Cryptography Standard

Version No	**5.0**
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	Katarzyna Wencka
Document Contact Job Title	Director, ICS Standards
Business Scope	All Businesses
Function Role	All Functions
Geography Scope	Global
Effective Date	2 June 2025
Approval Date	19 December 2024
Next Review Date	30 November 2027

Standard Chartered Bank

www.sc.com

Table of Contents

1 INTRODUCTION AND PURPOSE 4

1.1 Risks 4

1.2 Scope 4

2 ROLES & RESPONSIBILITIES 5

3 STANDARD REQUIREMENTS 6

3.1 Control Area: Cryptography Solutions 6

3.2 Control Area: Cryptographic Key Management 8

3.3 Control Area: Hardware Security Module [HSM] 12

3.4 Control Area: Post Quantum Cryptography (“PQC”) 14

3.4.1 PQC agility/readiness 14

4 INFORMATION & SUPPORT 15

4.1 General Information and Support 15

4.2 Reporting Non-Compliance 15

4.3 Breach of this Standard 15

5 GLOSSARY 15

6 REGULATORY / INDUSTRY REFERENCES 15

7 APPENDIX 16

7.1 [CRY-AP-010] Table 1a – Group Approved Cryptography Algorithms 16

7.2 [CRY-AP-020] Table 1b – Quantum Resistant Cryptography 17

7.3 [CRY-AP-030] Table 2 – Advantages of Cryptography 18

7.4 [CRY-AP-040] Table 3 – Operational guidelines for CRY controls 18

Appendix A – Version Control Table 20

Version Control Table

Document Author Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
Katarzyna Wencka **[ICS Standards]**	Administrative changes: 1. due to document ownership and template changes as well as changes in roles, 2. objectives definition (for ICS controls). Changes to ICS controls, in line with ICSCR-14Aug24-1 (PQC) and ICSCR-27Jan2023-1 (adding references to operational guidelines): 1. updated controls (CRY-090, CRY-320, 2. new controls (CRY-400, CRY-420, Table 1b CRY-AP-020, Table 3 CRY-AP-040)	Material	Jamie Cowan Head, ICS Risk Framework & Governance	5.0	19-Dec-24	02-Jun-25

1 INTRODUCTION AND PURPOSE

The objective of cryptography is to protect the confidentiality and integrity of data during storage and transmission as well as to confirm the identity of the originator of transactions or communications. Data is protected using encryption/decryption techniques. Such techniques ensure that data can only be read by the authorized user(s) on a need-to-know basis. The strength of cryptographic solutions depends largely on their design, construction, and the size of their keys.

Data is protected by converting the plaintext to cipher text (scrambled form of data) by using a cryptographic algorithm and a key before being shared with the legitimate recipient. This is known as Encryption. To read the data, the legitimate recipient(s) perform the decryption process using the same algorithm (which was used for encryption) and a decryption key.

There are three main classes of Cryptographic algorithms:

- Symmetric Cryptography – In such algorithms, the key is shared between the sender and recipient and the same key is used to perform the encryption and decryption process. [to protect confidentiality]
- Asymmetric Cryptography – In these types of algorithms each entity has a key pair – a Public Key and a Private Key where one key is used to perform the encryption and other is used to perform the decryption. The public key of the entity, as the name depicts, is made available publicly, and the private key is kept secret with the entity. [to protect confidentiality]
- Hashes – In order to maintain the integrity of the data, hash functions are applied. These are one-way non-reversible functions where a hash is generated from a given message and assigned to that message. The mathematical properties of Hash functions are designed in such a way that the slightest change in a message will result in an entirely new Hash value. These functions are most suitable for detecting alterations in the data (maliciously or un-intentionally) during rest as well as in transmission, by simply comparing the hash value before the data is stored or transmitted and after data is retrieved or received. If both the hash values match, then no modification has been done. [to protect integrity].

Please see section 7.3 "[CRY-AP-030] Table 2 – Advantages of Cryptography" for more context.

1.1 Risks

Failure to use cryptography appropriately and correctly may lead to a breach to the confidentiality and/or integrity of data 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 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 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 in line with applicable ICS controls defined in ICS Standards.

