IHI Power System Malaysia Sdn Bhd Company Policy	
Policy No.	IPSM/POLICY/IT/2021-03
Policy Title	Information Systems Management Rules
Effective Date	1st December 2021
Revision History	2.0

1. Purpose

These rules stipulate actual procedures such as actions to be observed by divisions in charge of information systems to appropriately manage information systems in IHI Power System Malaysia Sdn Bhd (hereinafter referred as the “company”) based on "Basic Rules of Information Security for the IHI Group" (GG207-01).

2. Scope

These rules apply to divisions responsible for information systems and divisions in charge of information systems (hereinafter referred to as the "divisions responsible for information systems and the like").

If there are any particular requirements/obligations regarding information systems based on agreements with customers, etc., those instructions take priority.

3. Related Documents

(1) GG102-01	IHI Group Information Security Policy
(2) GG207-01	Basic Rules of Information Security for the IHI Group

4. Definition of Terms

(1) Confidentiality

This means ensuring that only authorized persons access information.

(2) Integrity

This means protecting accuracy and completeness of information and its handling methods.

(3) Availability

This means ensuring that an authorized user is allowed to access information and related assets when necessary.

(4) Information system

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

(5) Division responsible for information system

Division that is responsible for information systems, and bears the responsibility for installation and operation of these systems.

(6) Division in charge of information system

Division that is responsible for the infrastructure information system (domain controllers and file servers shared by the entire company) and infrastructure communication network common throughout the company, and bears the responsibility for installation and operation of these systems.

(7) User

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

(8) External storage media

Removable devices and media that can be inserted or connected to servers, PCs or other peripheral devices to store information. Examples of external storage media are external hard disk drives, USB memory, memory card, CD/DVD/Blu-ray disks and other optical disks, and LTO tapes.

(9) VPN

Abbreviation of Virtual Private Network. This is a technology for building a virtual private network by encrypting the communication path when establishing a connection between two bases via the Internet. By establishing a VPN connection with an in-house network from a mobile PC outside the company, users are able to use the in-house information systems in a secure protected environment.

(10) Cloud services

Services where data and software located on the Internet are managed and provided to users by a service provider.

5. Environmental Security

5.1. Equipment

5.1.1. Equipment Siting and Protection

The divisions responsible for information systems and the like shall install server devices and network devices that make up the information system in the server room. The division responsible for the server room shall implement the following:

<1> The server room shall be placed at a location that cannot be seen from the office entrances, and the prevention of tipping over due to earthquakes, etc. and prevention of water leakage due to flooding, etc. shall be considered.

<2> For access control of the server room, people allowed to enter the server room shall be restricted and access records shall be kept.

<3> The server room access records shall be periodically checked every month and maintained for three years. The server room access records shall be protected from tampering and unauthorized access.

5.1.2. Cabling Security

The divisions responsible for information systems and the like shall embed communication cables for transferring data below the floor, in a wall, or in the ceiling to protect them from interception, interference or damage.

The division in charge of information systems shall encrypt the communication path by AES or TKIP systems when wireless LAN access points are installed.

5.1.3. Equipment Maintenance

The divisions responsible for information systems and the like shall perform the following maintenance on devices that make up the information system to maintain stable operation of the information system they are responsible for. These divisions shall study countermeasures immediately when problems are discovered.

- Alive monitoring of all devices that make up the information system and confirmation of error display
- Confirmation of the battery service life of uninterruptible power supplies (UPS)
- Confirmation of hard disk errors
- Cleaning of backup tape equipment

The divisions responsible for information systems and the like shall confirm the end of hardware maintenance contracts and study the timing for renewing these contracts. If necessary, these divisions shall draw up plans for installation of information related devices.

