IHI Power System Malaysia Sdn Bhd Company Policy	
Policy No.	IPSM/POLICY/IT/2021-01
Policy Title	Information Security Implementation Rules
Effective Date	1st December 2021
Revision History	2.0

1. Purpose

These rules stipulate actual procedures for actions, etc. that should be observed by employees relating to the handling of information assets and information security to appropriately manage information assets based on "Basic Rules of Information Security for IHI Group" (GG207-01).

2. Scope

These rules apply to all those using the information assets of IHI Power System Malaysia Sdn Bhd (hereinafter referred as the "company"); including but not limited to executives, employees, and temporary workers. (hereinafter referred to as the "employees"). Information assets covered in these rules shall be all information assets handled by our company.

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

3. Related Documents

(1) GG102-01	IHI Group Information Security Policy
(2) GG105-01	Basic Rules of Risk Management for the IHI Group
(3) GG106-01	Basic Rules of Crisis Management for the IHI Group
(4) 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 handling methods.

(3) Availability

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

(4) Transmission of information

This means that the author discloses information to addressees/disclosure destinations regardless of whether or not they are inside or outside the company.

5. Information Security Policies

Information security-related basic documents, the "IHI Group Information Security Policy" (GG102-01) and "Basic Rules of Information Security for the IHI Group" (GG207-01) are stipulated as IHI group regulations. The employees must comply with these rules. The "IHI Group Information Security Policy," "Basic Rules of Information Security for the IHI Group" and procedures relating to information security are posted on the in-house web site, and are notified to the employees. The procedures relating to information security are approved by the Information Security General Manager (hereinafter referred to as the "ISGM").

The ISGM considers the necessity for reviewing procedures relating to information security when an information security incident/accident occurs that may cause serious information security-related changes or may affect operations.

6. Organization of Information Security

6.1. Information Security General Manager (ISGM)

The ISGM is the chief information security officer (CISO) in charge of information security at our company. The ISGM shall be either the MD.

6.2. Information Security Manager (ISM)

The ISM shall be the Div. manager of each division, and bears the following responsibilities relating to the information security of his/her own division.

- The ISM bears management responsibilities relating to the protection of the information assets of his/her own division.
- The ISM bears implementation responsibilities relating to information security activities of his/her own division.
- The ISM bears response responsibilities relating to information security incidents/accidents at his/her own division.

To get a supplement of the ISM, the ISM appoints an administrator (hereinafter referred to as the "ISM and the like" being together with the ISM) as necessary.

Below list ISM in IPSM by Dept. and Projects;

Department	Name	Position Title	Extension telephone number*	E-mail address
Administration	Ahmad	GM	9-160-3007	ahmad@ihi-ps.com.my
TG. Bin / Jimah	Mani Arivazhagan	Maintenance Manager	9-160-3026	ari@ihi-ps.com.my
JEP/ Manjung	D. Jayachandra	General Manager	012-2243623	jayachandra@ihi-ps.com.my
Kapar / Manjung	Azrul	Manager	9-160-3008	azrul@ihi-ps.com.my
Procurement	Nik Masri	Procurement Engineer	9-160-3014	nikmasri@ihi-ps.com.my

6.3. Information Security Representative Core Person

The ISGM appoints an information security representative core person. The information security representative core person is the point of contact with the IHI Information Security Sub-Committee Secretariat, and coordinates/promotes information security activities at our company.

6.4. Department in Charge of Information Security Internal Audits

The ISGM appoints a division in charge of information security internal audits. The division in charge of information security internal audits implements the planning, execution and follow-up coordination of information security internal audit. Information security internal audit shall be performed once per year. Also, special information security internal audit is implemented when recognized as necessary by the ISGM.

6.5. Information Security Committee

An Information Security Committee shall be established as an organization to discuss/approve important matters relating to information security at our company. The Information Security Committee is equivalent to the management review in "Basic Rules of Information Security for IHI Group."

