Group Information and Cyber Security Standard: Payment Card Data Management

Version No	2.0
SCB Rulebook Document Reference	09-STND-0001-12
Document Type	Standard
Parent Document	ICS Policy
Document Approver Name	Liz Banbury [delegate of Group CISRO]
Document Approver Job Title	Head of Information and Cyber Security Policy
Document Owner Name	Liz Banbury
Document Owner Job Title	Head of Information and Cyber Security Policy
Document Contact Name	Yogeshkumar Venkatesan
Document Contact Job Title	Senior Information Security Manager, CISRO
Business Scope	All Businesses
Function Role	All Functions
Geography Scope	Global
Status	Approved
Approval Date	25 March 2020
Effective Date	25 March 2020
Last Review Date	25 March 2020
Next Review Date	25 March 2021

INTERNAL

Contents

Version Control Table

Version	Issue Date	Changes	Primary Reviewer	Secondary Reviewer	Approver
1.0	28th January 2019	New Standard	Liz Banbury	Bali Chandramouli	Gareth Carrigan
1.1	30th December 2019	To align with recent Org change, reference to CISO amended to CISRO accordingly, within the document.	Yogesh Kumar Venkatesan	N/A	Liz Banbury
2.0	25 March 2020	Annual review included update to the template structure and consultation feedback, corrections	CISRO Policy	Bok Chek Mee, Vijayakumar C, Mario Jetaun Wiley, Mehsum Raza Sayani, Mui Choo Leow,	Liz Banbury

		incoporated. [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, PCD-190, PCD-210 and PCD-230]		Ramesh Kumar PA, Robert Koch, CISRO ISO All, Heads of Information and Cyber Security.	

1. INTRODUCTION AND PURPOSE

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

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

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

<u>Payment Card Data is:</u>

Payment Card Data:
• Primary Account Number [PAN] • Cardholder Name • Service Code • Expiration Date • Magnetic Stripe [Tracks] • CAV2/CVC2/CVV2/CID • PIN/PIN block

Payment Card 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 Payment Card 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:

- Loss of customer trust.
- Adverse publicity and reputational damage.
- Financial loss
- Regulatory fines.

1.2 Scope

This Payment Card Data Management Standard is mandatory and applies to all Group businesses and Third Parties which process Payment Card Data except where explicitly prohibited by local Law or Regulation (see section 4.2 Policy Non-Compliance).

2. ROLES & RESPONSIBILITIES

Information Asset / Systems Owner

Information Asset and System Owners are responsible for the protection of Payment Card Data as part of their overall information asset portfolio. They are also accountable for ensuring that the Information Custodians 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

Information Custodian

The Information Custodian is responsible for complying with the control areas of this Information Security Standard which are applicable to them and must ensure the Payment Card Data processed by the Information Systems and Technology Infrastructure 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.

Staff

All Staff must ensure that the Group Information they use is protected in-line with the requirements of this standard.

Group Chief Information Security Office (CISO)

The Group CISO is responsible for complying with the control areas of this Information Security Standard which are applicable to them.

As first line role holders, the Group CISO will additionally perform effectiveness reviews to monitor first line compliance with this Information Security Standard.

- CISO Awareness team are responsible for ensuring that the Group is provisioned with the appropriate awareness and training tools (messaging, content, strategy and governance and training support).

Group Chief Information Security Risk Office (CISRO)

The Group CISRO is responsible for complying with the control areas of this Information Security Standard which are applicable to them.

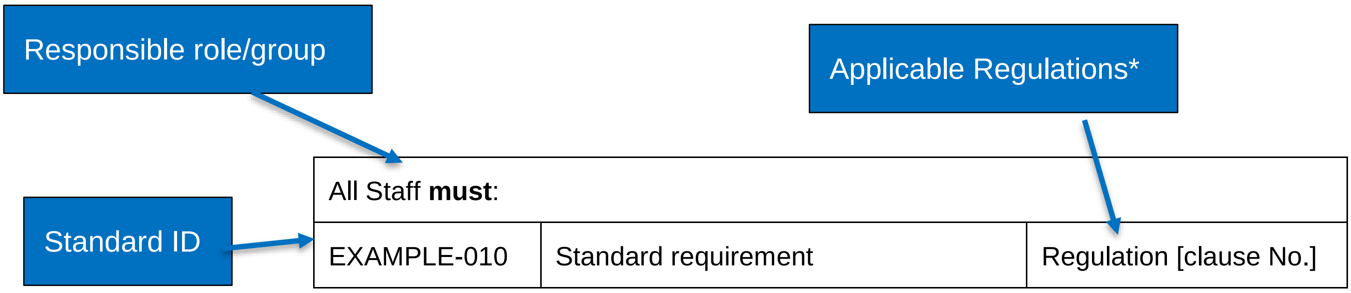
The Group CISRO is also the owner of this Standard and must ensure the document is updated to an agreed schedule. As second line role holders, the Group CISRO will additionally perform effectiveness reviews to monitor first line compliance with this Information Security Standard.