2 ROLES & RESPONSIBILITIES

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.

Application / Technology Infrastructure Owner

A named individual accountable for the protection of owned Application / Technology Infrastructure and for compliance with applicable Control Statements defined in this Standard.

Process Owner [Cryptographic Services]

POs (as defined by Enterprise Risk Management Framework) are Business or Function managers responsible for the end-to-end business or function processes as identified within the Group's Process Universe.

They are responsible for identification and management of the end-to-end process as defined in the Group's Process Universe and associated risks, including ICS related activities as mandated by the Standard.

Process Owner [Cryptographic Services] is an appointed CISO function.

CISO ICS Standards & Controls

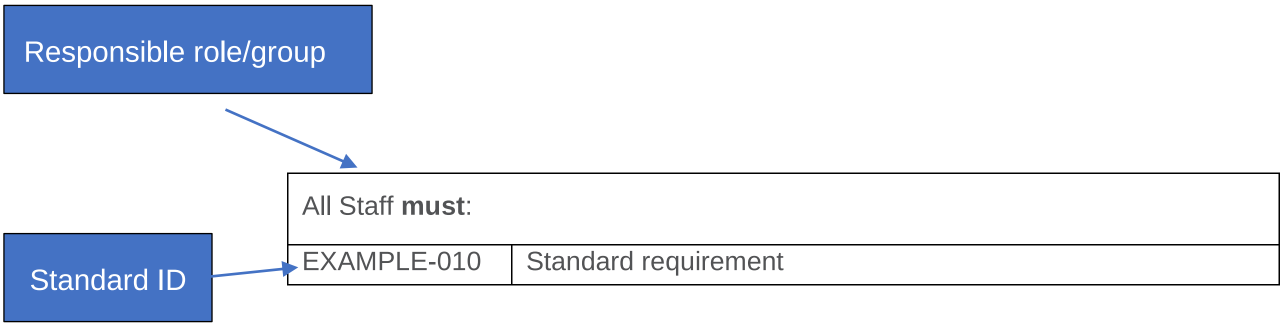
The CISO is the owner of this Information Security Standard and will ensure the document is updated to an agreed schedule.

***Note**: The Responsible role who 'must' execute against 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:



Responsible role/group

Standard ID

All Staff **must**:

EXAMPLE-010 Standard requirement

3.1 Control Area: Cryptography Solutions

Application Owner and/or Technology Infrastructure Owner **must**:	
CRY-010	Use only Group approved protocols and cryptographic algorithms in Information Systems. AND Ensure the usage of cryptographic algorithms must comply with legal and regulatory related encryption requirements. *Note: As defined in Appendix 7.1 "[CRY-AP-010] Table 1a – Group Approved Cryptography Algorithms"* *[Reference: Appendix 7.1 "[CRY-AP-010] Table 1a – Group Approved Cryptography Algorithms", Appendix 7.3 "[CRY-AP-030] Table 2 – Advantages of Cryptography"]* *[Objective: Group data and Information is effectively protected with the use of effective cryptographic solutions.]*

Information System/Application Owner and/or Technology Infrastructure Owner **must**	
CRY-030	Ensure that cryptographic keys are stored, at the minimum, in FIPS 140-2 level 2 validated key vault (exclusions apply – see 'Notes', 'Exclusions' and 'References' below). *[Notes:* *a) Crypto Key vaults that do not meet these criteria must be:* *- at least FIPS 140-2 level 1 validated* *AND* *- its Root-of-Trust must be derived from a compliant crypto device (such as HSM).* *b) Equivalent standards, such as FIPS 140-3, are acceptable.]* *[Exclusions: Local Cryptographic Key Stores (such as Windows Key Store, Java Key Store, PKCS#12, File System Locations) may be used for storing:* *a) End user keys on endpoint devices (such as laptops, desktops, and other mobile devices), used for the purpose of:* *- Full-disk encryption, file/folder encryption, email encryption & digital signatures,* *- Applications/User/Device authentication* *b) private keys associated with digital certificates for SSL/TLS or for authentication* *c) private key associated with self-signed certificates only as defined for use by DCM-145* *d) Cryptographic keys as enforced by regulatory requirements (mandating usage of software-based key store)]* *[References: CRY-034]* *[References: DCM-145]* *[Reference: Information Handling Standard – the definition of the encryption applicability/conditions]* *[Objective: Cryptographic keys used for the Group data and Information protection are secure and protected from disclosure or loss so data can be effectively protected from disclosure, manipulation AND can be retrieved when required.]*

