HUMANICA

Mobile Device and Teleworking Policy

Document Version : 4.0

Document No. : ISMS-PL-11

Document Owner: ISMR/ISMA

Last Updated: 21-06-2023

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: 21-06-2023	**Date:** 21-06-2023	**Date:** 21-06-2023

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	17-01-2022	Cancel BYOD register form and change to Jira- HUMANICA IT SERVICES	Tosapol Y.
3.0	01-07-2022	Annual review	Tosapol Y.
4.0	21-06-2023	Annual review	Poonnada C.

Reference: ISO 27001:2013 & ISO 27701:2019 requirement

ISO 27701:2019 clause	ISO 27001:2013 clause	Requirement
CL.6.3.2.1	A.6.2.1	Mobile device policy

Table of contents

Document Control 2
Mobile Device and BYOD Policy 4
Purpose 4
Scope 4
Definition 4
Mobile Device and BYOD Policy 4
1. Using Mobile Devices which are the Organization's Asset 4
2. Bringing Personal Computer Devices to Work 5
Supporting Documents 6

Mobile device and teleworking policy

Purpose

The purpose of this policy is to establish guidelines for secure usage of mobile devices, and personal computer in and to prevent leakage or loss of the organization's information from the use of mobile devices, and personal computer in business operation.

Scope

This policy covers usage of mobile devices, and personal computer in business operation by permanent employees, temporary employees, contract partners, trade partners, consultants, third-party, or any person who are permitted to use information, Information systems and other assets related to the organization's Information systems.

Definition

1. Mobile device: Laptops, smart phones, tablets, USB drives, portable hard disks and any other portable devices that are used in accessing the organization's information system networks and/or storing the organization's information.

Mobile device and teleworking policy

1. Using mobile devices which are the organization's asset

1.1. Users shall strictly comply to the organization's security policy when using mobile devices, which means any mobile devices used in linking and accessing to the organization's network system and/or storing the organization's information.

1.2. Mobile devices must be regularly checked to ensure that they are clear of unauthorized software, viruses, or malicious programs.

1.3. Mobile devices to be taken to use in the organization shall be registered and approved for usage by the management of the department which functions to support IT operation. Users of mobile devices shall provide such devices suitable physical protection.

1.4. Software installation in mobile devices shall only follow the organization's requirements.

1.5. Mobile devices shall be version-updated, installed with security patch firmware, and regularly updated anti-virus software according to each device's capacity.

1.6. The organization does not permit modification of operating systems of mobile devices or smart phones apart from those given by their manufacturers, e.g., Jailbreak (for iOS) or Rooted (for Android), etc.

1.7. Users shall only obtain the right as "User", in order to prevent unauthorized installation or removal of software. In a necessary case, users may ask for their management's approval to obtain a privileged user account sufficient for their job assignment. Such privileged account will have an expiration date.

1.8. Highly confidential and confidential data contained in mobile devices shall be classified according to the organization's *Information Classification and Handling* Policy.

1.9. Mobile devices shall be password-protected for every time of usage, depending on the maximum capacity of such device. They shall also be password-protected through auto screen log-on and log-off when not in use.

1.10. Mobile devices shall be protected such drive encryption at appropriate approach.

1.11. Users shall determine a secure password in accessing the devices according to the organization's *Password Standard.*

1.12. Users shall back-up important information in the mobile devices.

2. Bringing your own devices to work (BYOD)

2.1. Prior to bringing a personal computer device to work in the organization, employee shall get an approval and register such personal device with his/her manager. Employees shall strictly comply with the organization's *Information Security Policy.*

2.2. Employees work for the organization according to their assignment and duties, though done by personal computer devices, are regarded as the organization's intellectual property.

2.3. Employees shall let the organization examine their personal computer devices when the organization requests. This is to ensure security of the personal devices used in accessing the organization's information.

2.4. Software installed in employee's personal computer devices are regarded as personal software of such employees. The organization shall not count them as the organization's license, except for the software that the organization provides to employees for their operation or for maintaining the organization's information security on the personal computer devices.

2.5. Personal computer devices used in employees' operation shall be protected by software of security programs suitable for the device and the organization's standard. All software shall be regularly updated.

2.6. The organization reserves the right to deny access to the organization's information and systems from users' personal computer devices if it is discovered that such devices may incur risk to the organization's information, systems, employees, and customers.

2.7. The organization reserves the right to install a self-destructive program on employees' personal computer devices. The organization may give a command to delete information on employees' personal computer devices in case of an incident which may cause information leakage or insecurity.

2.8. All personal computer devices which can access the organization's network shall be examined and authorized by the organization. If an unauthorized personal device is found to attempt to access the organization's network, the organization can deny its access without prior notice.

2.9. Personal computer devices can access the organization's network and information from outside the organization's premise through VPN. The organization's VPN access data will be sent to an employee when permission is obtained. Employees who use personal computer devices shall keep their password a secret and not to share with any other people.

3. Teleworking

3.1. Using information

Information means information in either physical or electronic format which should always be appropriately protected from loss, destruction or unauthorized access as following:

- Highly confidential and confidential data in electronic format shall be properly backed up and stored at employee's computer or at a designated location on organization file server prior to taken off the premises.
- Highly confidential and confidential data in physical format shall be properly backed up and stored in locked cabinet except original file of such information has already been backed up.
- If applicable, paper document shall be kept in concealed envelope which identified employee name on it. For electronic information, encryption shall be executed at all time when not in use, especially for highly confidential and confidential data.
- Information shall be securely stored in safe at hotel room or in locked briefcase when not in use.

- Use of organization information in public area such as airport, restaurant, hotel lobby, elevator or coffee shop shall be avoided. If necessary, precaution shall be taken to protect information from unauthorized access.

3.2. Using mobile device

- Employee shall avoid connecting mobile device to public network system, for example, wireless hotspot available in airport or coffee shop.
- Wireless connection of mobile device shall be disabled when not in use.
- Connecting mobile device to untrusted or insecure devices shall be avoided.
- Employee mobile device in their possession at all times. In case traveling by air, employee shall not check these computers in airline luggage systems.
- Mobile device shall be kept in suitcase or cabinet which is lockable, or be protected by using security cable lock.
- Mobile device shall be protected by operating system password and BIOS password. All passwords shall be strong and secured.
- Employee shall not allow anyone to use their mobile device. If necessary, supervision is required at all times.
- Mobile device shall be kept in specific carrying case which purposely designed to prevent any damage from external impact.
- Employee's name, address and contact number shall be attached on carrying case or at device.
- If applicable, purchase of insurance should be considered to mitigate the risk of loss or damage to mobile device. Besides, Global Positioning System (GPS) technology should be applied to track the location of devices.
- Use of portable mobile device in public area such as airport, restaurant, hotel lobby or coffee shop shall be avoided. If necessary, precaution shall be taken to protect information from unauthorized access.

Supporting documents

1. Information Security Policy
2. Information Classification and Handling Policy
3. Jira- HUMANICA IT SERVICES/ BYOD Register
4. Password Standard

End of document