IHI Power System Malaysia Sdn Bhd Company Policy	
Policy No.	IPSM/POLICY/IT/2021-02
Policy Title	Information Systems User Rules
Effective Date	01st December 2021
Revision History	2.0

1. Purpose

These rules stipulate rules relating to information security, targeting general users of information systems in IHI Power System Malaysia Sdn Bhd (hereinafter referred as the "company"), to achieve both the protection of information and the safe and smooth operation of information networks, based on "Basic Rules of Information Security for the IHI Group" (GG207-01).

The content of these rules is the minimum required conditions common throughout the company, and cannot be relaxed at divisions, etc.

When divisions and departments have received special security requests from customers, this content shall be reinforced by divisional rules, etc.

2. Definition of Terms

Terms used in these rules are defined as follows:

(1) User

A general user of our company's information system, including executive officers, employees, temporary workers, transferred workers, etc.

(2) Information system

A generic term for a computer, computer-related devices, software, networks, etc.

(3) Information device

PC, server and external storage media related to information systems.

(4) External storage media

External hard disk drive, USB memory, memory card, CD/DVD/MO/FD, PDA and other mobile terminal, digital camera, etc.

(5) Division in charge of information systems

Division that is responsible for the infrastructure information system and infrastructure communication network common throughout the company, and bears the responsibility for installation and operation of these systems.

(6) Business data

Electronic information that is connected when business is done in a company and is information other than public information and private information of individuals.

(7) Privately owned information device

Information device shared among an individual and his/her family members.

(8) BYOD

Abbreviation of Bring Your Own Device. This means that a user uses privately owned information devices in business.

(9) Company owned information device

Information device owned by our company and loaned to employees.

(10) File sharing software

Software for sharing files between an unspecified large number of computers via the Internet such as a P2P network. This software is a hotbed for the illegal circulation of information and is used, for example, as a mechanism for the leakage of information through viruses. Typical examples are Winny, WinMX and Share. A request to "Not use Winny" has been issued by the prime minister's official residence (Chief Cabinet Secretary press release "Concerning Information Leaks via Winny" March 15, 2006).

(11) WSUS

Abbreviation of Windows Server Update Service. This refers to the program for fixing Windows (OS) and Office nonconformities and security problems.

(12) Spam

This refers to one-way e-mail that arrives for the purpose of advertising and fraud without users' consent.

(13) e-mail virus

This refers to malicious e-mail of a special nature since it sometimes comes with a virus attachment or with a URL attached that might cause your computer to be infected if accessed.

3. Personal Security

3.1. User Obligations

3.1.1. Registration/Review of Users

(1) Application for registration

Users who need to use network in IPSM for their business shall apply for registration to the division in charge of HR.

(2) Review of registrant

a. This refers to application for deletion by a user without delay to the division in charge of HR when acquired IDs or access rights are no longer required.

b. This refers to application by a manager in each division for the prompt deletion of user IDs, access rights, etc. when a dispatched worker has been replaced or his/her contract has been canceled.

c. This refers to application by a manager of each division for confirmation of the setting status of user IDs in his/her own division, and the deletion of unwanted IDs more than once a year.

3.1.2. Attendance at Information Security Education Course

To correctly use information devices, the user must attend information security education courses provided by our company. Those who were unable to attend courses for some reason shall attend courses when they become able to attend.

3.1.3. Action When a Problem Occurs

(1) Remedying information network problems

When a problem such as defective operation of information devices or communication network related devices is discovered, the user shall report it to the division in charge of information systems and receive instructions from that division.

(2) Remedying information leaks

When the user notices leakage of important information such as client information (including

instances where there is the possibility of leakage) or hears/sees the situation, he/she shall immediately report it to Information Security General Manager (ISGM) via Information Security Manager (ISM) and ask for instructions. He/she shall behave with the procedure in "Information Security Implementation Rules" Chapter 10(Information Security Incident Management).

3.2. Management Framework

Each division shall set up the following framework, and shall plan, implement, and improve information security. For details, refer to "Basic Rules of Information Security for the IHI Group."

