HUMANICA

Acceptable Use Policy

Document Version: 4.0

Document No: ISMS-PL-02

Document Owner: ISMR/ISMA

Last Updated: 23-11-2023

HUMANICA

Document control

Document Approvals

This document has been reviewed and approved by:

Prepared by	Reviewed by	Approved by
IT Security	***Head of Department***	***Chief Technology Officer***
Date : 23-11-2023	**Date :** 23-11-2023	**Date :** 23-11-2023

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.
2.1	24-03-2022	Add Data breach topic	Tosapol Y.
3.0	01-07-2022	Annual Review	Tosapol Y.
4.0	23-11-2023	Annual Review	Ronnakorn N.

Reference: ISO/IEC 27001:2013 & ISO/ IEC 27701:2019 Requirement

ISO/IEC 27701:2019 Clause	ISO/IEC 27001:2013 Clause	Requirement
CL.6.5.1.3	A.8.1.3	Acceptable use of assets
CL.6.5.3.1	A.8.3.1	Management of removable Media
CL.6.6.1.1	A.9.1.1	Access control policy
CL.6.6.1.2	A.9.1.2	Access to networks and network services
CL.6.6.3.1	A.9.3.1	Use of secret authentication information
CL.6.6.4.1	A.9.4.1	Information access restriction
CL.6.6.4.2	A.9.4.2	Secure log-on procedures
CL.6.8.1.2	A.11.1.2	Physical entry controls
CL.6.8.1.5	A.11.1.5	Working in secure areas
CL.6.8.2.1	A.11.2.1	Equipment siting and protection
CL.6.8.2.5	A.11.2.5	Removal of assets
CL.6.8.2.8	A.11.2.8	Unattended user equipment
CL.6.8.2.9	A.11.2.9	Clear desk and clear screen policy
CL.6.9.2.1	A.12.2.1	Controls against malware
CL.6.10.2.3	A.13.2.3	Electronic messaging
CL.6.13.1.2	A.16.1.2	Reporting information security events
CL.6.13.1.3	A.16.1.3	Reporting information security weaknesses
CL.6.15.1.3	A.18.1.3	Protection of records
CL.6.15.1.2	A.18.1.2	Intellectual property rights
CL.6.15.2.2	A.18.2.2	Compliance with security policies and standards

HUMANICA

Table of Contents

Acceptable use policy

Purpose

The purpose of this policy is to define acceptable use to be in accordance with related laws and security requirements of the organization, as well as to ensure appropriate protection of employees and the organization's assets and to prevent inappropriate use that could expose the organization to security risks including unauthorized disclosure of sensitive information, system and network attacks, service system attacks, legal violation actions, etc.

Scope

This policy applies to all personnel who involve with usage of the organization's information and computer systems including management, permanent employees, temporary employees, partners, business agents, affiliates and third parties who are hired by the organization, the organization's partner, contract partners, or service providers.

Definition

1. Sensitive Information: Information that is classified as "Highly Confidential" or "Confidential" according to *Information Classification and Handling Policy*.

Acceptable use policy

1 Protection of the organization's information and information systems

To preserve the security of business information, customer confidence and organization reputation, the organization will:

1.1 The organization's information: The organization's information is the most critical asset which shall be properly protected so that it remains:

(1) Private (Confidentiality)

(2) Accurate, complete, and authentic (Integrity)

(3) Available when needed (Availability)

1.2 The organization's computers: The organization's business operations have become totally dependent upon computers, networks, and electronic data. So, it is the duty of all employees and involving parties to do everything the best they can to secure the organization's computers and network systems.

1.3 The organization's offices: The organization's offices are the employees' and involving parties' working space. These offices' security can be violated if not being properly protected.

(1) Monitoring the usage of the organization's information assets and all system activities to enforce the provisions of information security policies.

(2) Installing or testing any controls consistent with the requirements of information security policies.

(3) Taking any other steps as deemed necessary to manage and protect organization information systems. These authorities may be exercised with or without notice to the involved personnel.

