HUMANICA

Cryptographic and Key Management Policy

Document Version: 5.0

Document No: ISMS-PL-10

Document Owner: ISMR/ISMA

Last Updated: 04-03-2024

Document Control

Document Approvals

This document has been reviewed and approved by:

Prepared by	Reviewed by	Approved by
IT Security	***Head of Development***	***Chief Technology Officer***
Date: 04-03-2024	**Date:** 04-03-2024	**Date:** 04-03-2024

Version History

The following table lists all the revisions made to this document:

Version	Date	Description	Revised By
1.0	31-07-2020	Initial version	Sathaporn K.
2.0	05-07-2021	Annual Review	Divya T.
3.0	01-07-2022	Annual Review	Tosapol Y.
4.0	04-11-2023	Annual Review	Poonnada C.
5.0	04-03-2024	Annual Review	Poonnada C.

Reference: ISO 27001:2013 Requirement

ISO 27701:2019 clause	ISO 27001:2013 clause	Requirement
CL.6.7.1.1	A. 10.1.1	Policy on the use of cryptographic controls
CL.6.7.1.2	A. 10.1.2	Key Management
CL.6.15.1.5 -	- A. 18.1.5	Regulation of cryptographic controls

Table of Contents

Cryptographic and key management policy

Purpose

The purpose of this policy is to define the organization's cryptographic method for internal information in order to prevent unauthorized access to sensitive information. Also, to determine secure sensitive information transmitting and proper encryption key management, so that the encryption key is not lost or compromised to others.

Scope

This policy covers determination of encryption levels, encryption in storage media, encryption in portable computer device, encryption in information transmitting, and correct and secure encryption key management.

Definition

1. Sensitive Information: Information that is classified as "Highly Confidential" or "Confidential" according to *Information Classification and Handling Policy.*
2. Secure Deletion: Secure deletion or elimination of information by a secure method, by which the deleted or eliminated information cannot be recalled or restored.
3. Portable Computer Device: Laptops, smart phones, tablets, flash drives, thumb drives, portable hard disks, as well as other portable devices being used in accessing the organization's IT systems and /or information storage systems.
4. Application Owner: Management of business departments or management who has duties and responsibilities over a work system.

1. Strength of encryption

(1) Strength of encryption of each level of information classification which is defined in Information Classification and Handling Policy shall comply with the organization's *Encryption Standard*.

(2) Strength of encryption of systems and applications shall comply with the organization's *Encryption Standard*.

(3) Encryption using Proprietary Algorithm is not allowed.

(4) *Encryption standard* related with cryptography shall be reviewed in terms of strength of encryption at least once a year or when cryptography technology changes significantly.

2. Encryption in storage media

(1) The organization's sensitive information being stored in storage media which is movable in the organization's internal computer system and owned by the organization shall be protected by encryption.

(2) Sensitive information shall always be protected by passwords together with encryption and comply with the organization's Encryption Standard.

(3) Elimination of encrypted information in different types of storage media shall be done by secure deletion in order to prevent information leakage or information access by unauthorized persons.

3. Encryption in portable computer devices

(1) Environment in Sensitive information in portable computer devices shall always be encrypted according to the organization's *Encryption Standard*.
(2) Removable media such as CDs, back-up tapes, or thumb drives which store sensitive information shall be encrypted and kept in a secure place.
(3) Users of portable computer devices with sensitive information shall check to ensure that such information is encrypted. They shall also take an action to ensure that in case that the encryption key is lost or forgotten, the information can still be accessed. For example, by storing back-up information in the organization's server's files or preparing a back-up key for the encryption.

4. Encryption in transmitting information

(1) Sensitive information transmitted via emails always requires encryption.
(2) Sensitive information or information files transmitted through a public network shall be encrypted or sent through encrypted channels; e.g., Secure FTP, VPN or SSL, etc.
(3) Information transmitted through Wi-Fi from portable computer device or the organization's internal network shall be encrypted at all times, by WPA2 method or a more secure method.
(4) Accessing the organization's information through a public network from a portable computer device shall be encrypted at all times.

