**Mitsubishi Electric Automotive India Private Limited**

**IMT Manesar, Gurugram – 122 052**

**1. Purpose:**

The purpose of this document is to define and clarify policies, principles, standards, guidelines, and responsibilities related to the security of the information technology and resources.

An information security management policy is necessary to:

1. Protect safety and integrity of information.

2. Prevent unauthorized access.

3. Insure proper use of communications.

The primary objectives of Information Security are:

1. To effectively manage the risk of security exposure or compromise within the Systems
2. To communicate the responsibilities for the protection of information
3. To establish a secure processing base and a stable processing environment
4. To promote understanding and compliance with all applicable laws and Regulations
5. To protect management and preserve management's options in the event of an information asset misuse, leaks, losses, damages or unauthorized disclosure.

**2. Scope:**

These policies and guidelines apply to all resources at Mitsubishi Electric Automotive India Pvt. Ltd, hereafter referred to as MEAI. These resources consist of business information in form of non-electronic or electronic, computer systems, computer peripherals and software applications such as electronic mail, access to the Internet, word processing and data storage. These resources are the property of MEAI, access to these resources is provided for business purpose use and is subject to MEAI policies and regulations. In order for these resources to operate at a reasonable and dependable level of service, it is essential that every user exercise responsible and ethical behaviour when using them.

Since it is nearly impossible to anticipate or predict all of the various ways that current and/or future users may misuse these resources, these policies and guidelines focus on, but are not limited to, a few general rules and the principles behind them.

**3. EFFECTIVE DATE**

The revision in this policy will be effective from 30th September 2024.

**4. CONTENTS**

The contents are follows: -

**Section 1 - General Provisions**

* 1. The Role of this Policy
  2. Compliance
  3. Terms and Conditions

**Section 2 – Internal Rule Management.**

2.1 Documentation

**Section3 – Management Framework**

3.1 Organization for Internal Communication

3.2 Organization for Evaluation

3.3 Organization for External Communication

3.3.1 Information security management standards for outsourcing of tasks.

3.3.2 Non-disclosure Agreement with outsourced/Business partner.

3.3.3 Use and management of external information systems/services.

**Section 4 – Confidential Corporate Information Management**

4.1 Setting Criteria for Classifying Corporate Confidentiality

4.2 Corporate Confidentiality Classification

4.3 Handling Confidential Corporate Information

4.4 Taking materials out of offices

4.5 Handling of Public Internet Websites

**Section 5 – People Security**

5.1 Non-Disclosure Agreements with Employee

5.2 Education and training for employees

**Section 6 – Physical Security**

**6**.1 Secure Areas

6.1.1 Definition of Area level

6.1.2 Site and Room access Control

6.1.3 Physical access device management

**6.2** Protection of Devices storing confidential Corporate Information

**Section 7 – Incident/Accident Management**

7.1 Reporting Incidents/Accidents

7.1.1 Reporting criteria

7.1.2 Accident Reporting System in case of accidents

7.2 Preventive Measures

**Section 8 –Compliance**

8.1 Legal Requirement

8.2 Continual Improvement of Information Security management

8.3 Collection of Evidence

**Section 9 - Approach to Information Security in the Event of an Emergency**

**Section 10 - Revision/Amendment in Policy**

**Section 1: General Provisions**

* 1. **The Role of this Policy**

This Policy sets out the basic thinking of **Mitsubishi Electric Automotive India Private Limited** (the Company) concerning confidential information management, and describes the security management measures it has adopted from four perspectives – organizational, human, physical and technological – with a view to preventing the leakage, loss or damages of Confidential Corporate Information retained by the Company. The Policy discusses measures that have been adapted to date and will add to them as necessary in the future.

Moreover, confidential information transferred between the company and its customers, subsidiaries, affiliates and suppliers constitutes confidential information, and in addition to adopting the security management measures indicated in this Policy. Respective user/s will institute countermeasures and controls based on contracts with customers, subsidiaries, affiliates and suppliers to ensure that it is not leaked or disclosed to third parties.