2 The organization's information

2.1 Classifying and labeling information

Data owners shall classify all information under their responsibilities in terms of confidentiality, by considering necessity to access information for business operation, related legal or regulatory requirements for protecting information and business impacts associated with such needs. By default, all information handled by the organization is classified as "Internal Use Only" unless explicitly classified otherwise. For more information, refer to rules and instructions set forth in *Information Classification and Handling Policy*.

2.2 Using and protecting sensitive information

(1) All users shall ensure that their usages of the organization's information strictly comply with rules and instructions set forth in *Information Classification and Handling Policy.*

(2) Users shall take special care when using "Highly Confidential" and "Confidential" information (hereafter, "sensitive information"), as specified in *Information Classification and Handling Policy* in order to prevent the unauthorized access to and disclosure of this information.

(3) The organization's sensitive information shall not be revealed or shared to others except in the case of normal business operation, or legal requirements, or getting approval from authorities.

(4) Users shall be aware of sensitive information being stored on their computers; especially the computers that are used by more than one user. All such information shall be properly protected by encryptions or any protections provided by operating system or Information systems. It shall be encrypted accordance with *Information Classification and Handling Policy.*

(5) Users should keep their sensitive documents and removable storage media in suitable locked cabinets and/or other forms of security furniture when not in use.

(6) Sensitive information should be cleared from information processing facilities, for example, printers, fax, photocopiers, etc., immediately.

(7) Employees shall not disclose the organization's information to outsiders, unless the information is public information, obtain an authority's approval, and such disclosure is covered by a valid Non-Disclosure Agreement.

2.3 Using storage media containing sensitive information

(1) Storage media and removable media and mobile equipment (such as smart phones, tablets, USB drive, CD-ROM, etc.) must be strictly controls before connecting with organization equipment or system, these devices are required to undergoing virus checks by the IT department and receiving authorization from a manager.

(2) Storage media and removable media and mobile equipment (such as smart phones, tablets, USB drive, CD-ROM, etc.) containing the organization's sensitive information shall be maintained and handled with care in accordance with *Information Classification and Handling Policy.*

2.4 Data breach

A data breach is any (potential) unintended loss of control over or loss of personal data within company environment. Preventing a data breach is the responsibility of all employees and contracted workforce. In addition, everyone is encouraged to notify IT support team in case of an irregularity in relation to personal data processing activities. A timely discovery, response, treatment, and notification (of both regulatory authorities and potentially the data subject's impacted) process is outlined in *Security Incident Management Procedure*.

3 The organization's computer

3.1 Usage of equipment

(1) The organization's Information systems and all related information processing equipment and facilities which belong to the organization or being provided by the organization are provided to users for the purpose of conducting the organization's business only. Personal use is not allowed.

(2) It is users' responsibilities to exercise reasonable care when using the organization's computers and computing equipment and strictly provide them protection according to the *Information Security Policy*.

(3) Users shall locate personal computers or workstations suitably in the secured office area and make sure outsiders cannot see sensitive information through the windows, glass wall, hallway, or guest areas.

(4) All the organization's personal computers, notebooks, servers, workstations, and terminals shall be secured using operating system password when logging on, and password-protected screensaver with automatic lock feature has been set to automatically turn on after 15 minutes of inactivity. Employees are expected to adhere to the practice of ensuring a clear desk and screen by either locking the screen or logging off when the equipment is not in use.

(5) Users shall not connect their privately own computers to the organization's network without permission.

(6) Laptop Computers that contain the organization's information shall be protected using the same standard as if it were inside the centralized Information systems. This includes installing approved personal firewall anti-virus software, security patch updates, etc. Users shall protect such information and equipment according to *Mobile Device and Teleworking Policy.*

(7) Computer equipment provided by the organization shall not be altered or added in any way without departmental management acknowledgement and authorization. Employees shall not allow anyone to add hardware or software to the organization's computer unless they have appropriate authority.

(8) Users shall get the 'user' right only, in order to prevent unauthorized software installation or removal. In a necessary case, user can ask for authority's permission to obtain a privileged user account suitable for their obligation. This is a case-by-case permission and the expiry date shall be determined.

3.2 Use of software (portable software)

(1) Employees are not allowed to install any software to the organization's computers unless obtaining an authority's permission.