The ISGM holds Information Security Committee meetings at least once per year. The Information Security Committee studies the necessity of review/improvement of the information security management system based on the results of the information security internal audit and implementation status of the activity plan, and issues the necessary instructions. The component members of the Information Security Subcommittee are as follows:

Committee chairman: CEO

Members: Department in charge

7. Human Resources Security

7.1. Implementation of Information Security Education

The ISM and the like shall set up an information security education plan for the fiscal year, and shall implement information security education once per year for division employees, etc. The ISM and the like shall conduct questionnaires and implement confirmation tests after implementing education to check the level of understanding of the education.

7.2. Oath (Excerpt from the Information Management Rules)

7.2.1. Oath at Recruitment

Upon the recruitment of employees, etc., the responsible personnel work divisions shall conclude a contract of employment that includes an oath to the effect that applicants shall not leak confidential information while in office and after retirement.

7.2.2. Oath at Retirement from Office

<1> When an employee, etc. retires, responsible personnel work divisions can request the employee to submit a pledge regarding the preservation of secrecy.

<2> When it is judged that non-competition obligations must be imposed on a retiring employee, etc., responsible personnel work divisions can request the employee, etc. to submit a pledge regarding non-competition based on a request from an ISM and the like.

<3> The person retiring shall return all information assets of our company, and the ISM and the like shall confirm the return.

8. Data Management (excerpt from Data Handling Guidelines)

8.1. Responsibilities for Data Management

Data governance ensures the appropriate people are involved in defining information requirements, and collectively setting data standards, data classification types, data usage and monitor integration across projects, subject areas and lines of business.

A strong data governance ensures consistent and relevant data, and by extension, competitive agility driven by sound business decision-making.

As such, it is important for IPSM to establish appropriate data management processes and to document the types of documents they have in possession. Having a data inventory allows IPSM to accurately assess existing gaps and develop strategies to improve their existing data management practices to further safeguard information and prevent unauthorized disclosure of documents and information which may impact IPSM's business operations practices.

For more information on how to manage data for IPSM, please refer to IPSM's Data Handling Guidelines.

8.2. Data Inventory

A data inventory is a record of the document which IPSM handles. It allows IPSM to assess what documents are available and in what format they exist. With a complete 360° view of all documents, organizations can determine which documents are important to their business operations accurately.

As such, the ISM and the like shall identify important information documents within their own division and list them in the data inventory template. Components present in the data inventory are:

- Document type
- Naming Convention
- Data Ownership
- Data Classification
- Asset Evaluation Value
- Risk Assessment
- Data Lifecycle

The ISM and the like shall implement a review of the data inventory at the beginning of the fiscal year.

8.3. Naming Convention

All documents identified in the data inventory shall be assigned a document ID.

A document ID is a running reference code, which uniquely identifies each document mapped out in the data inventory.

Document ID shall follow the sequence: BBB-CCCC-DDD-EEE

BBB	CCCC	DDD	EEE
Function by each division	Document Type	Data Source Type Number	List of documents at DDD level. For future use.
Function level of each division: 1. Management 2. Projects 3. Construction 4. Finance, Administration & Corporate Planning Division 5. Sales & Procurement	Classifies documents according to their context. Document Types have unique codes that consist of three alphabets describing the document category.	A number starting 001 shall be assigned to each document by type.	Extensive numbering of document type and shall be included in a separate document.

For more information on how to establish the naming convention for the documents, please refer to "Data Handling Guidelines".

8.4. Data Classification

Data classification is the foundation of an effective data governance strategy. By identifying the business value of data at the time of creation, IPSM can make intelligent, deliberate decisions on how that information is used, protected and shared.

All IPSM staff shall familiarize themselves with the data classification categories and handle them accordingly.

