HUMANICA

IT Operation Policy

Document Version: 4.0

Document No: ISMS-PL-05

Document Owner: ISMR/ISMA

Last Updated: 07-12-2023

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 : 07-12-2023	**Date :** 07-12-2023	**Date :** 07-12-2023

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	07-12-2023	Annual Review - Add content Storing back-up on cloud storage	Ronnakorn N.

Reference: ISO 27001:2013 Requirement

ISO 27701:2019 clause	ISO 27001:2019 clause	Requirement
CL.6.9.1	A.12.1	Operational procedures and responsibilities CL.6.9.1.1, A.12.1.1 Documented operating procedures CL.6.9.1.2, A.12.1.2 Change management CL.6.9.1.3, A.12.1.3 Capacity management CL.6.9.1.4, A.12.1.4 Separation of development, testing and operational environments
CL.6.9.2	A.12.2	Protection from malware CL.6.9.2.1, A.12.2.1Controls against malware
CL.6.9.3	A.12.3	Backup CL.6.9.3.1, A.12.3.1Information backup
CL.6.9.4	A.12.4	Logging and monitoring CL.6.9.4.1, A.12.4.1 Event logging CL.6.9.4.2, A.12.4.2 Protection of log information

ISO 27701:2019 clause	ISO 27001:2019 clause	Requirement
		CL.6.9.4.3, A.12.4.3 Administrator and operator logs CL.6.9.4.4, A.12.4.4 Clock synchronization
CL.6.9.5	A.12.5	Control of operational software CL.6.9.5.1, A.12.5.1 Installation of software on operational systems
CL.6.9.6	A.12.6	Technical vulnerability management CL.6.9.6.1, A.12.6.1 Management of technical vulnerabilities CL.6.9.6.2, A.12.6.2 Restrictions on software installation
CL.6.9.7	A.12.7	Information systems audit considerations CL.6.9.7.1, A.12.7.1 Information systems audit controls
CL.6.13.1.7	A.16.1.7	Collection of evidence
CL.6.15.1.3	A.18.1.3	Protection of records
CL.6.15.2.3	A. 18.2.3	Technical compliance review

HUMANICA

Table of Contents

IT Operation Policy

Purpose

The purpose of this policy is to establish security guidelines to ensure standardized, correct, and secure IT operations of the organization and to prevent any pitfalls that may happen.

Scope

This policy covers Information Systems and operations related to IT operation systems of the organization.

Definition

1. IT Operations: Control, supervision, and management of Information systems so that they maintain availability, integrity, and security.
2. Application owner: Management of a business department or management who has duties and responsibilities over an application.

1. Documentation of operational policy

1.1. Important operation procedure related to IT shall be properly documented as Operation Procedures / Operation Manual to be the guidelines for all relevant authorities / employees.

1.2. Application owners or system administrators shall create Operation Procedures / Operation Manual for they own application on the vurapplication under their responsibility. They shall undertake regularly review and update the documents to ensure that they are always correct and up-to-date. These documents shall be disseminated to those who need to use the Operation Procedures / Operation Manual according to their job functions.

1.3. In case of using System/product manuals received from manufacturers, vendors or service providers, both in document and electronic format, as reference or in operation, they shall be securely stored and made available at all time.

2. Audit logging and monitoring system usage

2.1 Usage, operation, and security related events of the organization's Information systems shall be logged, both in the level of operating system and application, to collect the information at a minimum the following:

1) System logs.
2) Application logs.
3) Access logs.
4) Login attempts logs.
5) Firewall/IPS logs.
6) Backup logs.
7) Remote access/VPN logs.
8) Traffic Logs and user information as stated in Computer Related Crime Act B.E.2550 (2007) including Regulations or Notifications issued under the Computer-related Crime Act B.E. 2550 (2007), Commission of Computer Related Offences Act (No.2), B.E.2560 (2017).

2.2 Logs of sensitive or critical systems shall be kept to be secured for the analysis benefits and to protect them from unauthorized access and modification.

