process Payment Card Data on behalf of the Group including a description of the service provided. *[Reference: Security in Interactions with Third Parties Standard]*

Group CISO **must**:	
PCD-190	Implement a formal security awareness program to make all staff with access to Payment Card Data aware of the Payment Card Data security policy and procedures.
PCD-200	Maintain a program to monitor service providers' PCI DSS compliance status at least annually. *[Reference: Security in Interactions with Third Parties Standard]*
PCD-210	Provide appropriate training to staff with security breach response responsibilities.

3.7 Control Area: Security Testing

Information System and/or Technology Infrastructure Owner **must**:	
PCD-220	Ensure that Live PANs are not used for testing or development.
PCD-230	Perform external vulnerability scans at least once every three months by a PCI SSC Approved Scanning Vendor (ASV). *[Reference: ASV Program Guide]*

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 could for serious breaches 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

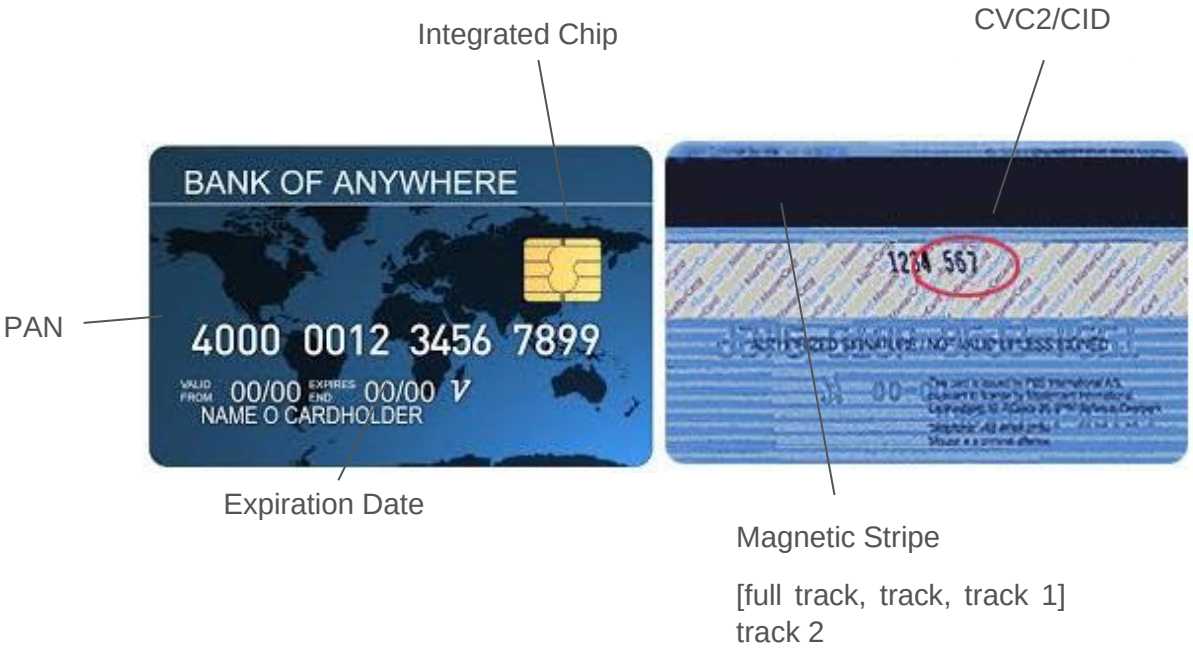
The ICS Standards Glossary has been defined and is available via the *GovPoint* – see the *Technology Glossary* via the *GovPoint Glossary* reference.

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 Payment Card Data Elements



Appendix A – Version Control Table

Document Author Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
CISRO ICS Policy	New Standard	-	Gareth Carrigan	1.0	28-Jan-19	29-Jan-19
CISRO ICS Policy	To align with recent Org change, reference to CISO amended to CISRO accordingly within the document.	-	Liz Banbury	1.1	30-Dec-19	30-Dec-19
CISRO ICS Policy	Annual review included update to the template structure and consultation feedback, corrections incorporated. [Added: PCD-120, Modified: PCD-010, PCD-020, PCD-030, PCD-040, PCD-070, PCD-110, PCD-130, PCD-140, PCD-150, PCD-160, PCD-170, PCD-180,		Liz Banbury	2.0	25-Mar-20	25-Mar-20

Document Author Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
	PCD-190, PCD-210 and PCD-230]					
CISRO ICS Policy	Annual Review – Alignment of Scope, Risks, Roles & Responsibilities with correct functions; Amended statements: Administrative, Editorial: PCD-050, PCD-180 Administrative, Removed: PCD-060, PCD-070, PCD-080	-	Liz Banbury [delegate of Group CISRO]	2.1	8-June-21	8-June-21
CISRO ICS Policy	Migrated to latest ERM/ICS Standard Template. ICSCR-19Jan2021-1 Including results of PCI DSS regulatory requirement gap assessment (PCD-015).	-	Samantha Finan, Global Head, ICS Policy, Standards and Reporting	2.2	15-Dec-21	20-Dec-21
CISRO ICS Policy	1. Modified PCD-010 in line with ICSCR-27Aug23-4 2. Editorial changes: Modified Introduction Section and Purpose, PCD-10, PCD-20, PCD-30, PCD-140 in line with ICSCR-27Aug23-5 3. New controls added: a. PCD-120 in line with ICSCR-27Aug23-2 b. PCD-230 in line with	-	Paul Hoare Head, ICS Policy and Best Practice	3.0	18-Dec-23	24-Dec-23

Document Author Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
	ICSCR-27Aug23-3					