(1) ISGM: shall be responsible for promotion of the Information Security Management System within his/her division.
(2) ISM: shall give information assets users required instructions to ensure information security, and manage information assets within his/her division.
(3) Information Security Representative Core Person: shall manage/ implement information security initiatives in the IPSM.

3.3. Other

In the following cases, our company shall be able to review the transmission/reception records of e-mails, Internet browsing records and other electronic data of users and other related persons.

(1) When it is suspected that actions that conflict with laws and regulations have been conducted.
(2) When it is suspected that actions that conflict with office regulations and other rules have been conducted.
(3) When it is suspected that actions that conflict with dispatch workers contracts, subcontracting contracts and other agreements have been conducted.
(4) When information security such as virus countermeasures is required.

4. Handling of Information Devices

4.1. Appropriate Use of Information Devices

4.1.1. Appropriate Use of Hardware

(1) Business data shall be processed/saved on information devices (PCs, external storage media, etc.) loaned by our company, and a superior shall be reported to when there is lack of information devices. Each division shall closely examine the content of relevant reports, provide the enough number of information devices required for business, and manage their operation.
(2) Company issued Information device shall not be brought out office at all time, unless for official offsite business meetings / activities or approved overseas business trips.
(3) The bringing in of privately-owned information devices and other companies' information devices to our company, connecting them to our company's information systems, and processing/saving business data on these devices is prohibited.
(4) Our company's information systems must not be used for purposes other than business.
(5) External storage media shall be stored/managed according to the confidentiality category of the recorded information.
(6) When distributing external storage media on which information is stored, the following countermeasures shall be implemented to protect the media from illegal accessing, improper use or damage during distribution:

a. A reliable delivery company or courier shall be used.
b. Media shall be sufficiently packed to protect contents from physical damage during delivery.
c. Items that require special care in handling, such as strictly confidential information, shall be handed over in person to the other party.

4.1.2. Appropriate Use of Software

(1) The user shall use software purchased by legitimate procedures. Especially, the user must not use pirate edition, license obtained illegally, license that exceed the number of purchases, academic license limited to academic use.
(2) Individuals must not install privately purchased software on our company's information devices.
(3) File sharing software must not be installed on our company's information devices.
(4) In principle, free software shall not be installed.

4.1.3. Appropriate Use of Networks

(1) Browsing of web sites outside the company shall be restricted. How to apply for cancellation of browsing restrictions shall be displayed on the access restriction screen.
(2) The transmission of electronic data to web sites outside the company shall be restricted. Application for cancellation of transmission restrictions shall be performed when data must be sent for business (how to apply will be displayed on the access restriction screen). Application details shall be reviewed by the IHI Information Systems Division who shall judge whether or not to cancel restrictions.
(3) When a user wants to perform data communications with a server outside the company using ftp Proxy, the user shall register the computer to be used in advance (how to apply will be displayed on the access restriction screen).
(4) Otherwise, when a network service outside the company is to be used, the approval of the IHI Intelligent Information Management HQs shall be obtained.
(5) Users of IPSM shall use the designated LAN when working in offices of the IPSM (The local wireless LAN is prohibited to use in offices of the IPSM.
(6) Users shall use VPN immediately when starting to use network outside.

4.2. Security Countermeasures for Information Devices

4.2.1. Password Management

Passwords are important keys for using the in-house information networks. For this reason, each user shall manage passwords properly to prevent them from being used illegally by other people.

(1) Never share your password to anyone else. Do not write it down on a sticky note or the like and paste it on the computer.
(2) The password must be a combination of letters and numbers. Make it 8 characters or longer. Do not use a simple password such as "ihi".
(3) If possible, include symbols (!,#,$,<,>, etc.).
(4) The server administrator in particular must follow the one above.

4.2.2. Implementation of Virus Countermeasures

(1) Installation of anti-virus software

The user shall confirm that the latest version of anti-virus software and pattern files are always installed on PCs to be used by checking the Virus Buster icon at the bottom right of the PC screen.