* 1. **Compliance**

The Company shall manage all confidential corporate information concerning business activities appropriately in accordance with the laws of India and Company Regulations.

* 1. **Terms and Conditions**

Within this document, the definitions of “confidential corporate information” and “personal data” are set forth below. Furthermore, “personal data” that meets the definition of “confidential corporate information” must be managed as “confidential corporate information”.

**(1) Confidential Corporate Information**

"Confidential corporate information" refers to the following types of information:

(a) Personal data, or valuable technical or business information (including valuable technical or business information and know-how introduced from other organizations on the basis of a contract or the like as well as the technology, knowledge, and experience--and the accumulation thereof--required for product development, etc.)

(b) Information that if leaked to a non-pertinent party (who, whether they may be inside or outside the company, could not normally access the information), lost, damaged, or used without authorization could be detrimental to the interests of the group company and/or its stakeholders

**(2) Personal Data**

Information that pertains to an individual person and enables the identification of said individual via their name, birth date or other descriptions, or numbers, symbols or other codes, images, or audio allocated on an individual basis. (Included under this definition is the information that alone cannot be used to identify an individual but can easily be combined with other information to enable the identification of said individual.)

\* Note that employee information is also included in the scope of personal data.

**Section 2: Internal Rules Management**

**2.1 Documentation: -**

This document provides information security baseline for MEAI. Thus, MEAI establishes its information security rules or other documents in line with this policy. Enhancement of information security measures will be encouraged, according to each jurisdiction's requirement.

|  |
| --- |
| **Reference** |

Mitsubishi Electric declared the "Declaration of Confidential Corporate Information Security Management" as the Information Security Policy. Based on it, Company Rules and Regulations were established with implementing security measures overall Mitsubishi Electric.

The following is the declaration in Mitsubishi Electric.

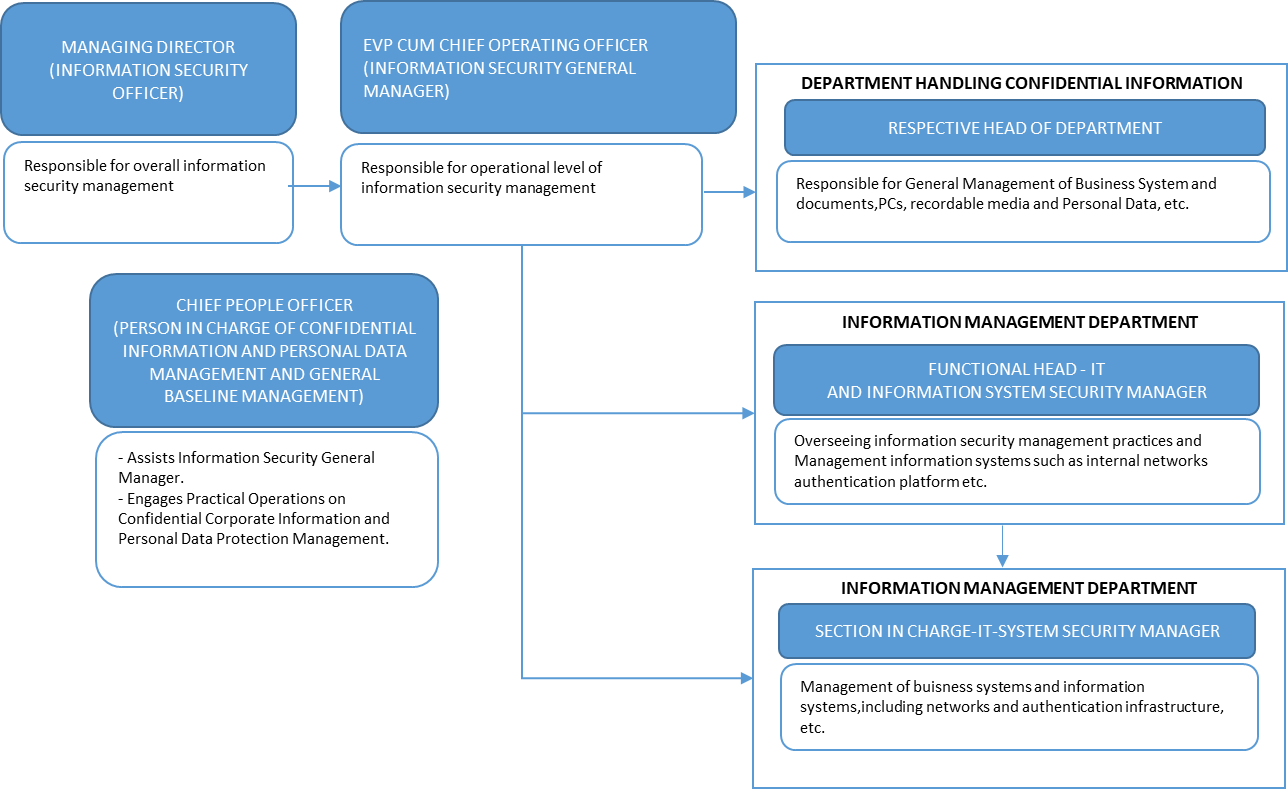
<http://www.mitsubishielectric.com/infosec/corporate.html>