2.3 Application administrator shall regularly monitor all logs and record the results. In case an error or something abnormal is discovered, their supervisors or the Security Incident Team shall be reported.

3. Logging and monitoring system administrator operation

3.1 System Administrator activities shall be logged, especially their operation in important activities; such as, creating a new user in the system, modifying the system, etc.
3.2 Such system administration logs shall be recorded, reviewed, and monitored at least 2 times per year.
3.3 Fault logging shall be enabled for all the information systems, equipment and network devices irrespective of the business criticality and the data handled by the systems.
3.4 Fault logs shall be reviewed on the monthly basis to ensure that all the incidents are reported, investigated and resolved in a timely manner.

4. Change management

Change management process shall be implemented to ensure that any change which may cause negative impact to sensitive or critical Information systems will be appropriately controlled and approved by authority as indicated in *Change Management Procedure.*

5. Capacity planning and management

5.1 When there is a need to purchase or upgrade sensitive or critical equipment or systems, application owners or system administrators shall forecast the future usage (capacity) needs of such equipment, system so that they can serve the future needs.
5.2 System administrators shall regularly monitor the operation of sensitive or critical Information systems to ensure operational efficiency and continuity. The findings will be used to evaluate performance and capacity of the systems.
5.3 Application owners and system administrators shall regularly evaluate the efficiency of the Information systems and all relevant equipment by surveying user's current and future needs, usage volume, system response time and other variables to improve performance and capacity of the systems. *Refer to Capacity Management Procedure.*

6. Protection against malicious code

6.1 All servers and workstations/clients connected to the organization's networks shall be protected by installing appropriate anti-virus software. Engine and virus database/signature/definition of such software shall be regularly updated (no more than 2 days of signatures being released by the vendor). Effective controls shall be implemented to protect the software from unauthorized disabling or interfering.
6.2 Anti-virus software shall be configured to weekly scan for virus.
6.3 Anti-virus software administrators shall regularly follow updated news and information about virus and malicious code from reliable sources and communicated updated information about virus and malicious codes to users.
6.4 User shall not install unauthorized software into any computer, server and other relevant equipment.

7. Information back-up

7.1 Important information back-up shall be appropriately implemented to protect availability and continuity of information and systems.
7.2 Backing up information

(1) Business information, operating systems, application systems, source codes, configurations, scripts/commands/instructions and utilities shall be completely backed up for continued availability.

(2) Information Backup Procedure shall be established as a guideline for operating persons.

7.3 Testing Back-up Information

(1) Back-up Information Restoration and Testing Procedure shall be established to be guidelines for operation employees.

(2) Back-up information of important systems shall be tested at least once a year to ensure integrity and availability of the information and system programs.

7.4 Storing back-up media

(1) Back-up media shall be properly labeled to ensure the quick retrieval and to prevent confusion or error.

(2) Back-up media containing sensitive information classified as “Highly Confidential” and “Confidential” shall be properly protected in accordance with the importance of information contained therein. In general, back-up media shall be classified as “Confidential”, except when other classification is indicated.

(3) Back-up Information, related procedures, and documents shall be stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site. Such location shall maintain appropriate levels of physical and environmental.

(4) For back-up media needs to be stored for a long period, future restoration method shall be considered and planned; such as, storing related software or equipment which are used to read information from those media altogether.

(5) Request to use back-up information shall be considered and approved by data owners or related authority.

(6) Rotating of back-up media between main site and remote location shall be logged and tracked completely and correctly at all times.

(7) Back-up information which is no longer in use shall be appropriately destroyed to prevent unauthorized restoration of information.

7.5 Storing back-up on cloud storage

(1) The frequency and extent of backups must be in accordance with the importance of the information and the acceptable risk is determined by the data owner.

(2) Back-up Information, related procedures, and documents shall be stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site. Such location shall maintain appropriate levels of physical and environmental.

(3) Request to use back-up information shall be considered and approved by data owners or related authority.