IHI Intelligent Information Management HQs web site: "About Three Modes of Virus Buster"
http://www.imail.ty.ihi.co.jp/Vinst/trend/reference.htm#t2

(2) Checking for viruses

a. Users shall cooperate in virus inspections performed by the division in charge of information systems.

b. When external storage media brought in from outside the company is inserted or connected to PCs, users shall run anti-virus software to check the media for viruses.

(3) Browsing web sites

Browsing web sites that have nothing to do with business is prohibited.

(4) Remedy when a PC is infected

When a PC in use is infected with a virus, or there is a risk that it is infected with a virus, perform the following remedies:

a. Immediately disconnect the LAN cable from the PC to make the PC offline from the network. (Do not reconnect it until the PC is disinfected.)

b. On PCs such as laptops set with a wireless LAN, turn the wireless switch OFF.

c. Users shall report to the nearest division in charge of information systems and receive instructions from the division.

4.2.3. Implementation of Software Patches

(1) Setup of WSUS for IHI

The user shall set up automatic updating of WSUS on PCs to be used from the following site:

IHI Intelligent Information Management HQs web site: "Windows/Office Updates for IHI"
http://www.imail.ty.ihi.co.jp/update/20_sus/

(2) Other programs

The user shall implement software patches on software purchased individually by the user.

4.2.4. Handling of e-mails

(1) E-mail security countermeasures

When sending important information by e-mail, security countermeasures such as data encryption shall be taken.

(2) Entry of correct destinations (addresses)

a. The user shall take care to prevent e-mails from being sent to a wrong party. Example precautions are as follows:

(a) Display the properties of the destination in the address book, and confirm that the destination is correct from the affiliated div. or personal code.

(b) In Outlook, a list of people you have sent e-mails to in the past will be displayed when you enter a part of the destination name, therefore make use of the function.

b. Persons who have received an e-mail by mistake shall notify it to the sender immediately, and delete the e-mail, etc. that was received by mistake (do not save or forward the e-mail).

(3) Prohibiting of automatic forwarding to addresses outside the company

Automatic forwarding to outside the company (including individual's private e-mail address) using Outlook's automatic forwarding function is prohibited.

If use of automatic forwarding is unavoidable for business, this must be reported to a superior and the superior's approval shall be obtained.

(4) Remedy when e-mail is infected with virus

a. When an e-mail that is suspected of being virus e-mail is received, the user shall observe the following:

(a) Do not touch the file attachment.

(b) Do not click URLs in the message.

b. When an e-mail that is suspected of being virus e-mail is received, the user shall immediately contact the following e-mail point of contact and receive instructions from the point of contact. When contacting the e-mail point of contact, send the received virus e-mail as an attachment to a newly created e-mail (this is because the transmission route information will be lost if the virus e-mail itself is forwarded). There is no need to contact the e-mail point of contact if the e-mail is sorted as a spam or sorted to the Outlook spam folder.

Enter the e-mail address of the anti-virus point of contact here.

c. When a contact destination mentioned in the item above is determined separately by division, contact that destination.

4.2.5. Measures When Away from a PC

The user shall implement the following to prevent peeping or illegal use of user IDs (spoofing):

(1) When away from his/her PC, the user shall either turn it OFF or press ALT+CTRL+DEL and select "Lock".

(2) Just in case the user forgets to lock his/her PC when he/she is away from it, he/she shall preset a screen saver with password to start up automatically. (In principle, set the automatic startup time to ten minutes or less.)

(3) When away from his/her PC overnight or long time, the user shall turn it OFF and leaves it fixing on the desk with the lock or in the locked cabinet.

4.2.6. Management of Shared Folders

On information networks, you cannot tell who is browsing important information and where it is being browsed from. For this reason, access rights to shared folders on the network shall be managed as follows:

(1) The user must not save important information to folders that can be browsed easily by anyone (e.g. folders set with "everyone").

(2) When the user is to save confidential information to a shared folder, disclosure shall be restricted only to authorized personnel by using, for example, folder access rights or RMS encryption.

(3) The person who manages shared folders in the division shall periodically check those assigned access rights for folders where important information is saved, and shall promptly delete inappropriate users such as those who have been transferred to other divisions.