5. Confidentiality and key management

(1) The organization's employee shall keep the encryption key and information used to create the encryption key in confidentiality and not to reveal it to non-involving persons, unless it is a disclosure by law, or the information owner's and key's owner have given a written consent, or the senior authority has given his/her approval.
(2) Accessing the encryption key and information used to create the encryption key shall be done only for the organization's business operation and according to the purpose of assigned responsibilities only. Record of the encryption key accessing shall be made and kept for checking within the designated timeframe.
(3) Encryption authorities shall not be able to directly access the encryption key in use unless obtaining permission from the system owner and a system supervisor shall assist them in accessing the system to adjust or change the encryption key.
(4) A key custodian has the responsibilities in protecting the confidentiality, integrity, and availability of the encryption key.
(5) A key owner has the responsibilities to check availability of all encryption keys in his/her scope. The encryption key checking shall be done every year. If a key is lost or reasonably believed to be accessed by an unauthorized person, the encryption authority shall be immediately notified.

6. Request to use, generate, or exchange encryption keys

(1) The organization's employee can request to use or generate an encryption key. In doing so, he/she shall present his authentication data and the system owner's written consent or management's approval.
(2) The organization's employee who requests to generate the encryption key shall register with the IT Infrastructure, indicating all sensitive data; e.g., the IT system's name, reasons to use the encryption key, time period to use the encryption key.
(3) The generation of the encryption key shall be done by the encryption key custodian only, using a secure algorithm according to the organization's *Encryption Standard*.
(4) In generating an encryption key which needs a linkage between the entity (a person, a department, or the organization) and the encryption key, the person, the department's head,

and senior management, respectively, shall give their approval. And the encryption key shall be checked if it correctly identifies the right entity as indicated.

(5) The encryption key generation shall be done systematically with sufficient protection so that involving authority cannot change or take any actions than impact the encryption key generation ceremony and outputs.

(6) In generating or exchanging the encryption key, the data used to generate the encryption key shall be designed with appropriate segregation of duties. The encryption key generation or exchange shall not be able to be accomplished by the encryption key custodian only.

(7) In moving or sending the encrypted key, the authentication of the sender and receiver shall be confirmed. The receiver shall confirm and check if the encryption key received is correct. This process shall be recorded for checking within the designated timeframe.

7. Key usage

(1) The encryption key loading shall be designed with secure segregation of duties and shall be recorded with relevant evidence.

(2) The encryption key which can be used in the system shall have the following qualifications:
   1) It shall be within the crypto period.
   2) It shall be generated and used for a specific purpose and never been used before. For example, the encryption key used in test environment shall be different from the encryption key used in production environment, or the encryption.
   3) Key used in one work system shall be different from that of another system.
   4) The encryption key shall never be revealed to unauthorized persons.

(3) During the use of IT systems, unauthorized key access shall be appropriately prevented.

(4) To access the encryption key in use, one shall get a written permission from the system owner and key custodian. The access shall be recorded and stored for backward checking within the designated timeframe.

8. Backup and recovery

(1) The encryption key in use shall be backed-up so that it can be recovered if the encryption key is lost.

(2) Back-up of the encryption key shall be protected for its confidentiality, integrity, and availability or physical control of the same qualification shall be executed. There shall be a measurement to detect unauthorized key access.

(3) In case that the encryption key exceeds its crypto period but may be recalled for use in the future, such encryption key shall be stored in Archive Storage with protection of its confidentiality, integrity, and availability as if it is in the crypto period.

(4) Recovery of the encryption key from the Archive Storage (Backup and Archive) shall obtain a written permission from the system owner and key custodian. The recovery shall be recorded and stored for backward checking within the designated timeframe.

9. Key change

(1) The encryption key shall be changed when:
   1) An annual rotation of the encryption key is recommended as an effective way to improve security and reduce the possibility of persistent vulnerabilities.
   2) It can be reasonably believed that the encryption key has been compromised.
   3) It is near the end of its designated cryptographic period. The crypto period refers to the predefined duration during which the encryption key is considered secure.
   4) It nearly expires as indicated in the timeframe when making the encryption key request.

(2) When the encryption key is changed, the existing key shall be backup and then destroyed when data is end of retention period until it cannot be restored or reused.

(3) Change of the encryption key shall obtain a written permission from the system owner and key custodian. The encryption key change shall be recorded and stored for backward checking within the designated timeframe.

10. Key cancellation and elimination

(1) The encryption key which is near the end of its crypto period and is not necessary to be used for data decryption or electronics signature confirmation shall be immediately destroyed. One shall ensure that the encryption key can no longer be restored.
(2) In case that the encryption key is linked with an entity, the linkage with such entity shall be cancelled. The linkage cancellation shall be recorded and stored for backward checking within the designated timeframe.
(3) The encryption key cancellation and elimination shall be recorded and stored for backward checking within the designated timeframe.

Supporting Document

1. Encryption Standard

End of document