(2) Employee shall not install or distribute "pirated" software products to the organization's system.

(3) Employees shall not install the organization's software for their personal use or make a copy without permission.

3.3 Usage of email

(1) All email users shall be provided with an individual email account. The organization may provide an email account to users who are not employees after they obtain the departmental management's permission and agree with *Third Party Security Policy*.

(2) Every email account shall be password protected, as a deterrent to potential intruders and to the misuse of email.

(3) Special purpose email account may be created to be centrally used for the department and/or may be shared by more than one user. One of the users who manage and supervise the use of this email account shall be appointed as an email account owner.

(4) The entire organization's email accounts and all emails (including personal emails) created and stored on the organization's computer networks are property of the organization.

(5) Users shall only use the approved email client software to access to and/or communicate with corporate email system.

(6) Employees' use of email accounts to engage in illegal activity (for example advertising illegal goods, counterfeit products, contempt, or spreading illegal copies of computer software is strictly prohibited.

(7) Employees shall not use the organization's email address to post information to electronics community (such as web board, blog, newsgroup, etc.), unless such posting is under the course of business duties.

(8) Sensitive information sent via email shall be encrypted, so that only the intended recipient can read it.

(9) The disclaimer notifications stating that the message sent is intended solely for the addressee and the organization does not accept responsibility for the content of the email shall be attached automatically at the footer of the all outgoing mails from the organization.

(10) Email users shall create content of the email carefully, always aware that they are sending out that email in the name of the organization.

(11) Access to other people's email account is prohibited unless obtaining authority's permission.

(12) Users shall definitely not imitate, forge or attempt to forge email messages, headers, signatures and identities or account of other users.

(13) In case that users have another person to send email using their accounts such as their secretaries, assistants and any other subordinates, such person shall send the email 'on behalf of' the users.

(14) Users shall send emails to the involving recipients who need to know such information only.

(15) Users shall not send unsolicited email messages, including "junk mail", "spam mail", "chain letter schemes", or any fraudulent mails of any type.

(16) Users shall not send or forward emails containing words, phrases, photos, or other materials which may be libelous, defamatory, offensive, racist, blackmailing, gambling, or obscene, pornographic, sexually or racially abusive.

(17) Users shall use extreme caution when opening e-mail attachments received from unknown sources or senders, which may contain viruses, email bombs, or malicious software.

3.4 Usage of internet

(1) Users shall exercise extreme caution when using the Internet. The use of Internet shall not cause the organization or the persons with which the organization has any form of relationship, into disrepute or being exposed to any legal or regulatory action. Any misuse of the service may result in disciplinary action or, in appropriate cases, legal proceedings.

(2) Access to the internet may only be conducted either through the organization's approved gateways. The organization reserves the right to monitor users' Internet activities to detect inappropriate usage.

(3) Users shall not view, use, download, receive or proliferate any pornography, offensive, obscene, or illegal materials/contents.

(4) If users notice the abnormality of computers after visiting any website, they shall immediately notify Support desk to correct such problems.

3.5 Prevention of virus

(1) Users shall not create, store or distribute malicious program (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) into the organization's computing environment, unless it is the operation under responsibilities.

(2) User shall not obstruct or interfere with the operation of corporate approved anti-virus software.

(3) The only files which shall be transmitted and/or received are files related to business purposes. Files should be accepted from known counterparts and only when the communication is expected. Before open received files, they shall be scanned by corporate approved anti-virus software.

(4) If virus infection is suspected or informed by anti-virus software, user shall suspend all works and contact Support desk immediately.

3.6 Usage of user account, password and secured identity verification equipment

(1) Each individual user shall be granted unique user account/password for accessing to the organization's systems or services. This shall be in accordance with the "need-to-know" and "need-to-use" basis.

(2) Users will be held responsible for all activities performed by their user accounts and associated passwords.

(3) All passwords shall be changed at first use and at the defined interval in accordance with the organization *Password Standard*.

(4) All passwords shall be secure and meet or exceed all the requirements in the *Password Standard*.

(5) Passwords shall be treated as "Confidential" information. It is each user's responsibility to keep their passwords secured and do not share accounts/passwords or allowing other people to use their account.