**Section 3: Management Framework**

**3.1 Organization for Internal Communication**

To achieve adequate protection of confidential corporate information and personal data,

MEAI ‘s organizational Framework is given below.



**Figure 3-1: Organization Internal framework for protection of confidential corporate information and personal information**

* 1. **Organization for evaluation**

MEAI ensures that ISMS evaluation system at MEAI is independent of evaluator’s interests which evaluate the effectiveness of information security measures. A reviewer with independence will inspect and evaluate status of operation on information security measures objectively in addition of the self-inspections.

* 1. **Organization for External Communication**
     1. **Information security management standards for the outsourcing of tasks**

Where an external organization is selected to perform tasks that involve confidential corporate information, MEAI does a Non-Disclosure agreement equivalent to that concluded by a Mitsubishi Electric Group Company and also ensure that the outsourcing party implement other security measures. This is intended to prevent confidential information from being inappropriately leaked or disclosed to a third party.

Following are the rules that has to be included on selecting contractors asked to perform tasks involving confidential corporate information

[Domestic affiliates] Outsourcing conditions with regard to the contractor (who shall satisfy at least one condition):

- ISMS-certified

- P mark certified (only for outsourcing of the handling of personal data)

- If the contractor is an affiliate company, it has undergone the Mitsubishi Electric Group information security self-check program and an information security assessment by the primary management department.

- The company outsourcing tasks has judged the contractor as conforming based on the results of a self-evaluation form filled out and submitted by the contractor

\* For outsourcing of tasks involving handling of personal numbers, the contractor's business circumstances shall be confirmed is free of problems

-- [Overseas group companies] Outsourcing conditions with regard to the contractor (who shall satisfy at least one condition):

- The contractor has acquired certification for information security management relating to the entrusted tasks. (ISO 27001, PCIDSS, SOC2, etc.)

- If the contractor is a group company, it has undergone the Mitsubishi Electric Group information security self-check program and an information security assessment by the primary management department.

- The self-evaluation form (a sample is shown below for reference) included with the agreement concluded with the company outsourcing tasks shows the contractor's compliance with the required items.

- The company outsourcing tasks has judged the contractor as conforming based on the results of a self-evaluation form filled out and submitted by the contractor (a sample is shown below for reference).

The outsourcing company providing information to an external organization defines the confidential corporate information provided and specifies confidentiality classification labels so that the external organization can properly manage the information.

-- Definition and clarification of confidential corporate information

- For information on loan to the contractor by the outsourcing company, the outsourcing company specify the confidential corporate information.

- The company outsourcing tasks and the contractor shall clarify and treat confidentiality classification labels in the same manner.