Process Owner [Cryptographic Services] and/or Information System Owner and/or Technology Infrastructure Owner **must**:	
CRY-031	Ensure that physical/hardware devices, for example, Hardware Security Modules (HSMs) used for cryptographic keys storage are tamper resistant. *[Reference: CRY-030]* *[Objective: Cryptographic keys used for the Group data and Information protection are secure and protected from disclosure or loss so data can be effectively protected from disclosure, manipulation AND can be retrieved when required.]*

Information System Owner/Application Owner and/or Technology Infrastructure Owner **must**:	
CRY-034	Ensure that keys used in the PCI data processing are stored in the PCI-DSS compliant crypto modules. *[Reference: CRY-030]* *[Objective: Cryptographic keys used for the Group data and Information protection are secure and protected from disclosure or loss so data can be effectively protected from disclosure, manipulation AND can be retrieved when required.]*

Application Owner and/or Technology Infrastructure Owner **must**:	
CRY-060	Ensure that when software-based cryptography is implemented then the private keys and authentication data (e.g. passwords, passphrases, PINs) are not stored in plain text (e.g. in program, batch file, script file, database). *[Objective: Cryptographic keys used for the Group data and Information protection are secure and protected from disclosure or loss so data can be effectively protected from disclosure, manipulation AND can be retrieved when required.]*
CRY-065	Ensure that when tokenization or salting or peppering methods are used then uniqueness and randomization is enforced with the usage of a National Institute of Standards and Technology [NIST] defined random number generator or a pseudo-random number generator that passes all the basic tests for statistical randomness. *[Reference: NIST Special Publication (SP) 800-22 – "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications".]* *[Objective: Randomisation is introduced when generating cryptographic artifacts (such as keys or hash values) to ensure those artifacts, its derivatives or originals can't be easily reproduced or predicted.]*
CRY-066	Ensure that hashed passwords are salted. *[Objective: Randomisation is introduced when generating cryptographic artifacts (such as keys or hash values) to ensure those artifacts, its derivatives or originals can't be easily reproduced or predicted.]*

3.2 Control Area: Cryptographic Key Management

Information Asset Owner and/or Information System Owner **must**:	
CRY-090	Ensure that owners of cryptographic keys: a) Are made aware of their responsibilities for using and protecting keys (and where necessary disclosing keys) assigned to them. b) Confirm they clearly understand their responsibilities for using and protecting cryptographic keys. c) Manage owned keys in line with this Standard requirements and predefined guidelines (as defined in CRY-100). *[Objective: Cryptographic keys used for the Group data and Information protection are secure and protected from disclosure or loss so data can be effectively protected from disclosure, manipulation AND can be retrieved when required.]*

Process Owner [Cryptographic Services] and/or Information System Owner **must**:	
CRY-100	Establish a documented process for managing cryptographic keys (including software-based and Hardware Security Module [HSM]), which covers: a) key life cycle management (generation using approved algorithms and key lengths, rotation, renewal, revocation, destruction), b) secure distribution, activation, and storage, c) key backup and recovery (including assessment to decide which cryptographic keys need to be preserved), d) key validity period (encryption / decryption), e) restriction of access to cryptographic keys to authorised Staff, f) sharing of cryptographic keys (e.g. using split key generation) required for protecting confidential information and critical systems, g) restriction that compromised, revoked, or expired cryptographic keys cannot be used for encryption of any new data, h) Key Ceremony [CRY-105]. *[Note: Cryptographic Services - Process Owner is the appointed CISO function.]* *[Reference: 7.4 "[CRY-AP-040] Table 3 – Operational guidelines for CRY controls" – Operational guidelines, criteria, checklists and templates for CRY Standard requirements adoption'* *[Objective:* *1) Cryptographic keys used for the Group data and Information protection are secure and protected from disclosure or loss so data can be effectively protected from disclosure, manipulation AND can be retrieved when required.* *2) Cryptographic keys are strong, i.e. generated with the use of effective algorithms and parameters mitigating the risk of key prediction, reproduction or brute forcing.* *3) Cryptographic keys lifecycle is adequately defined and maintained to limit the risk of key misuse or protected data/information disclosure or manipulation.]*
CRY-102	Ensure that: 1) any top-level key generation/rotation for devices that are providing cryptography services are performed from a physically secured location, 2) any key lifecycle management operations are: a) conducted with appropriate level of approvals, b) in line with a formal and valid change request, c) documented and auditable. *[Objective:* *1) Cryptographic keys used for the Group data and Information protection are secure and protected from disclosure or loss so data can be effectively protected from disclosure, manipulation AND can be retrieved when required.* *2) Cryptographic keys are strong, i.e. generated with the use of effective algorithms and parameters mitigating the risk of key prediction, reproduction or brute forcing.* *3) Cryptographic keys lifecycle is adequately defined and maintained to limit the risk of key misuse or protected data/information disclosure or manipulation.]*