(6) All privileged user IDs in the organization's critical systems shall be controlled by IT security team or any formally assigned authorities.

(7) If an account or password is suspected to have been revealed or used by unauthorized persons, users shall report the incident to IT Security Team, and change all passwords immediately.

(8) Password reset requested by users will be performed only through the organization's standard request process where user shall identify him/herself and ownership of the requested account. The responsible authority may request for appropriate identification or verification process.

(9) It is the duty of all users to keep the security of identification verification equipment such as Hardware Token, Software Token or Access Card (if any); e.g., Employee ID Card, Third-Party ID Card. This equipment cannot be shared or used by any other people who are not involved or possess the right.

(10) When the identification verification equipment is damaged, lost, cancelled, or adjust information or right, the users shall request IT security team or the department which manage such identification verification equipment to immediately cancel, terminate, change, or correct such equipment.

4 The organization's office

4.1 Physical security

(1) Employees shall maintain their working environment to be in a good order and secure at all times.

(2) Visitors and third party shall be verified their identification cards for the organization's visitor badge before being allowed to access the organization's premise. The identification card to be used shall be issued by government offices with a clear photo, e.g., ID card, driving license, passports in accordance with *Physical and Environmental Security Policy*.

(3) The organization's employees and third parties shall wear their Identity or visitor badges on the organization's premises at all times. Identity and Visitor badges are not transferable. One shall not lend his/her badge to another person.

(4) Employees shall not leave a door open or allow anyone to enter the organization's premises with them or behind them unless they can show a valid Identity Badge or visitor badge. This is to prevent access to the organization's office and security-controlled areas by unauthorized persons.

(5) When noticing strangers or anyone who does not wear a valid Identity or visitor badge, employees shall notify security guards immediately.

(6) Employees should escort, observe, supervise and advise their visitors for their entire visit to the organization's premise.

(7) Employees should check their working area as a security routine at the end of each working day to ensure all safes, document cabinets, desks and workstations are locked and the keys are secured.

(8) The organization's information, recording media, and storage equipment shall not be left on unattended desks, in empty meeting rooms / boards or unlocked cabinets.

(9) The organization's information, recording media, and storage equipment shall not be disposed to waste bin without being properly destroyed in accordance with *Information Classification and Handling Policy*.

(10) Employees shall not allow their computer or storage media to be removed from their work area or facility unless they are certain that the person removing it is authorized and has a valid command from the organization.

4.2 Network security

(1) Users shall not install modems or mobile hotspots relating to their computers or anywhere on the organization's network without permission.

(2) Third-parties and outsiders are definitely not allowed to freely connect their laptops, equipment or any other outside computing devices to the organization's systems or networks. In a necessary case, appropriate approving procedure shall be followed prior to connection.

(3) Users shall definitely not install hardware or software that provides network services, such as routers, switches, hubs and wireless access points, without appropriate management approval.

(4) Remote access to the organization's network requires a proper authentication and shall comply with *Network Management Policy*.

4.3 Usage of telephone, fax, and copy machine

(1) Users shall do their best to ensure full security of sensitive information when transmitting it via facsimile machines. Refer to *Information Classification and Handling Policy* for more details.

(2) If users receive a facsimile in error (wrong number, person, office, location or department), they shall notify the sender, and the misdirected facsimiles shall be destroyed.

(3) Users shall not print sensitive information to printers residing in common areas unless there is a person authorized to receive the information waiting at the machine.

(4) Users shall not record or leave messages containing sensitive information on answering machines or voice mail systems.

(5) Sensitive information shall not be discussed through the phone's speakerphones or other electronic media, including Voice over IP systems, during conference calls unless:

- All authorized parties participating in the call have been authenticated and have the right to know such information;
- All authorized parties have previously verified that no unauthorized persons are in such proximity that they might overhear the conversation
- The conference call is made in an area of the building that is secure (e.g. offices or conference rooms where the door can be closed and conversations cannot be overheard through thin walls)

(6) Care shall be taken to ensure that sensitive information cannot be overheard when it is disclosed or communicated over the telephone.