8.4.1. Data Classification Levels

Level	About	Disclosure	Risk of Disclosure
Restricted	• Most valuable business information • Highest class of sensitivity • Must have the tightest security and access controls	**Internal only** *IPSM, IHI and IHI Group* **External** Authorization is required	**High** Unauthorized disclosure could result in **severe financial or reputational damage** towards IPSM and its stakeholders.
Sensitive	• Access to this information should be controlled and limited to authorized personnel based on job responsibility.	**Internal only** *IPSM, IHI and IHI Group* **External** Authorization is required	**Medium** Unauthorized disclosure could result in **financial or reputational damage** towards IPSM and its stakeholders.
General Use	• Classification applies to all other information which does not clearly fit into Restricted and Sensitive.	**Internal only** *IPSM, IHI and IHI Group* **External** Authorization is required	**Low** Unauthorized disclosure is **not expected to seriously or adversely impact** towards IPSM and its stakeholders.
Public	• Classification applies to information that has been explicitly approved by IPSM, IHI, IHI Group Management for release to the public	**Public**	**No risk**

8.4.2. Labeling of Documents

- The author of information or recipient of information from outside the company shall label all documents which are classified as "Restricted" or "Sensitive". The data classification level shall be tagged on document which are created, received or transferred out of IPSM.
- For documents which fall into the Public or General Use category, it is not necessary to apply a label to these categories of information.
- If there is a mixture of different categories of information, the information will be labelled with the most stringent classification.

8.4.3. Handling Restricted Information

8.4.3.1. Roles and Responsibilities

- The author of "Restricted" information must report promptly to the ISM after the information is created.
- The author of "Restricted" information must obtain the approval of the ISM when "Restricted" information is to be transmitted.
- The author of "Restricted" information must clearly write the disclosure destination as well as the addressee in the documents to be transmitted when "Restricted" information is to be transmitted. Also, when the archiving period is determined, the archiving time also must be clearly written.
- The recipient of "Restricted" information must not disclose information to persons other than the disclosure destination.

8.4.3.2. Management

- "Restricted" information must be managed to prevent it from being touched by unauthorized persons, for example, by separating it from information in other information categories and storing it in lockable cabinets.
- "Restricted" electronic information s~~hall~~ be stored on ~~a CD-R, etc., and must not be stored~~ on a server.
- When information equivalent to "Restricted" information is received from outside the company, the recipient reports that to the ISM. When the information is to be transmitted, the approval of the ISM must be obtained.

8.4.3.3. Delivery

- "Restricted" information shall, in principle, be delivered to the other party by a method where it is handed over in person. When delivering to remote locations, "Restricted" information shall be delivered by registered mail; delivery by FAX must not be used.
- When sending "Restricted" information by e-mail, maximum precautions must be taken, such as data encryption, to prevent the information from leaking to persons other than the disclosure destination.
- When "Restricted" information is to be disclosed outside the company, the approval of the ISM of the division where the information was created must be obtained, and an appropriate agreement that includes conditions for preserving secrecy, such as non-disclosure agreement or equivalent must be concluded with the person concerned outside the company.

8.4.3.4. Disposal

- When discarding "Restricted" information, employees, etc. themselves must make that information illegible.

8.4.4. Handling Sensitive Information

8.4.4.1. Roles and Responsibilities

- The author of "Sensitive" information must report promptly to the ISM and the like after the information is created.
- The author of "Sensitive" information must obtain the approval of the ISM and the like when "Sensitive" information is to be transmitted.
- The author of "Sensitive" information must clearly write the disclosure destination as well as the addressee in documents to be transmitted when "Sensitive" information is to be transmitted. Also, when the archiving period is determined, the archiving time also must be clearly written.
- The recipient of "Sensitive" information must not disclose the information to persons other than the disclosure destination without obtaining the approval of the ISM and the like of the division from where the information is to be disclosed.

8.4.4.2. Management

- "Sensitive" information must be managed to prevent it from being easily touched by unauthorized persons, for example, by storing it in exclusive cabinets or folders set with access rights.
- When information equivalent to "Sensitive" information is received from outside the company, the recipient reports that to the ISM and the like. When the information is to be transmitted, the approval of the ISM and the like must be obtained.

8.4.4.3. Delivery

- When "Sensitive" information is to be disclosed outside the company, the approval of the ISM and the like of the division where the information was created must be obtained, and, in principle, an appropriate agreement that includes conditions for preserving secrecy, such as non-disclosure agreement or equivalent must be concluded with the person concerned outside the company.
- When in-house only information is to be disclosed to outside the company, the approval of the ISM and the like of the division to which the discloser belongs must be obtained.