Information System Owner and/or Technology Infrastructure Owner **must**:	
CRY-103	Ensure that cryptographic keys are securely destroyed (i.e. non-recoverable manner) when no longer required and all traces of key material is removed effectively (including existing key copies). *[Objectives: Cryptographic keys or cryptographic material used for Group data/Information protection must be effectively destroyed, so the Group Information or data cannot be recovered with their use.]*

Process Owner [Cryptographic Services] and/or Information System Owner **must**:	
CRY-105	Perform Key Ceremonies: a) During the master key (top level key) generation process for HSMs; b) For top level keys of the Information systems providing cryptography services (for example: PKI/RCA/ICA) to multiple downstream systems with the Banks central Crypto Services; c) For top level keys of the Information Systems providing or supporting services, where cryptography acts as a core functionality or is fundamental for core functionalities (for example: distributed digital ledgers, crypto currencies/digital assets). *[Reference: 7.4 "[CRY-AP-040] Table 3 – Operational guidelines for CRY controls" (3) Key Ceremony Criteria Document, (7) Cryptography Key Ceremony Sample Template]* *[Objective: Secrets must be generated securely, preventing unauthorized access, and be recoverable in case of loss. The associated processes and technology must be auditable for transparency towards customers, auditors, or regulators.]*
CRY-120	Protect cryptographic keys against: a) Access by unauthorized individuals or applications, b) Accidental or malicious destruction. *[Objective: Cryptographic keys used for the Group data and Information protection are secure and protected from disclosure or loss so data can be effectively protected from disclosure, manipulation AND can be retrieved when required.]*
CRY-130	In order to ascertain required entropy during cryptographic keys creation, ensure that all cryptographic keys and cryptographic key components are generated using a random number generator or a pseudo-random number generator that passes all the basic tests for statistical randomness, as defined in the National Institute of Standards and Technology [NIST]. *[Reference: NIST Special Publication (SP) 800-22 – "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications".]* *[Objective: Randomisation is introduced when generating cryptographic artifacts (such as keys or hash values) to ensure those artifacts, its derivatives or originals can't be easily reproduced or predicted.]*
CRY-135	Ensure there is dual control and split knowledge in place to manage manual clear-text cryptographic key generation, transmission, loading, storage, and destruction (where applicable). *[Objective: Cryptographic keys used for the Group data and Information protection are secure and protected from disclosure or loss so data can be effectively protected from disclosure, manipulation AND can be retrieved when required.]* *[Reference: PCI DSS Version 4.0]* *[Reference: CRY-102]*

