IHI Power System Malaysia Sdn Bhd Company Policy	
Policy No.	IPSM/POLICY/IM/2022-01
Policy Title	Information Management Rules
Effective Date	1st January 2022
Revision History	1.0

1. Purpose

These rules are made for the purpose of protecting information owned by in IHI Power System Malaysia Sdn Bhd (meaning "Company A" in the "IHI Group Basic Management Regulations for Subsidiaries and Affiliated Companies" (GG110-01). The same shall apply hereinafter) and persons outside our company, for appropriate management and appropriate use of the information, by stipulating necessary matters for managing information owned by IHI and subsidiaries of IHI based on the IHI Group Information Security Policy" (GG 102-01).

2. Principles

Information created by IHI Power System Malaysia Sdn Bhd, and information obtained from persons outside our company by IHI Power System Malaysia Sdn Bhd, is, in principle, regarded as "(write a name of your company)'s internal use only," and shall not be disclosed (or transmitted or delivered, etc. The same shall apply hereinafter) outside our company.

3. Dispatch of information

"Dispatch" in these rules means disclosure of information made by its creator, regardless of whether the information is disclosed to inside or outside our company.

4. Confidentiality classification of information

All information shall be classified into one of the confidentiality classifications mentioned in the following items, depending on the extent of disclosure and importance of the information.

(1) Highly confidential : Information that must not be disclosed to anyone other than designated person(s).

(2) Confidential : Information that must not be disclosed to anyone other than designated person(s) or persons in the designated division(s).

(3) (Write a name of your company)'s internal use only
: Information that must not be disclosed to anyone outside our company.

(4) IHI Group internal use only
: Information that shall only be disclosed to IHI and subsidiaries of IHI.

(5) Disclosed information : Information that is disclosed to parties outside our company by IHI or any of subsidiaries of IHI after going through certain procedures, or information that is disclosed by person(s) outside our company.

2. In these rules, "confidential information" means information that falls under any of the items (1) to (4) in the previous clause.

6. Most important information, important information

"Most important information" and "important information" of IHI and subsidiaries of IHI are defined as follows.

(1) Most important information : Information that is related to defense, space and nuclear energy, leakage of which can endanger national security. Most important information must be classified as "highly confidential."

(2) Important information : Information whose leakage will affect an unspecified number of persons, damage trust from customers or harm competitiveness, or information that is under legal restriction. Important information must be classified as "confidential."

7. Scope of application

These rules apply to persons handling information of IHI or subsidiaries of IHI, including officers, employees and temporary employees (hereinafter referred to as an "employee, etc.").

Chapter 2 Information Management Managers and their responsibilities

8. Management system

1. Information Management General Managers and Information Management Managers are placed as a part of the information management system of IHI and subsidiaries of IHI, and a unit for placing these positions, etc. is decided in accordance with Article 7 of the" Basic Rules of Information Security for IHI Group" (CG207-01).
2. Notwithstanding the provision of the previous clause, cases falling under any of the following items require establishing a separate management system, and placing the Information Management Manager for handling the information.
   (1) When establishing a committee or project team, etc.
   (2) When handling "highly confidential" information

9. Responsibilities of Information Management General Managers and Information Management Managers

1. The Information Management General Manager is primarily responsible for information management in an organization where he/she belongs.
2. The Information Management Manager must give necessary instructions for employees, etc. to secure information and also appropriately manage information within the scope of his/her responsibility.
3. The Information Management Manager must, to the extent possible, establish "Criteria for classifying the confidentiality of information" that shows examples under which confidentiality classification information under his/her responsibility shall fall.

10. Management of disclosed information

The Information Management Manager must strictly manage disclosed information from each division in order to prevent tampering.

Chapter 3 Management of confidential information

11. Designation of confidentiality classification

1. A creator shall designate confidentiality classification into which information to be created is classified by following instructions from the Information Management Manager.
2. A creator must clarify the confidentiality classification of any information when the information is confidential.

12. Clarification of securing period

When a period during which information created by a creator shall be handled as confidential information is already decided, the creator must clarify the period as a securing period.

13. Creation of an information asset inventory

The Information Management Manager must create an information asset inventory related to the most important information and the important information, and always keep its content up to date.

14. Management of "highly confidential" information

"Highly confidential" information must be handled as shown in the following items.

(1) The information shall be separated from information that falls under other confidentiality classifications, and be managed in a way that a person without authority cannot access it.

(2) The information must not be dispatched or duplicated.

15. Disposal of "highly confidential" information

When disposing of "highly confidential" information, the person conducting the disposal must turn the confidential information into a state where restoration and decipherment of it is impossible.