8.4.4.4. Disposal

- When discarding "Sensitive" information, employees, etc. themselves or a commissioned vendor must make that information illegible.

8.5. Asset Evaluation Value

Each document should also be evaluated from the standpoint of confidentiality, integrity and availability, and list them in the information asset catalog. The table below shows the description for each component and how an asset evaluation value is determined.

Asset Evaluation Value				
Component	**Confidentiality (C)**	**Integrity (I)**	**Availability (A)**	**Asset Evaluation Value**
About	Confidentiality level is determined by data classification levels in 2.3. The lesser the sensitivity, the lower the confidentiality level.	Time required for the document to remain in the division's possession. The shorter the time period, the lower the integrity level.	The allowable time you can continue business as usual without the document with minimal disruption to business operations. The longer the allowable time period, the lower the availability level.	Process of assessing the value of the document. If the asset evaluation value is 3, guidelines to safeguard the document shall be developed.
Criteria	1: Public 2: General Use 3: Sensitive 4: Restricted	1: Low *Maintained less one year* 2: Middle *Maintained over one year* 3: High *Maintained over five years*	1: Low *Allowed a few days inaccessible* 2: Middle *Allowed one day inaccessible* 3: High *Allowed a few hours inaccessible*	Define asset value from total: 1: *Total is 5 or less* 2: *Total is 6 or 7* 3: *Total is over 8* *or Confidentiality is 4* *or Scored 3 for two components* or *Including personal data*

Policies and/or guidelines shall be developed for all documents identified with an asset evaluation value of 3.

8.6. Risk Assessment

The ISM and the like shall identify risk exposures which IPSM may face in terms of financial, regulatory, operational and reputational risks, by considering the type of consequence to the organization if the document is unintentionally disclosed.

This assessment of risk impact shall be aligned to the risk levels (i.e. No risk, low risk, medium risk and high risk) as identified in the data classification levels in 8.3.

Procedures for studying risk/analysis/countermeasures shall be implemented according to the same procedures as in the risk management plan stipulated in "IHI Group Risk Management Basic Rules" (GG105-01).

The table below shows the measurements of risk severity which can be assessed in three levels "Low", "Medium" and "High" to assist ISM and the like to measure impact level of the risk type identified.

				Effect When Risk Occurs (Impact)			
			Qualitative Expression	Minor	Slight	Sizable	Serious
			Example	Loss rate of profit plan to target ordinary profit			
				Less than 0.2%	0.2% or more and less than 5%	5% or more and less than 20%	20% or more
	Qualitative Expression	Example	Symbol	L (Low)	M (Medium)	H (High)	C (Critical)
Frequency of occurrence (Likelihood)	Rarely occurs	Possibility of occurrence within this fiscal year is low	I	Low	Low	Medium	High
	Occasionally occurs	Possibility of occurrence within this fiscal year is high	II	Low	Medium	High	High
	Often occurs	Possibility of occurrence within this fiscal year is high	III	Medium	High	High	High

The results of the risk assessment shall be listed in the Risk Management Activity Sheet, and the studied countermeasures shall be reflected in the activity plan for the fiscal year. The ISM and the like shall implement a review of the risk assessment at the beginning of the fiscal year.

8.7. Security Requirements in Outsourcing Contracts

When there is a chance that there will be contact with our company's information assets as a result of subcontracting to another company, the following content shall be listed in an agreement, and the implementation status of subcontracted services and the implementation status of security countermeasure shall be confirmed by a report or record.

<1> The contractor shall carefully handle the information assets that were disclosed from our company as Restricted, and the information assets must not be disclosed or leaked to a third party without the written consent of our company beforehand.

<2> The contractor must not use, copy, reproduce, or recycle our company's information assets for uses other than those agreed upon regardless of the format (paper media/electronic media) without the written consent of our company beforehand.

<3> When use of our company's information assets is completed by the contractor, the contractor shall return those information assets to our company or assume responsibility for discarding them him- or herself.

<4> The contractor shall, upon managing the information assets that were disclosed from our company, implement security-conscious countermeasures such as the installation of anti-virus software and the prohibition of processing/saving on privately owned information devices.