6. Operation Security

6.1. Operation Procedures and Responsibilities

6.1.1. Documented Operating Procedures

Since there is the possibility of operational errors being made in operation of information systems, the divisions responsible for information systems and the like shall prevent the occurrence of this by creating operation procedures and enabling use of them for all persons-in-charge of operation. The following content shall be described in Operation Procedures:

<1> System startup procedure

<2> System stop procedure

<3> Data backup procedure

<4> Data restore procedure

<5> System user registration procedure
<6> System user deletion procedure
<7> Password notification procedure
<8> Password reset procedure

6.1.2. Capacity/Capabilities Management

The divisions responsible for information systems and the like shall periodically check the following system operating statuses so that the information system they are responsible for has sufficient processing capabilities and storage capacity available.

<1> There is sufficient space in storage such as hard disks.

<2> Processing response speeds such as CPU usage rate, memory usage rate, network traffic, etc. do not drop excessively.

<3> The number of software licenses is secured for the required number of users and business is not obstructed.

The divisions responsible for information systems and the like shall predict the required capacity/capability from the future system load based on system operational results so far and if necessary, these divisions shall draw up plans for installation of information related devices.

6.1.3. Separation of Development, Test and Operational Environments

To reduce risks caused by unauthorized accessing or changes on the actually operating operation environment for the information system, the divisions responsible for information systems and the like shall isolate the development environment and test environment for the information system from the operation environment. Even if the environments cannot be separated, countermeasures shall be taken such as isolating the directory exclusively for development from the directory exclusively for operation on the same server, and running the development software and operation software separately. When tests are performed in the development and test environments, actual data in the operation environment shall not be used; test data for testing shall be prepared. The divisions responsible for information systems and the like shall implement sufficient acceptance tests before applying it to the operation environment.

For the development environment and test environment for the information system, room access restrictions shall be implemented by, for example, IC card control.

6.2. Protection from Malware

The divisions responsible for information systems and the like shall confirm that the latest version of anti-virus software and pattern files are installed on the servers and PCs of the information system they are responsible for, and periodically run anti-virus software to check the media for viruses.

6.3. Backup

For rapid recovery from loss of data or system failure accidents on information systems, the divisions responsible for information systems and the like shall periodically back up data and software on the information system they are responsible for. On implementing backups, the divisions responsible for information systems and the like shall study backup schedules, backup methods and storage methods for external storage media in which backup data is stored (e.g. storage in fireproof safes and remote storage in consideration of fires and natural disasters). External storage media in which backup data is stored shall be stored/managed according to the confidentiality category of the stored information.

The divisions responsible for information systems and the like shall constantly monitor that backups are being conducted correctly, and implement recovery tests to see whether or not backup data can be restored to the system.

6.4. Log Acquisition and Monitoring

To prevent illegal access to the information system they are responsible for, the divisions responsible for information systems and the like shall record application-, security- and system-related event logs including user logon/logoff histories and shared folder and database access histories, periodically check for exceptional processing, system faults, suspicious activity, etc. every month, and store these logs and records for three years. The divisions responsible for information systems and the like shall check the internal clock of the information system they are responsible for, and correct any variance between the internal clock and standard time.

The divisions responsible for information systems and the like shall record operation work implemented by the system operation administrator, periodically check work every month, and store these records for three years.

The divisions responsible for information systems and the like shall protect log acquisition functions and log information from tampering and unauthorized access.

6.5. Technical Vulnerability Management

The divisions responsible for information systems and the like shall apply the latest security patches to the OS and applications of the information system they are responsible for. To do so, the divisions responsible for information systems and the like shall acquire information relating to the technical vulnerability of the information system they are responsible for (such as security-conscious configuration information and security patch update information for OS and applications), and implement the required countermeasures after assessing risk. When applying security patches, the divisions shall, if necessary, implement preliminary tests on the development environment, etc. to confirm that there is no impact on the information system functions.

7. Acquisition, Development and Maintenance of System

7.1. Access Restriction on Information Systems and Network

7.1.1. Secure Logon Procedures

To keep information systems and access to applications safe, the division in charge of information systems shall install Windows logon authentication and issue a user ID for each user.

Passwords are important keys for using in-house networks. For this reason, the divisions responsible for information systems and the like shall manage administrator privilege passwords as follows to prevent them from being used illegally by other people.