The Information Security Management Standards for Contractors-

Self-Evaluation Form covers the overall status of information security management in terms of five perspectives: (1) organizational information security initiatives, (2) physical security measures, (3) operational management of information systems and communication networks, (4) status of information system access control, and (5) responses to information security incidences. Two types of forms have been prepared:

-- Information Security Management Standards for Overseas Affiliate Contractors (Including Business Partners)--Self-Evaluation Form

-- Information Security Management Standards for Domestic Affiliate Contractors (Including Business Partners)--Self-Evaluation Form

* + 1. **Non-disclosure Agreement with Outsourced/Business Partner**

Information security requirements (containing non-disclosure requirement) shall be included in written contract or others, which is exchanged at the time of outsourcing of business operations.

All confidential corporate information gained from customers, Group companies and business partners is the confidential corporate information of each respective company. In addition to safety management measures to prevent any inappropriate leaks or disclosures to third parties, it is also critical that measures and management are implemented based on agreements with customers, group companies, and business partners.

MEAI will stipulate security requirements to counterparties in contractual documents in cases where MEAI is sharing any confidential data with suppliers, vendors, consultants etc. i.e. commercial, financial, legal, marketing, business and technical or other information, including, but not limited to, specifications, algorithms, calculations, formulae, processes, business methods, diagrams, drawings etc. In these cases, along with NDA (Annexure 7), **Annexure 4 (General Baseline)** will be filled by the suppliers, vendors, and consultants. If any of suppliers, vendors, consultants etc. has acquired information security management certification related to the entrustment (ISO27001, PCIDSS, SOC2, etc.\*), then the **Annexure 4 (General Baseline)** is not required to be filled. To manage the names and evaluation results of all subcontractors **Annexure 5 (General Baseline),** Subcontractor Management List will be maintained.

Furthermore, security management situation of counterparties will be regularly reviewed in writing in accordance with the contract. If treating important information, on site audit activities shall be considered. When outsourcing activities that involve the handling of confidential corporate information, the contract shall also specify the following matters:

* A definition of the information to be protected
* Expected duration of the contract
* Disposal/return of provided confidential corporate information
* Expected actions to be taken in case of a breach of this contract
* Outsourcing to subcontractors
* Subcontractors’ obligations of confidentiality\*1

\*1 Definition of “confidential information” in the non-disclosure agreement (NDA) determines the scope of information to be confident. For example, in the case of outsourcing cleaning or security where an employee of the contractor works in our office or site, we should properly define the “confidential information” as “Any information which the employee has obtained in the work,” if we want information which the employee sees or hears in our office or site to be in the scope of NDA. Moreover, we can have the case where the contractor outsources our cleaning or security to a subcontractor and an employee of the subcontractor sees or hears our confidential information in our office or site.

In cases where a business partner/contractor outsources to a subcontractor, to prevent the subcontractor from triggering an incident related to confidential information, the following wording shall be specified in the contract with the business partner, as it is necessary for the business partner to ensure the subcontractor is placed under obligations of confidentiality.

“In the event the business partner/contractor outsources all or a portion of these business operations to a third party, the business partner/contractor shall oblige said third party to have the same obligations of confidentiality as the business partner/contractor owe to the Company. And the business partner/contractor shall be responsible for the actions of said third party”

* Also, when receiving disclosure of confidential information from a business partner, and when entering into a non-disclosure agreement, caution should be taken so that excess obligations are not imposed on one’s company. Implement management with a sufficient understanding of contract details to avoid a breach of contract when carrying out management\*2.
* \*2 Regardless of whether the confidential information was legitimately received from a third party, the illegal use of said information will subject the company to an injunction and damage claims under the Unfair Competition Prevention Act. As such, should said information be used for purposes that differ from its initial purpose, the terms and conditions of the contract should be confirmed by the manager of the information owner division (Respective FH). The manager of the information owner (Respective FH) division shall routinely confirm the status of compliance with the terms and conditions of contracts.

Furthermore, the necessity of the following matters should be considered:

- Scope of Responsibility within MEAIand at the partner organisation.