Process Owner [Cryptographic Services] and/or Information System Owner **must**:	
CRY-140	Only allow use of cryptographic keys for a single intended purpose and restrict reuse between Information Systems. *[Objective:* *1) The likelihood of a cryptographic key disclosure is limited due to use and access restrictions.* *2) The impact of cryptographic key disclosure is limited due to its use and scope limitations.* *3) Cryptographic keys attributes are selected in line with the intended use and anticipated ICS risk.]*
CRY-150	Define and follow cryptographic keys life cycle that should: a) ensure operational stability, b) include regular reviews to confirm being in line with the requirements defined in 6.1 Regulatory/Industry References, c) reconciliation, d) expiry notifications, e) enforce key rotation (i.e. change) at least as: • Key Type: Private Signature key; Originator Usage period: 3 years, Recipient usage period: NA, • Key Type: Private/Public Authentication Key; Originator Usage period: 2 years, Recipient usage period: 2 years, • Key Type: Symmetric Authentication key; Originator Usage period: 2 years, Recipient usage period: 5 years, • Key Type: Symmetric Data encryption Keys; Originator Usage period: 2 years, Recipient usage period: 5 years, • Key Type: Symmetric Key-Wrapping Keys; Originator Usage period: 2 years, Recipient usage period: 5 years (i.e. OUP + 3 years), • Key Type: Symmetric Master Keys; Originator Usage period: 1 years, Recipient usage period: NA. *[Note: A higher frequency may be determined by the Key Owner. In the case of key compromise its cryptoperiod is no longer considered valid.]* *[Objective:* *1) Cryptographic keys used for the Group data and Information protection are secure and protected from disclosure or loss so data can be effectively protected from disclosure, manipulation AND can be retrieved when required.* *2) Cryptographic keys lifecycle is adequately defined and maintained to limit the risk of key misuse or protected data/information disclosure or manipulation.* *3) Cryptographic keys are rotated with frequency limiting the risk of protected data disclosure or manipulation due to the cryptographic disclosure.]*

Information System Owner and/or Technology Infrastructure Owner **must**:	
CRY-160	In the case of suspected or factual key compromise, without undue delay: a) perform a risk assessment for the impact on the downstream/upstream system as well as backups. b) replace the cryptographic key or key component (if applicable) c) replace any key(s) that are derived from the compromised key d) report the breach and communicate the impact of the key compromise through Group's Security Incident Management Process. *[Objective: Anticipated ICS risk from cryptographic keys disclosure is adequately assessed and mitigated.]*

Process Owner [Cryptographic Services] and/or Information System Owner **must**:	
CRY-170	Perform an assessment to establish which cryptographic keys need to be preserved (Backup and Recovery) for possible recovery. The key backup must be performed on an independent, secure electronic storage media device. The backup of keys must be retained in line with the requirements from Group Records Management Policy. *[Objective: Cryptographic keys used for the Group data and Information protection are secure and protected from disclosure or loss so data can be effectively protected from disclosure, manipulation AND can be retrieved when required.]*

3.3 Control Area: Hardware Security Module [HSM]

Process Owner [Cryptographic Services] and/or Information System Owner **must**:	
CRY-191	Document and maintain Security Configuration requirements for HSM, that takes part in Payment processing (storing, processing, and transmitting data) under PCI DSS requirements, which must follow: a) Payment Card Industry [PCI] PIN Transaction Security [PTS] Hardware Security Module [HSM] Modular Security Requirements Version 3.0, b) Security Manual/Operational Configuration (where applicable) as provided by HSM products vendor. *[Objective: HSM devices are securely managed and configured to ensure required security and confidence for the processed cryptographic keys and corresponding cryptographic elements.]*
CRY-192	Document and maintain Security Configuration requirements for HSM, that do not take part in Payment processing (storing, processing, and transmitting data) under PCI DSS requirements, which must follow Security Manual/Operational Configuration (where applicable) as provided by HSM products vendor. *[Note: It is recommended that PCI, PTS, HSM, Modular Security Requirements Version 3.0 should also be considered.]* *[Objective: HSM devices are securely managed and configured to ensure required security and confidence for the processed cryptographic keys and corresponding cryptographic elements.]*
CRY-205	Configure all HSMs by implementing documented Secure Configuration requirements. *[Objective: HSM devices are securely managed and configured to ensure required security and confidence for the processed cryptographic keys and corresponding cryptographic elements.]*

Process Owner [Cryptographic Services] and/or Information System Owner **must**:	
CRY-300	Ensure that only API connections and those required for maintenance purpose are only allowed to the HSM and/or its server. *[Objective: HSM devices are securely managed and configured to ensure required security and confidence for the processed cryptographic keys and corresponding cryptographic elements.]*