<1> Passwords must never be told to other people.

<2> Passwords must not be written on labels and stuck on monitors.

<3> Passwords must be a combination of letters (uppercase and lowercase), numbers and symbols (!, #, $, <, >. etc.), and must be at least eight digits.

<4> Simple passwords that can be easily guessed by other people must not be used.

7.1.2. User Access Management

To make access to information systems and services by authorized users reliable and prevent unauthorized access, the divisions responsible for information systems and the like shall register users, delete registered users, and grant, change and delete access rights by the following procedures.

(1) User registration

The divisions responsible for information systems and the like shall register a user ID for each user based on registration applications from divisions that use the information system. Only users authorized by the ISM, etc. of divisions that use the information system shall be registered, and application by irregular methods other than this shall not be accepted. The same shall apply to registration and changing of access rights.

(2) Review of users

<1> The divisions responsible for information systems and the like shall delete user IDs based on deletion applications from divisions that use the information system. The divisions shall also delete access rights, etc.

<2> The divisions responsible for information systems and the like shall check the user ID setting status of the information system they are responsible for at least once per year, and delete unwanted user IDs, access rights, etc.

7.1.3. Access to Network Services

<1> The division in charge of information systems shall install VPN equipment for accessing the in-house network from outside the company, and implement authentication functions.

<2> The division in charge of information systems shall install a mechanism that enables only registered PCs to access the in-house network. such as equipment for preventing illegal connections.

<3> The division t in charge of information systems shall install a proxy server, and implement communication control for accessing the Internet via the proxy server from the in-house network.

<4> Wireless LAN access points must not be installed without the approval of the division in charge of information systems. In order to secure wireless LAN access, appropriate control such as periodical password change should be required

<5>Users shall understand Wireless LAN in the IPSM offices is basically installed just for visitors of IHI group

7.2. Security in Development and Support Processes

7.2.1. Secure Development Policy

Since it is difficult to add alterations after the business system is completed and costs also will be generated, information security must be considered from early stages such as planning and design. Therefore, the divisions responsible for information systems and the like shall implement the following in each stage of information system development.

(1) Planning stage

Required security requirements shall be defined, and security requirements shall be listed in the specifications.

(2) Design stage

Reflection of the security requirements listed in the specifications in the design specifications shall be confirmed.

(3) Implementation stage

Implementation of the security functions listed in the design specifications and functionality as requested shall be confirmed. Security function testing shall be implemented in the implementation stage.

7.2.2. System Change Control Procedures

When changes to the system are made in development or maintenance of the information system, the risk that problems in security occur and business is obstructed may occur if the changes are not proceeded with an appropriate change management procedure. Possible problems are confidentiality problem such as data leaking to unauthorized people as a result of conflict between new functions and existing functions; integrity problem such as the wrong data being processed resulting in data being corrupted; and availability problem such as certain functions not being available when an attempt is made to use them. Therefore, the divisions responsible for information systems and the like shall implement the following procedure when changing information systems.

<1> The scope, content, procedure, etc. relating to the change in configuration shall be created and reviewed by related personnel. Records of review results shall be stored for three years and be protected from tampering and unauthorized access. When expenses are generated, the suitability of the expenses shall be studied and then a budget shall be secured.

<2> When software is developed, source code shall be centrally managed and backups of all versions including old versions shall be kept. Access to the source code shall be restricted to only authorized developers.

<3> At the implementation stage, newly implemented functions shall be checked to see if they operate as requested, and other functions shall be checked to see if they operate as they have done so far.

<4> When development and maintenance are outsourced, the above security requirements shall be listed in the agreements, and their implementation status shall be confirmed. Before the outside vendor ships the information system, the vendor shall be made to run a virus check to see if all servers and PCs that make up the information system are free of any illegal programs.

7.3. Use of Cloud Services

When cloud services are used, the following points shall be complied with.