- Instruction in outsourcing Personal data Handling

- Security measures for asset protection

- Education and training to who will handle confidential information

- Change personnel who will handle confidential information

- Access Control policies

- Service level agreement

- Monitoring

- Protection of Intellectual Property Rights

- Review and cancellation of the contract

- Incident response procedure

Note that Outsourcing of IT operation management and using cloud computing environment or SaaS are "Technical Security Control Measure".

-When allowing an outsourcer to access Mitsubishi Electric confidential corporate information, consider measures to reduce security risks (limit access, identify persons with access privileges, outline access procedures, conduct monitoring, etc.), and conclude an agreement with the outsourcer.

-For products and services provided by the outsourcer, confirm that the outsourcer has evaluated security risks for all relevant elements (including secondary subcontractors, purchased products, etc.) and has taken appropriate measures.

-Regularly monitor, review, evaluate, and manage changes in the information security activities and services of outsourcers, etc.

* + 1. **Use and management of external information systems/services.**

MEAI ensures appropriate use and management of external information systems and services in the corporate activities and maintain the records of the same. There are two types of information systems which are defined as below: -

1. Internal Information System: - Items that are managed and operated by MEAI which includes

* where information system manufacturing, development, and operation work is outsourced.
* where cloud services, etc. are used to construct the information system environment.

1. External information system (service): - Items that are not managed or operated by MEAI which are those where the Company does not have decision-making or supervisory rights regarding the management and operation of information systems (services). It further defined as:-

* Information systems managed and operated by business partners, affiliated companies, etc.
* Cloud services (SaaS, PaaS, IaaS)
* Services provided to unspecified people
* File exchange/sharing services, translation services, SNS, etc.

Following are the usage management of external information systems: -

1. Matters to be managed

When using the service, the following items should be managed.

* Manager of handling information
* System/service name
* System/service provider
* Usage department
* Purpose of use
* Management location
* In particular, when using information systems (services), the person in charge of security, etc. should be made clear.

1. Management methods and procedures

The information systems department will create and manage a list of systems (services) used based on communications from the usage departments as Annexure-6. In addition, the list will be maintained in an appropriate manner through periodic (once a year) stocktaking by the user department.

**Section 4: Confidential Corporate Information Management**

**4.1 Setting Criteria for Classifying Corporate Confidentiality**

Mitsubishi Electric classifies Confidential corporate information based on the level of impact in the event of information leak.

Designating confidential corporate information and the media used to store said information as subject to management, and then deciding handling and storage methods based on the importance of said information is an appropriate and effective way to protect the assets of each company.. In light of this, these classifications are implemented in line with the current conditions at the respective companies and countries. The handling and storage methods should be documented and incorporated into workflow procedures. Important information especially shall be protected so that no serious loss or harm is incurred from a cyberattack.

The classification of confidential information received in a disclosure by a third party shall conform to the terms of the contract with said third party.

Furthermore, designate an appropriate classification for the following as information that, if leaked, lost or damaged, could cause the company to incur severe losses or disadvantages (for Mitsubishi Electric, this is the equivalent of “Secret” or higher)- Information for which no confidentiality classification has been stipulated in a contract or agreement(information that if leaked, lost, or damaged, a report to a third party would be required.)- Information classified as sensitive information for security reasons (any leak overseas would infringe on the Foreign Exchange and Foreign Trade Act)

That said, as long as an agreement has been reached with the third party that possesses the disclosure rights for said information, it is acceptable to designate said information with a classification equivalent to that for information that is below the level of being deemed as inappropriate for disclosure outside the company (Mitsubishi Electric classifies this as “Confidential” or below).