Process Owner [Cryptographic Services] **must**:	
CRY-310	Define and maintain security decommissioning requirements for HSMs, which adopt applicable ICS controls of Secure Decommissioning and Destruction Standard. *[Reference: Secure Decommissioning and Destruction Standard, 7.4 "[CRY-AP-040] Table 3 – Operational guidelines for CRY controls" (5) Decommission Checklist]* *[Objective:* *1) HSM devices are securely managed and configured to ensure required security and confidence for the processed cryptographic keys and corresponding cryptographic elements.* *2) Cryptographic keys or cryptographic material used for Group data/Information protection must be effectively destroyed, so the Group Information or data cannot be recovered with their use.]*

Process Owner [Cryptographic Services] and/or Information System Owner **must**:	
CRY-320	Ensure that HSMs are decommissioned (when no longer required) in line with Secure Decommissioning and Destruction Standard requirements and applicable Process Owner [Cryptographic Services] guidelines. *[Reference: Secure Decommissioning and Destruction Standard, 7.4 "[CRY-AP-040] Table 3 – Operational guidelines for CRY controls" (5) Decommission Checklist]* *[Objective:* *1) HSM devices are securely managed and configured to ensure required security and confidence for the processed cryptographic keys and corresponding cryptographic elements.* *2) Cryptographic keys or cryptographic material used for Group data/Information protection must be effectively destroyed, so the Group Information or data cannot be recovered with their use.]*

3.4 Control Area: Post Quantum Cryptography ("PQC")

3.4.1 PQC agility/readiness

Process Owner [Cryptographic Services] **must**:	
CRY-400 *[new]*	Define, document, maintain and execute a resilient strategy for Post Quantum Cryptography ("PQC") ensuring the Group readiness to migrate to quantum resistant cryptography, when and where required. *[Objective:* *1) Group's data and Information is effectively protected with the use of cryptography in the quantum computing era.* *2) The Group demonstrates required agility to effectively move to quantum-resistant cryptography.* *3) The Group approach and strategy for transition to PQC is defined, planned and validated to ensure the ICS risk is managed with the Group Risk Appetite and operational impact is limited.* *4) The Group can effectively move to quantum resistant cryptography once such solutions are ready, validated and the quantum computing threat is tangible.]*

Information System/Technology Infrastructure/Technology Product Owner **must**:	
CRY-420 *[new]*	Ensure, that for the owned Technology Assets or Products, the use and maintenance of cryptographic components, either implicitly or explicitly, is well documented and validated as per the Process Owner [Cryptographic Services] guidelines. AND Ensure that any Technology Assets, Product or solution planned for acquisition/onboarding, including those that are hosted or managed by 3rd party is validated for the PQC readiness & crypto agility (as per the applicable Process Owner [Cryptographic Services] guidelines). *[Objective:* *1) Group's data and Information is effectively protected with the use of cryptography in the quantum computing era.* *2) The Group demonstrates required agility to effectively move to quantum-resistant cryptography.* *3) The Group approach and strategy for transition to PQC is defined, planned and validated to ensure the ICS risk is managed with the Group Risk Appetite and operational impact is limited.* *4) The Group crypto agility and readiness for quantum resistant cryptography is, where possible, tested for effectiveness.]*

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 [CRY-AP-010] Table 1a – Group Approved Cryptography Algorithms

Algorithm	Minimum Key Length
Symmetric Key Algorithms	
Advanced Encryption Algorithm (AES)	128 bits *[256 bits preferred]*
CAST-256	256 bits
Rivest cipher 6 (RC6)	256 bits
Twofish	256 bits
Camellia	256 bits
SEED-192/256	256 bits
SEED[1]	128 bits
SM4[2]	128 bits
Asymmetric Key Algorithms / Public-key cryptography	
Rivest–Shamir–Adleman (RSA)	2048 bits *[3072 preferred for new technologies]*
Digital Signature Algorithm (DSA)	2048/256
Diffie Hellman (DH)	2048
Elliptic Curve Digital Signature Algorithm (ECDSA)	P-256 Curve OR secP256k1 Curve
Elliptic Curve Diffie-Hellman (ECDH)	P-256 Curve OR secP256k1 Curve
EdDSA / Ed25519	Curve25519 with SHA-512 (SHA-2)
EdDSA / Ed448	Curve448 with SHA-3
SM2[3]	256 bits
SM9 (PKI equivalent)[4]	n/a
Hash functions	
SHA-2	256 bits
SHA-3	256 bits *[384 or 512 preferred]*
SM3[5]	256 bits