4.2.7. Safe Disposal of Information Devices

When disposing of an information device (including re-use by other people), the user shall render electronic information saved internally on the device impossible to reuse and illegible by an appropriate method such as described below:

(1) Use dedicated software to wipe the entire hard disk by overwriting it at least once with a fixed pattern or the like.
(2) Use dedicated equipment to electrically and magnetically wipe the information device.
(3) Physically destroy the hard disk.
(4) Perform the same when disposing of other electronic media such as floppy disk, magneto-optical disks (MO disks) and CD-R.

5. Strengthen Countermeasures Outside the Company

There are lots of hidden dangers such as loss and theft outside the company. This section stipulates items that must be taken into consideration for information security outside the company.

5.1. Restricting Information Taken Outside the Company

(1) In principle, business data is not to be taken outside the company.
(2) If business data must unavoidably be taken outside the company, observe the following:
   a. Obtain the approval of a superior before taking that device outside the company, selecting data by storing unnecessary data on the file server etc.
   b. Take security countermeasures such as data encryption before taking information devices outside the company.
   c. Do not save business data on privately owned information devices, and also do not browse, process or perform other operations on business data on privately owned information devices.
(3) The division in charge of Information System shall periodically check the devises existing and data or transaction log in the devises.

5.2. Management of Information Devices Taken Outside the Company

(1) PC: In addition to having a hard disk with an encryption function, the very latest information security countermeasures such as automatic startup of a screen saver with an anti-virus password shall be taken.
(2) Storage media: This media shall have a forced encryption function.

5.2.1. User Obligations

(1) Before take-out
   a. Do not save extra data on information devices to be taken out.
   b. Do not set passwords that can be easily guessed to the information device to be taken out, and do not write passwords on labels, etc. and stick the label on the information device.
   c. On PCs, check functions for in-house accessing (iS-VPN, secure remote, etc.) and the point to contact regarding suspension of accessing.
   d. Before taking an external storage media outside the company, run anti-virus software to check the media for viruses.

(2) While information devices are taken out

a. Carried information devices shall not be used for purposes other than business.

b. Pay attention to theft.

(a) When moving by train, bus, etc., the case that contains the information device concerned shall not be placed on luggage racks, for example.

(b) Pay particular attention overseas since there are lots of cases where damage is encountered.

c. (b) Pay attention to surreptitious viewing.

d. When connecting PCs to the Internet outside the company, promptly connect by iS-VPN regardless of wired or wireless connection methods.

(3) At return

a. The return deadline shall be observed. When the return deadline must unavoidably be exceeded, the administrator of the information device exclusively for taking outside the company shall be notified.

b. When returning an external storage media after it has been taken outside the company, run anti-virus software to check the media for viruses.

(4) At loss/theft

When a PC is lost or stolen, take the measures in 3.1.3. Furthermore, contact the administrator of the equipment concerned, and arrange for functions for in-house accessing (iS-VPN, secure remote, etc.) on that PC to be suspended.

5.3. Private Use of IT

5.3.1. Restrictions in Posting In-house Information in Web Sites Outside the Company

In-house information shall not be posted on web sites outside the company (individual web site or blogs, or web sites that can be browsed by an unspecified large number of people such as Internet forum provided by a third party).

(1) Be aware of the danger that in-house information might be posted unknowingly even if it is not intentional.

(2) Even when you have written and posted something as your own personal opinion, be aware of the danger that it might be misunderstood as the opinion of our company when it is viewed by a third party.

5.3.2. Restrictions in File Sharing Software (Winny, Share, etc.)

Be discreet in using, browsing, etc. file sharing software such as Winny or Share even in private spaces.

6. Use of BYOD Tools

Only BYOD tools that have been examined and approved by the IHI Intelligent Information Management HQs from the standpoint of security, convenience, expense, user literacy, etc. and having reasonable security counter measure like installing appropriate security tool may be used on privately owned information devices.

Supplementary Provisions

1. Date of enforcement: 01 December 2021

2. Approver: .....
Masato Tamura
Managing Director

IHI POWER SYSTEM MALAYSIA SDN BHD 861385-P

3. Responsible Division: Projects, Procurement, Finance, Administration & Corporate Planning Div.