The corporate confidentiality classification of confidential corporate information may change as time elapses or due to other factors (ex. product information before and after a press release). As such, regularly confirm that the corporate confidentiality classification of assets is appropriate

**Table 4-1 outlines the definitions for “Top Secret,” “Secret,” and “Confidential” as stipulated by Mitsubishi Electric.**

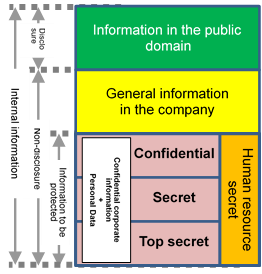
Personnel-related secrets are called personnel secret. They are classified into personnel confidential, personnel secret or personnel top secret according to the impact level.

It classifies confidential corporate information based on the level of business impact in the event information is leaked, lost, or damaged. From the perspective of confidential corporate information, a summary of internal information is as shown in Table 4-1.

**Table 4-1 Corporate Confidentiality Classification definitions**

|  |  |  |
| --- | --- | --- |
| **Confidential Corporate Information Levels** | **Definition** | **Example** |
| **Top Secret** | Refers to Information concerning the core of management that, if leaked, lost or damaged, would cause extremely serious loss or disadvantage to the Company or could do so. This further refers to the confidential corporate information deemed by the manager of the owner division to have a level of confidentiality such that, in addition to external parties, disclosure to internal parties not directly relevant to said information is prohibited. | M&A information, personnel matters relating to executive officers, etc. |
| **Secret** | Confidential Corporate Information that is not "Top Secret" but whose leakage to third parties would cause serious loss or disadvantage to the Company or could do so.  Furthermore, with the respect of disclosing, the manager of the information owner division shall clearly decide not revealing outside of the company but also internal personnel other than concerned parties. | Business strategies, PL forecast, personal data, etc. |
| **Confidential** | Confidential Corporate Information other than "Top Secret" or "Secret" information.  Furthermore, with the respect of disclosing, the manager of the information owner division shall clearly decide not revealing outside of the company. | Company Regulations,  Research reports, order  plans, operating data, Design data, etc |

* **Internal Information**



**Figure 4-1: Internal information**

**4.2 Corporate Confidentiality Classification**

Confidential corporate information shall be classified based on the criteria of Corporate Confidentiality Classification of Asset.

At the very least, identify the corporate confidentiality classification on the cover page (first page of document) of confidential corporate information.

**4.3 Handling Confidential Corporate Information**

It determines the procedure for the disclosure, storage, reproduction, disposal, transmission, or taking out confidential corporate information and ensure appropriate management.

To prevent confidential corporate information and personal information from unauthorized disclosure, alteration and deletion, the establishment of proper handling procedures to protect confidential corporate information from unauthorized leaks, loss, or damage is important. Furthermore, existing risks in each stage shall be recognized and necessary countermeasures shall be taken against such risks.

For trade secrets to receive legal protection under India’ cyber security Law, it is not enough for a business entity to merely think subjectively in terms of trade secrets. Additionally, the following considerations are required:

(1) Information shall be managed as necessary to maintain confidentiality (access controls)

(2) The person accessing information shall objectively recognize that it is confidential (possibility of objective recognition)

In other words, there are specific judgement factors. Above (1) depends on the existence of locks or other security hardware, whether passwords are set, etc.; and (2) depends on whether the information is distinguished from other general information, and the existence of indicators to the effect that the information is secret.

At least, the following measures shall be conducted to any confidential information received from Mitsubishi Electric.

(1) Indication of corporate confidentiality classification

- The corporate confidentiality classification shall be clearly indicated on the cover page (or first page of document)

(2) Conclusion of an agreement for accessing confidential corporate information

- A person in charge of contract shall properly conclude an agreement with an employee who access confidential corporate information on items to be complied with in writing.

- Person in charge of confidential corporate information and personal data protection management (PIC of CPM) shall confirm the above conclusion. The conclusion can be substituted by Non-disclosure Agreement with an employee.

(3) Taking materials out of the office

- When any material is to be taken out of the office, the immediate manager shall be authorized it, in advance. Such information shall be minimized.

- Especially when any confidential corporate information is to be taken out of the office using a recording device or sent to external parties, use an encryption tool(\*), etc., to implement measures against information leakage, loss, or damage.