[1] only when use of SEED-192/256 is not technically feasible

[2] only for use within markets where regulator(s) requires it

[3] only for use within markets where regulator(s) requires it

[4] only for use within markets where regulator(s) requires it

[5] only for use within markets where regulator(s) requires it

keccak256[6]	256 bits
Transport Layer Protocol	
Please refer to section 3.8.1 Table 2 – Approved TLS versions AND DCM-700 and DCM-710 in Digital Certificate Management Standard.	

7.2 [CRY-AP-020] Table 1b – Quantum Resistant Cryptography

The below cryptographic primitives are **recommended** (not yet mandated) for new technologies, where feasible and supported. The use of the below cryptography should be consulted with the Process Owner [Cryptographic Services]/Group appointed Security Architecture function.

The list is not closed, as this is an area of constant development. Any new additions to this list will be maintained by the PO [Cryptographic Services] upon consultations and agreement with Security Architecture function.

Algorithm	Minimum Key Length
Asymmetric Key Algorithms / Public-key cryptography	
ML-KEM (aka CRYSTALS-Kyber)	As per the NIST FIPS PUB 203
ML-DSA (aka CRYSTALS-Dilithium)	As per the NIST FIPS PUB 204
Leighton-Micali Signature (LMS)	As per the NIST SP 800-208
Xtended Merkle Signature Scheme (XMSS)	As per the NIST SP 800-208
Hash functions	
SLH-DSA (aka SPHINCS)	As per the NIST FIPS PUB 205

[6] use limitations apply - to be used only in blockchain/crypto asset projects which do not support SHA-3 implementation; use/deployment of keccak256 to be supported with risk assessment.

7.3 [CRY-AP-030] Table 2 – Advantages of Cryptography

#	Advantages of cryptography/encryption	Description
1	Confidentiality protection	Protection of confidential and restricted information at rest or in transit (E.g., financial data, customer data such as PINs, Passwords, regulated data, PII – Personally identifiable information etc.) by making data readable only for authorized Users.
2	Integrity protection	Protection of confidential and restricted information to ensure that data is not altered between source and destination. (E.g.: password hashing, file level integrity checks etc.)
3	Authentication	Establishing the trust in a virtual entity, i.e., the receiver can validate the identity of the sender, which is established by a trusted third party.
4	Non-repudiation	Ensuring authenticity of Sender (Claim that Sender indeed has sent the message) of high value/sensitive messages through use of digital signing and certificates.

Assurance	Protection Against	Symmetric Key	Asymmetric Key	Hash Algorithms
Confidentiality	Unauthorized disclosure of data	Yes	Yes	No
Authentication	Masquerading (pretend to be someone)	No	Yes	No
Integrity	Unauthorized modification of data	No	No	Yes
Non-repudiation	Sender's false denial	No	Yes	No

7.4 [CRY-AP-040] Table 3 – Operational guidelines for CRY controls

#	External reference (guidelines document)	Applicable CRY control(s)
1	Decentralised Cryptography - Governance Framework	CRY-100 & general applicability
2	Key Management Guideline	CRY-065, CRY-090, CRY-100, CRY-102, CRY-103, CRY-105, CRY-120, CRY-130, CRY-135, CRY-140, CRY-150, CRY-160, CRY-170
3	Key Ceremony Criteria Document	CRY-100, CRY-105
4	Smart Card/Key Fob Management Guideline	CRY-100

#	External reference (guidelines document)	Applicable CRY control(s)
5	Decommission Checklist	CRY-310, CRY-320
6	Criteria for Key Custodian & Security Officer	CRY-100
7	Cryptography Key Ceremony Sample Template	CRY-100, CRY-105