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 the minimum mandatory requirements applicable for the secure management of Payment Card Data.

Requirements are set out in the following format:



All Staff **must**:		
EXAMPLE-010	Standard requirement	Regulation [clause No.]

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

3.1 Control Area: Risk Assessment

CISO Office **must:**		
PCD-010	Establish a risk assessment process and perform a control effectiveness assessment at least every twelve months and upon significant changes to the Payment Card Data Environment. *[Reference: The Information & Cyber Security Risk Type Framework]*	PCI-DSS: 12.2

3.2 Control Area: Architecture

Information Custodian **must**:		
PCD-020	Define and maintain a description of the Payment Card 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 Payment Card 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]*	PCI-DSS: 1.1.2 MAS TRM 9.1.1
PCD-030	Maintain an inventory of system components that support the Payment Card Data Environment and review it at least every twelve months and upon	PCI-DSS: 2.4 MAS TRM 13.1.4

	significant changes to the Payment Card Data Environment. *[Reference: The Information & Cyber Security Risk Type Framework Section: Sub-Risk Types]*	

3.3 Control Area: Data Protection

Information Custodian **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 and Unstructured Data Storage Standard]*	PCI-DSS: 3.1 HKMA TM-G-1_3.1.3
PCD-050	Not store authentication data, after authorization, even if encrypted. *[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]*	PCI-DSS: 3.2 MAS TRM 13.1.1
PCD-060	Not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) after authorization. *[In the case of issuers, it may be necessary to retain some data elements for the business to be operational. Where this is required ensure that only the data elements required are stored and that the data is securely stored]*	PCI-DSS: 3.2.1 MAS TRM 13.1.2
PCD-070	Not store the card verification code or value (CVC or CVV, three-digit or four-digit number printed on the front or back of a payment card used to verify card-not-present transactions) after authorization.	PCI-DSS: 3.2.2 MAS TRM 13.1.2

PCD-080	Not store the personal identification number (PIN) or the encrypted PIN block after authorization.	PCI-DSS: 3.2.3
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.	PCI-DSS: 3.3 MAS TRM 13.1.1
PCD-100	Never use PAN as a Customer Reference Number or any type of Customer Identifier [e.g. user ID].	PCI-DSS: 3.3
PCD-110	Render PAN unreadable anywhere it is stored by use of approved hashing and encryption methods. *[Reference ICS Standard Cryptography]*	PCI-DSS: 3.4 MAS TRM 13.1.1 HKMA TM-E-1_5.1.1

All Staff **must**:		
PCD-115	Not store live PAN details locally in their Mobile Devices. *[Note: Includes the mail pst files]*	

3.4 Control Area: Encryption

Information Custodian **must**:		
PCD-120	Document and implement processes to protect keys used to secure stored Payment Card Data against disclosure and misuse. *[Reference ICS Standard Cryptography]*	PCI-DSS: 3.5 HKMA TM-E-1_5.1.1 RBI Advisory No: 6/2018 2 (vi)
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 and ICS Standard Cryptography]*	PCI-DSS: 4.1 MAS TRM 13.1.1 HKMA TM-E-1_5.1.1 RBI Advisory No: 6/2018 2 (vi)
PCD-140	Ensure wireless networks transmitting Payment Card Data or connected to the Payment Card Data Environment deploy approved encryption methods for authentication and transmission. *[Reference ICS Standard Cryptography]*	PCI-DSS: 4.1.1 MAS TRM 9.3.5 HKMA TM-E-1_4.2.3, 5.1.1 & TM-G-1_6.3.2 RBI Advisory No: 6/2018 2 (vi)

PCD-150	Never send unprotected Live PANs by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat). *[Reference ICS Standard Information Handling]*	PCI-DSS: 4.2 MAS TRM 9.1.5 RBI Advisory No: 6/2018 2 (vi)

3.5 Control Area: Media Handling

Information Custodian **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.	PCI-DSS: 9.6.2 MAS TRM 8.4.4 HKMA TM-G-1_3.1.3