(4) Back-up status and back-up history shall be logged and tracked completely and correct accordance with retention period.

(5) For back-up information needs to be stored for a long-term cloud storage, future restoration methods shall be considered and planned. This may involve ensuring compatibility with future software or equipment necessary for data retrieval from the cloud.

(6) Back-up information which is no longer in use shall be appropriately destroyed to prevent unauthorized restoration of information.

8. Clock synchronization

8.1 Clock of all systems, servers and computers, including security devices shall be synchronized to an agreed standard time of a reliable source such as clock.nectec.or.th, time.google.com.

8.2 There shall be regular random checking of the clock of servers and computers.

8.3 Clock of all systems, servers and computers, including security devices that are joined to the domain are synchronized with the domain controller's Network Time Protocol Server.

9. Technical vulnerability management

9.1 Control and correction of technical vulnerabilities

(1) Update news and information about new release of software/operating system patches and other relevant equipment shall be followed from websites or reliable sources and patches shall be installed to correct such defect.

9.2 Technical compliance checking

(1) The organization shall arrange Technical Security and Compliance Checking by authorized staffs or outsourced specialists at least once a year and least quarterly for vulnerability scanning to ensure that all systems are appropriately installed, configured and used. The target systems for checking can be randomized and rotated as deem appropriate.

(2) Management's written approval shall be obtained before the checking is carried out.

(3) Changes to information caused by the checking process are absolutely prohibited. If it is necessary to modify data for the checking purpose, written approval from managements of applicable departments shall be obtained prior to executing the modification and such changes shall be made only to the copies of information. (Changes are definitely not allowed for original information).

(4) All copies of information used for technical compliance checking shall be properly destroyed at the end of the process (except the result of technical compliance checking).

(5) Method and details of information access shall be logged and documented.

(6) In case that technical compliance checking is executed by outsourced specialists, Non-Disclosure Agreement and Contract shall be properly.

(7) At the end of checking process, user ID and password provided for outsourced specialist shall be immediately terminated or changed.

(8) Results of technical compliance checking shall be sent to IT Security Team for reviewing and finding solutions, in order to send the results further to management for approval of the solution implementation

10. Protection of original software and control of software installation on the information systems in use

10.1 Original software, including applications, tools, operating systems, license key, and related document shall be kept in a secure place with a good management system or process in order to prevent damage, loss, or unauthorized access.

10.2 Approval shall be obtained before installing software on the Information systems in use.

11. System audit control and protection of system audit tools

In case system security audit is done by the organization's personal with the use of software or tools, such software or tools shall be kept in a secure place and protected to prevent unauthorized access or misuse.

12. Separation of development testing and operation environment

Development and test environments shall be separated from production operational environments in order to reduce the risk of accidental changes, configuration/data incompatibilities and unauthorized access.

Development and production environments shall be segregated by the most appropriate controls including:

(1) Running on separate computer/systems
(2) Running on different domains
(3) Secure disposal of data/information used in the test environments.
(4) Use of test/temporary usernames and passwords
(5) Access control procedures which apply to operational systems should also apply to test applications.
(6) The production system(s)/environment(s) shall be logically and physically separated from the development and test environments. The use of virtualization for the segregation of system(s)/environment(s) shall be approved by the IT manager based on the results of a risk assessment.
(7) Access to production, development and test environments shall be provided on the basis of segregation of duties.
(8) Physical access to the production environment should be monitored.
(9) The data used for the test and development systems/environments shall be dummy data. If the production data is required for testing and development activities, it shall be sanitized and masked prior to its use in the test or development environments.
(10) All test data, temporary accounts and temporary passwords shall be removed from the systems prior to deploying them into the production environment.
(11) Where practical, separation of duties should be maintained to ensure no one individual can gain unacceptably high levels of access to the organization's systems and information processing facilities.

Supporting documents

1. Change Management Procedure
2. Security Incident Management Procedure
3. Disposal Media Procedure
4. Log Management Procedure
5. Vulnerability Management Procedure

End of document