	No of Pages	1 of 5
	Document Classification:	Internal
	Effective Date	1 Aug 2025
CRYPTOGRAPHIC CONTROLS	Doc No	ISMS-TECH-09
	Revision	1.0

AMENDMENTS LOG

Revision History

Version	Revision Author	Reviewer / Approver	Date	Summary of Changes
1.0	Nor Asfiah Binte Jamalludin (ISMS MR)	James Chia (CEO)	1 Aug 2025	Initial Release



	No of Pages	2 of 5
	Document Classification:	Internal
	Effective Date	1 Aug 2025
CRYPTOGRAPHIC CONTROLS	Doc No	ISMS-TECH-09
	Revision	1.0

TABLE OF CONTENTS

PURPOSE	3
SCOPE.....	3
REFERENCE	3
RESPONSIBILITIES & AUTHORITIES.....	3
PROCEDURE.....	3
A. Data Classification and Use of Encryption	3
B. Cryptographic Algorithms and Key Strengths	4
C. Key Management.....	4
D. Secure Communication and Remote Access	4
E. Digital Signatures and Integrity Protection	4
F. Exceptions and Monitoring	4

	No of Pages	3 of 5
	Document Classification:	Internal
	Effective Date	1 Aug 2025
CRYPTOGRAPHIC CONTROLS	Doc No	ISMS-TECH-09
	Revision	1.0

PURPOSE

This procedure defines the organization's approach to using cryptographic controls to ensure the confidentiality, integrity, authenticity, and, where required, non-repudiation of sensitive data, both at rest and in transit, across its systems, services, and communication channels.

SCOPE

This procedure applies to all:

- Cloud-hosted services and infrastructure under the organization's control
- Internal applications that store, transmit, or process sensitive or personal data
- Data exchanges between systems, APIs, users, and third parties
- Endpoints and personnel devices used for remote access
- Use of cryptographic tools for authentication, encryption, key management, and digital signing, where applicable

This procedure does not apply to the shared office network infrastructure, which is not owned or managed by the organization.

REFERENCE

ISO/IEC 27001 Standard Annex A 8.24 Cryptographic controls

RESPONSIBILITIES & AUTHORITIES

Top Management has the prime responsibility and approval authority for this control.


The Management Representative (MR) shall ensure the cryptographic controls are implemented and that encryption keys are managed all throughout its lifecycle.

PROCEDURE

A. Data Classification and Use of Encryption

All confidential and personal data is protected using encryption:

Data Type	Encryption Requirement
Data in transit (external and internal)	Encrypted using TLS 1.2+ or HTTPS (mutual TLS for sensitive APIs)
Data at rest in cloud storage or databases	Encrypted using AES-256 or cloud-native equivalents

	No of Pages	4 of 5
	Document Classification:	Internal
	Effective Date	1 Aug 2025
CRYPTOGRAPHIC CONTROLS	Doc No	ISMS-TECH-09
	Revision	1.0

Data Type	Encryption Requirement
Credentials and secrets	Stored using hashing (e.g., bcrypt) or secrets managers
Backups	Encrypted both in transit and at rest
Emails	Encrypted using PGP/S/MIME where applicable

B. Cryptographic Algorithms and Key Strengths

Only strong and approved cryptographic algorithms and key lengths shall be used:

Function	Approved Algorithm / Method
Symmetric Encryption	AES-256 (minimum AES-128)
Asymmetric Encryption	RSA-2048 or ECC (e.g., P-256)
Hashing	SHA-256 or higher (no use of MD5/SHA-1)
Key Exchange	ECDH, DH with 2048-bit keys
Password Storage	bcrypt, scrypt, or PBKDF2 with salt

Use of deprecated or weak algorithms (e.g., RC4, DES, MD5, SHA-1) is strictly prohibited.

C. Key Management

Key management process shall include:

- Generation of strong, unique keys
- Rotation at defined intervals or after compromise
- Access control to keys (based on least privilege)
- Revocation and disposal when keys are no longer needed

Cloud-native Key Management Services (KMS) are used for managing cryptographic keys.


D. Secure Communication and Remote Access

- All access to organizational systems must be over secure encrypted channels (e.g., VPN, HTTPS).
- Remote staff must use:
 - Devices with full disk encryption (e.g., FileVault, BitLocker)
 - Encrypted cloud collaboration tools
- Use of unsecured protocols (e.g., FTP, Telnet, HTTP) is prohibited.

E. Digital Signatures and Integrity Protection

Digital signatures may be used to verify integrity and origin of critical data (e.g., audit logs, code signing). Integrity of software builds and containers is validated using checksums or signed artifacts (e.g., SHA-256 hashes or GPG signatures).

F. Exceptions and Monitoring

	No of Pages	5 of 5
	Document Classification:	Internal
	Effective Date	1 Aug 2025
CRYPTOGRAPHIC CONTROLS	Doc No	ISMS-TECH-09
	Revision	1.0

Any exceptions from this cryptographic control procedure must be risk-assessed and compensating controls must be identified and implemented to mitigate associated risks.