3.6 Control Area: Security Awareness

Information Custodian **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.	PCI-DSS: 12.8.1

Information Asset Owner **must**:		
PCD-180	Maintain a list of service providers who process Payment Card Data on behalf of the Group including a description of the service provided. *[Reference ICS Standard Security in Interactions with Third Parties]*	PCI-DSS: 12.8.1

CISO Office **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.	PCI-DSS: 12.6 MAS TRM 3.4.1 HKMA TM-G-1_2.1.4

PCD-200	Maintain a program to monitor service providers' PCI DSS compliance status at least annually. *[Reference ICS Standard Security in Interactions with Third Parties]*	PCI-DSS: 12.8.4 MAS TRM 5.1.6
PCD-210	Provide appropriate training to staff with security breach response responsibilities.	PCI-DSS: 12.10.4 MAS TRM 3.4.1

3.7 Control Area: Security Testing

Information Custodian **must**:		
PCD-220	Ensure that Live PANs are not used for testing or development.	PCI-DSS: 6.4.3

4. INFORMATION & SUPPORT

4.1 General Information and Support

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

4.2 Reporting Non-Compliance

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

4.3 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 require to be escalated to the Policy Owner for appropriate actions.

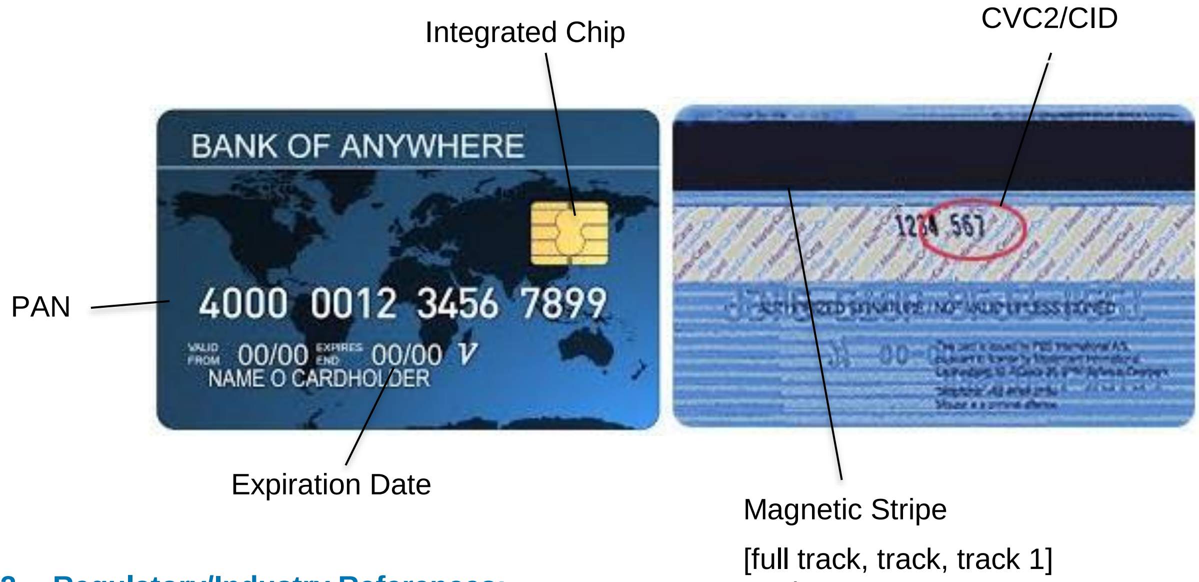
5. GLOSSARY

All definitions from the ICS Standards Glossary have been defined and are available via the *ICS Glossary of Terms* document:

http://teamsites.sc.com/sites/CISO/Governance/Policy/Control%20Framework%20Library/ICS%20Glossary%20Of%20Terms%20v1.pdf

6. APPENDIX

6.1 Payment Card Data Elements



6.2 Regulatory/Industry References:

[REGULATOR NAME]	REGULATOR DOCUMENT	SECTION/Version
PCI DSS	Payment Card Industry [PCI] - Security Standard	v3.2
Monetary Authority Singapore (MAS)	Technology Risk Management [TRM] Guidelines	2013
Hong Kong Monetary Authority (HKMA)	HKMA General Principles for Technology Risk Management - TM-G-1	2003
Hong Kong Monetary Authority (HKMA)	HKMA Risk Management of E-banking - TM - E- 1	2015
Reserve Bank of India (RBI)	Cyber Security & IT Examination Cell - Advisory No: 6/2018	2018