16. Management of "confidential" information

"Confidential" information must be managed in a way that a person without authority cannot access it.

17. Dispatch of "confidential" information

A creator shall follow the provisions of the following items when dispatching "confidential" information.

(1) When dispatching the information to a party outside our company, permission must be obtained from the Information Management Manager.
(2) The creator must clarify to which the information is disclosed.
(3) The creator must not disclose the information to anyone other than designated person(s) and division(s).

18. Disposal of "confidential" information

When disposing "confidential" information, the person conducting the disposal must turn the confidential information into a state where restoration and decipherment of it is impossible or by outsourcing the disposal to a contractor.

Chapter 4 Acquisition of confidential information from outside our company, and disclosure of confidential information to outside our company

19. Receiving information from outside our company

1. A receiver of information from outside our company must set a confidentiality classification for the information by following the criteria set in Article 8, Item 3, and ensure that the information clearly shows the classification. Also, when the information is "highly confidential" information or "confidential" information, the receiver shall report that fact to the Information Management Manager.
2. When disclosing "confidential" information acquired from outside our company after following the provisions in the previous item, the disclosure must be made after obtaining permission of the Information Management Manager.
3. When there is a need to acquire confidential information owned by a person outside our company in order to perform work, employees, etc. must investigate and check to make sure that the party outside our company has the proper authority.

4. employees, etc. must make a proper contract that includes confidentiality provisions with the party outside our company prior to or immediately after the acquisition, in order to clarify restrictions imposed when the acquisition is made.

20. Disclosure of confidential information

1. When disclosing "confidential" information to a party outside our company, permission must be received from the Information Management Manager of its creator, or from an employee in a position equal to or higher than that of administrative employees who are designated by the Information Management Manager, and after that, in principle, an appropriate contract that includes confidentiality provisions must be made with a party outside our company to whom the information is disclosed.
2. When disclosing information that is "(write a name of your company)'s internal use only" to a party outside our company, in principle, a person who discloses the information must obtain permission from an employee in a position equal to or higher than that of administrative employees who belongs to the same division as the person disclosing the information.
3. When disclosing information that is "IHI Group internal use only" to parties outside IHI or subsidiaries of IHI, in principle, a person who discloses the information must obtain permission from an employee in a position equal to or higher than that of administrative employees who belongs to the same division as the person disclosing the information.

Chapter 5 Pledge

21. Pledge at the time of hiring

When hiring an employee, etc., responsible personnel and the human resource division shall make an employment contract with the applicant which includes a pledge that the applicant will not leak confidential information during his/her tenure in our company or after resigning from our company.

22. Pledge during one's tenure in our company

When an employee, etc. is engaged in work that requires contacting confidential information that falls under "highly confidential" or "confidential," the Information Management Manager may request the employee, etc. to submit a written pledge

stating that confidential information related to the work shall not be disclosed to anyone other than affiliated persons.

23. Pledge at the time of resigning

1. When resigning, employees, etc. shall submit a written pledge, which includes a statement that work-related confidential information that can be known to the employees, etc. during their tenure at our company will not be leaked after resigning, to responsible personnel and the human resource division by following the designated format.
2. In the case mentioned in the previous item, when it is decided that a non-competition obligation must be imposed on an employee, etc. who is resigning from our company, responsible personnel and the human resource division may request the employee, etc. to submit a written pledge about the non-competition obligation, upon the request of the Information Management Manager.

Chapter 6 Others

24. Inspection

The Administration Division and Intelligent Information Management Headquarters of IHI shall conduct a periodic inspection of the state of information management, including classification of confidential information, creation of asset inventories and maintenance of their content and access management, etc., in each division once a year.

25. Measures to take in case of violation

When employees, etc. violate these rules, responses to such violations shall be implemented as described in the following items.

(1) Penalties shall be applied to officers or employees as per the work rules of each company.

(2) Temporary employees, etc. shall be dealt with strictly as per contract with a company that has an employment relationship with such temporary employees, etc.

26. Guidelines

Among information management, classification and management of the most important information and the important information shall be made in accordance with guidelines provided separately.

27. Relationship with related rules

Matters related to confidentiality that are subject to the following rules at IHI and each subsidiary of IHI are governed by the provisions of these rules as well as each of the following rules.

(1) Rules on confidentiality related to the Ministry of Defense

(2) Rules on regulating insider trading

(3) Rules on protecting personal information

Supplementary Provisions

1. Date of enforcement: 01 January 2022

2. Approver: .....
MASATO TAMURA
Managing Director

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