<5> The contractor is subject to the same obligations for his or her subcontractors also.

9. Physical Security

9.1. Areas Where Security Should Be Maintained

9.1.1. Physical Security Perimeter

<1> Office boundaries

Entry to offices shall be restricted by IC cards, or PIN-based locking systems.

<2> Office room boundaries

Entry to room in offices shall be restricted by IC cards, or PIN-based locking systems.

9.1.2. Physical Entry Controls

<1> When visitors enter inside office boundaries, they shall be instructed to enter via the intercom at the reception counter.

<2> When visitors enter inside room in offices, they shall be instructed to enter by employee. Also, they shall record the name, title and company in front of the door.

<3> The Admin Dept. shall store records of entered/exited locations, entered/exited buildings and entered/exited offices for three years. The Admin Dept. shall protect those records from tampering and unauthorized access.

<4> When visitors are to work inside buildings or offices, they shall be made to perform their work with an employee in attendance.

<5> When an outside vendor such as a cleaning company is to work within the site, zones that they shall enter as part of their business shall be designated, and they shall be instructed not to enter non-designated zones or not to perform work other than that they are contracted to perform.

10. Information Security Incident Management

10.1. Emergency Reporting Route

The ISM and the like shall create an emergency contact network for when an information security incident/accident occurs, and make the network known within his/her own division. When a change occurs in the content of the emergency contact network, the ISM and the like shall immediately review that change and make it known within his/her own division.

10.2. Handling Procedures for When an Information Security Incident Occurs

<1> When an information security incident such as the following occurs, or there is the possibility of it occurring, the discoverer shall notify his/her superior in accordance with the emergency contact network described in the item above.

- Leakage/loss/theft/alteration/destruction of our company's information assets
- Violation of rules relating to information security

<2> After receiving the report from the discoverer, the superior shall check the status, note down the status, and instruct the discover about on-site corrective action. The superior shall also contact the ISM in accordance with the emergency contact network.

<3> The ISM shall assess the crisis level as indicated below in accordance with "IHI Group Crisis Management Basic Rules" (GG106-01).

Crisis Level	Status/Description of Crisis
Level 4 Serious	Incident/accident where the effect on operations is extremely large or might be extremely large as a result of loss of assets/social credibility, prolonged suspension of business activities, enormous operations loss (roughly 20% or more of the target ordinary profit in the profit plan), etc. Leakage/loss/theft/tampering/destruction of large amounts of Top-Secret information
Level 3 Sizable	Incident/accident where there might be loss of assets/social credibility or where operations might be considerably affected as a result of prolonged suspension of business activities or operations loss (roughly 5% or more and less than 20% of the target ordinary profit in the profit plan) Leakage/loss/theft/tampering/destruction of Top-Secret information
Level 2 Slight	Events/cases where business operations shall be affected, even though the possibility that assets/social credibility gets damaged is low Leakage/loss/theft/tampering/destruction of Secret information
Level 1 Minor	Minor level that does not fall under levels 2 to 4 Leakage/loss/theft/tampering/destruction of in-house only information

<4> In the case of crisis level 1 or higher, the ISM shall create an emergency contact report, and contact the president, ISGM information security representative core person, and related divisions.

<5> The information security representative core person shall contact IHI responsible divisions and the Information Security Sub-Committee Secretariat.

<6> The ISM shall discuss with the president, and when the crisis level is assessed to be 3 or higher, comply with the procedure in "IHI Group Crisis Management Basic Rules" (GG106-01).

<7> The ISM shall discuss with the president, and when the crisis level is assessed to be 2 or lower, implement the following procedure.

<8> The ISM shall collect originals or copies of the information that was involved in the incident/accident. Even if originals or copies have disappeared due to theft, etc., they shall be reproduced as best as possible by conducting interviews with related personnel, etc.

<9> The ISM shall promptly set up a countermeasure's headquarters, and hold a countermeasure meeting with related divisions. At the countermeasures meeting, the required corrective measures shall be studied after discussing the necessity of a report to interested parties, emergency measures and permanent measures (reoccurrence prevention measures).

<10> The information security representative core person shall follow up until corrective actions are completed.

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.