Appendix A – Version Control Table

Document Author Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
CISO Policy	Annual review includes: 1. Migrated existing standard to ERM standard template. 2. The existing Cryptography Standard, HSM HLSTS and Guidelines for Cryptography documents have been uplifted into this standard. Consultation feedback, corrections incorporated.	Material	Gareth Carrigan, Global Head, ICS Governance, Policy and Risk	1.0	11-Jul-19	11-Jul-19
CISRO ICS Policy	Based on outcome of ICS Change request forum, CRY-070 updated by removing word 'Confidential'.	Non-material	Liz Banbury, Head, ICS Policy	1.1	17-Dec-19	17-Dec-19
CISRO ICS Policy	Annual review.	Material	Liz Banbury, Head, ICS Policy	2.0	02-Oct-20	02-Oct-20
CISRO ICS Policy	CRY-066 added as result of CR.	Non-material	Liz Banbury, Head, ICS Policy	2.1	08-Jun-21	01-Jul-21
CISRO ICS Policy	Aligned 1.1 Risks to RTF, PO role. Editorial change to CRY-010.	Non-material	Samantha Finan, Global Head, ICS Policy, Standards and Reporting	2.2	10-Nov-21	15-Nov-21
CISRO ICS Policy	CRY-100 updated and CRY-105 added in line with ICSCR-2Jul2021-1	Non-material	Samantha Finan, Global Head, ICS Policy, Standards	2.3	14-Dec-21	01-Jan-22

Document Author Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
	Administrative changes: document template, risks mapping, roles with ICS RTF alignment		and Reporting			
CISRO ICS Policy	1. Table in section Table 1 – Group Approved Cryptography Algorithms amended in line with ICSCR-24Sep2021-1 and ICSCR-24Mar2022-1 2. CRY-150 updated in line with ICSCR-5Oct2021-1 3. TLS references in Table 1 updated in line with ICSCR-14Oct2021-1 4. ICSCR-1Jun2022-1: CRY-102 & 103 added; CRY-135 & 160 amended	Material	Samantha Finan, Global Head, ICS Policy, Standards and Reporting	3.0	22-Jun-22	01-Jul-22
CISRO ICS Policy	1. Table in section Table 1 – Group Approved Cryptography Algorithms amended in line with ICSCR-14Apr2022-1 2. CRY-105 amended in line with ICSCR-1Sep2022-2 3. CRY-310 & 320 added in line with ICSCR-1Sep2022-2	Non-material	Paul Hoare Head, ICS Policy and Best Practice	3.1	08-Mar-23	22-Mar-23

Document Author Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
CISRO ICS Policy	Amendment to supplement the requirement for FIPS 140-2/140-3 in line with ICSCR-10Oct2022-1: 1. CRY-030 updated 2. CRY-031 and 034 added 3. CRY-040 removed	Material	Paul Hoare Head, ICS Policy and Best Practice	4.0	27-Apr-23	15-May-23
CISRO ICS Policy	Editorial changes: 1. Role names realigned with the Group role library, 2. CRY-010 amended for more clarity, 3. References to the DCM Standard corrected in CRY-030 (ICSCR-28Jul23-1) and Table 1 in section 7.1 Controls updated: 1. CRY-105 & CRY-130 (as per the ICSCR-2Sep2022-1) to ensure digital assets coverage	Non-material	Paul Hoare Head, ICS Policy and Best Practice	4.1	03-Nov-23	01-Jan-24
Katarzyna Wencka **[ICS Standards]**	Administrative changes introduced to update document template, references, roles and ownership.	Non-material	Jamie Cowan Head, ICS Risk Framework & Governance	4.2	19-Dec-24	23-Dec-24

Document Author Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
Katarzyna Wencka **[ICS Standards]**	Administrative changes: 1. due to document ownership and template changes as well as changes in roles, 2. objectives definition (for ICS controls). Changes to ICS controls, in line with ICSCR-14Aug24-1 (PQC) and ICSCR-27Jan2023-1 (adding references to operational guidelines): 1. updated controls (CRY-090, CRY-320, 2. new controls (CRY-400, CRY-420, Table 1b CRY-AP-020, Table 3 CRY-AP-040)	Material	Jamie Cowan Head, ICS Risk Framework & Governance	5.0	19-Dec-24	02-Jun-25