7.3.1. Application for Use

The ISM of the division that is to install cloud services (hereinafter referred to as the "installing division") shall apply for use with the IHI Information Systems Division. The IHI Information Systems Division shall check that items 7.3.3 and 7.3.4 can be complied with by the installing division, and then judge whether use of cloud services is possible or not.

7.3.2. Responsibilities on Use

The ISM of the installing division shall be responsible for the following.

(1) Remedying information security incidents/accidents in the cloud services to be used.

(2) Implementation of 7.3.3 and 7.3.4

7.3.3. Restrictions on Use

(1) Secret information beyond confidential information shall not be saved.

(2) The in-house communication line shall not be saturated.

7.3.4. Security Countermeasures

(1) The following user authentication shall be implemented.

<1> Collaboration shall be performed with the common authentication base (mechanism that enables users to be confirmed as the person in question so that cloud services are used safely) that is prepared by the IHI Information Systems Division.

<2> When collaboration with the common authentication base stipulated in the previous item is not possible, user authentication shall be reliably implemented by the installing division, and sharing of IDs and passwords and use of cloud services in their own homes shall be prevented.

(2) Upon selecting an operator who will supply cloud services, a reliable and safe operator shall be selected by referring to the "Cloud Services Usage Guidelines" created by the Information Systems Division.

(3) The content of agreement documents to conclude with the vendor who will provide cloud services shall be checked, and user obligations shall be fulfilled.

(4) Usage logs of users, operation details, dates and time, etc. shall be acquired/stored, and any symptoms of incidents shall be monitored.

8. Information Security Requirements Analysis and Specification

Among events that adversely affect availability, which is an important element of information security, the most severe event is the failure of information system related devices. Therefore, the divisions responsible for information systems and the like shall study the necessity of the following items as requirements relating to the availability of the information system, and list the results of their study in plans or specifications.

- Uninterruptible power supplies (UPS)
- Backup equipment
- Hard disk multiplexing (mirroring, RAID configuration), hot swapping (hot-line exchange)
- Redundancy of information processing facilities (power supply facilities, air conditioning facilities, key network devices)
- Method of switching (hot stand-by/cold stand-by) from the operating system to the spare system in the case of a redundant system
- Installation of a disaster recovery site

The divisions responsible for information systems and the like shall create remedy procedures for when a failure occurs and implementation instruction manuals for dealing with failures, and implement education for remedying failures for persons-in-charge of operation.

9. Business Continuity Plan

There is the possibility of risks where facilities and system devices may be destroyed by natural disasters such as earthquakes, typhoons and floods, and where an information system may be stopped by a serious accident occurring on the information system and there is no longer the prospect of recovery within a short time. In order to make it possible for operations to continue even in circumstances such as this, the divisions responsible for information systems and the like shall implement the following countermeasures.

<1> The effect on business in the event of an information system stopping shall be studied, and the following shall be implemented when it is judged that business will be affected.

<2> The allowable stoppage time of the information system shall be determined. The time having the severest demand in delivery delay to customers, etc. shall be set as the allowable stoppage time. However, when there is an alternative means when the system is down, the stoppage time that is allowed including that alternative means shall be set. The allowable stop time becomes the Recovery Time Objective (RTO) of the information system.

<3> In order for at least the mission-critical business to be able to continue, as an alternative means when the information system has stopped, a business continuation plan that describes business execution procedures by manual shall be created.

<4> Software assets and business data shall be backed up, and external storage media on which these are stored shall be stored in a safe place.

<5> An information system disaster recovery manual that describes procedures for rebuilding the information system from backed up software assets and business data shall be created.

<6> An information system recovery test shall be implemented once per year to verify whether or not the information system can be rebuilt according to the disaster recovery manual. If a malfunction is discovered as a result of the information system recovery test, backup methods and rebuilding methods shall be reviewed, and the result shall be reflected in the disaster recovery manual.

Supplementary Provisions

1. Date of enforcement: 01 December 2021

2. Approver:

....
MASATO TAMURA
Managing Director

EM MALAYSIA SDN BHD ★ IHI
861385-P

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