(7) If sensitive information is requested over the telephone, before the information is disclosed, the identity of the caller or requester shall be verified to ensure that they are authorized persons to receive such information.

(8) Users shall use the information for operation as the intended purpose stated when asking for permission from the information owner. Permission shall be received from information owner before photocopying or scanning of sensitive documents. Copied or scanned sensitive documents shall receive the same protection level as the original documents in accordance with *Information Classification and Handling Policy*.

(9) Employee shall definitely not disclose the location of data center to outsider unless it is required for business operation.

5. The organization's employees

5.1 Compliance with policies and regulations

(1) all employees are expected to be aware of, understand and strictly follow the released/announced information security policies and relevant documents.

(2) the information created/stored on or transmitted through the organization's information systems is the property of the organization. In case of legal actions, request from government authorities, or any crime investigation, the organization can disclose or use such information for such purposes without prior user notification.

(3) to manage and ensure the organization's information systems 's security, the organization reserves the right to monitor computing facilities or computer equipment, systems and network traffics at any time to ensure compliance with the published security policies.

(4) the organization retains the right to access, review and monitor user's email without prior notification. However, such an action will be taken only when the circumstances deem it necessary. In such cases, the organization will not disclose any user's information unless required by courts, legal enforcement or with the consent of the user.

(5) all the organization's employees shall not violate any laws of the kingdom of Thailand or international laws with the use of the organization-owned asset, information systems and resources in any cases.

(6) Unauthorized usage and copying of copyrighted materials including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, articles, books or other documents, and the installation of any copyrighted software for which the organization or the user does not have an active license is strictly prohibited.

(7) exporting software, the organization's information, encryption software or technology outside the country shall comply with the international or regional export control laws, as well as the law of the kingdom of Thailand. Employees shall consult with supervisors and legal experts before exporting such materials.

5.2 Incident Reporting

All employees and third-party users have a duty to report all observed or suspected information security violation, incidents, weaknesses or fraudulent activities in a software or hardware to his/her supervisors or its security team immediately so that prompt remedial action can be taken. They shall not attempt to prove suspected security weaknesses by themselves.

5.3 Other prohibited activities the following activities are prohibited:

(1) Making fraudulent offers of products, items, or services using any of the organization's user account.

(2) Endorsement or guarantee of any document, statement, or object in the name of the organization, either explicitly or implicitly, unless such endorsement and guarantee is a part of assigned responsibilities.

(3) Attempts to conduct security violation or disruptions of network communication; such as, accessing data of which the employee is not an intended recipient or logging into a server of account that the employee is not expressly authorized to access, network sniffing, or any actions that attack or hack the organization's system without permission or for malicious purposes.

(4) Transmitting excessive information or consuming excessive bandwidth which may affect the network, especially when using P2P (peer-to-peer) file sharing applications.

(5) Circumventing user authentication or security measurement of any computers or networks.

(6) Using any program/script/command, or sending messages of any kind, with the intent to interrupt, degrade service performance, or deny service provided to users, via local systems or any networks.

(7) Conduct any form of threatening or harassment via email, telephone or text messaging, whether through words, language used, frequency, or size of the text.

(8) Violations of the personal rights, the organization's copyright, trade secret, patent or other intellectual property, or similar laws or regulations.

(9) Checking-in to social media when entering the security-required and highly-sensitive areas of the organization; such as, Data Center, Network Control Room, Strong Room, etc.

(10) Posting the organization's information which is classified as 'Highly Confidential', 'Confidential', or 'Internal Use only" in social media.

(11) Posting comments in social media about the stock price or other financial information of the organization; e.g., business plan, future annual reports or future performance report.

(12) Posting comments about or referring to the organization's customers, trade partners or service providers in social media without written permission from such persons or organizations.

(13) Conducting the organization's business with the organization's customers, trade partners or service providers through an employee's personal social media account.

(14) Registering to use social media in the name of the organization, unless doing the assigned responsibilities.

Supporting documents

1. Information Classification and Handling Policy
2. Information Security Policy
3. Third Party Security Policy
4. Network Management Policy
5. Mobile Device and Teleworking Policy
6. Security Incident Management Procedure

End of document