(\*) Set company standards for encryption tools. When using an encryption key, stipulate the handling of the encryption key. When encrypting and taking overseas, make sure to adhere to the laws and rules of the relevant country or region.

- If using a file sharing service, etc. to disclose confidential corporate information to another company, stipulate rules for use. In particular, implement measures to ensure the immediate deletion or restriction of access upon expiration of the disclosure period. If removing personal data or other sensitive information, confirm the necessity of removal, consider anonymization or pseudonymization, and limit removal to the minimum information necessary.

(4) Storage

- In principle, all confidential levels of documents, CD-ROMs or other materials shall be stored in storage spaces such as cabinets. In particular, access to confidential corporate information that will or could potentially cause significant losses or be significantly detrimental to the company should it be leaked, lost or damaged (in Mitsubishi Electric’s case, “Secret” or “Top Secret”), should be denied to anyone that is not a related party, such as by storing said information under lock and key.

- In particular, in the case of electronic information that will or could potentially cause significant losses or be significantly detrimental to the company should it be leaked, lost, or damaged (in Mitsubishi Electric’s case, “Secret” or “Top Secret”)and would require reporting to customers, store centralized on a server and set individual and department-specific access privileges for server folders. In addition to the above, strict security management measures should be put in place for protection (in Mitsubishi Electric’s case, in principle the information is encrypted).

- To enable the immediate implementation of an impact analysis in the event of a cyberattack or infiltration, manage storage locations so that it is clear what confidential corporate information is stored on the server and where on the server it is stored(Mitsubishi Electric assigns a confidentiality classification to each filename and folder name, and personal data is affixed with a label indicating that the information is personal data).- To prevent information from be becoming in accessible due to future changes in technology, establish procedures for ensuring data accessibility(readability of media and file format)throughout the storage period. Also, stipulate procedures for the storage and handling of record shaving given consideration to the possibility of media deterioration.

(5) Logging

- For important information, special care for leakage or unauthorized usage, access logs for such information shall be acquired and reviewed regularly check for such inappropriate use.

(6) Disposal

- A decision shall be made on the necessity to store confidential corporate information that has exceeded the confidential classification period and said information shall be disposed of or deleted if it is deemed unnecessary. Should the storage of said information be deemed necessary, a confidential classification period shall be newly instituted.

- In the case of the disposal paper documents, and other such materials, they shall be disposed of in an appropriate manner, including shredding, incinerating, dissolving or some other method that will leave no trace of the document. The disposal of recording/storage mediums shall constitute the complete deletion of data or the physical destruction of the medium.

- Confidential corporate information that is unnecessary and is stored as electronic information on a computer, including any such information contained in the trash, on the desktop, or in downloaded folders, shall be routinely deleted.

- When disposing of recordable media or devices containing recordable media, make sure that the data is deleted.

- In cases where the disposal of confidential corporate information is outsourced to a third party, a non-disclosure agreement shall be entered into with the third party and proof of disposal or some other confirmation of disposal shall be obtained from the third party upon completion of disposal.

MEAI defines handling procedures of information provided as (1) Paper materials and (2) Electric document files as follows.

**Table 4-2: Handling of paper documents**

| Type | Action | | Implementation Summary | Corporate Confidentiality Classification | | |
| --- | --- | --- | --- | --- | --- | --- |
| Top Secret | Secret | Confidential |
| Paper Documents | Designation of confidentiality classification\*1 | | Indication of corporate confidentiality classification, corporate confidentiality valid term, owner’s name, disclosure target, etc.  (The corporate confidentiality classification shall be indicated in each document.) | “Top Secret” shall be indicated on cover page. Other attributes (corporate confidentiality valid term, owners’ name and disclosure target) shall also be specified. | “Secret” shall be indicated on cover page. Other attributes (corporate confidentiality valid term, owners’ name and disclosure target) shall also be specified. | “Confidential” shall be indicated on cover page. Other attributes (corporate confidentiality valid term and owners’ name) shall also be specified. |
| Copy\*4 | | Rules on copying  documents | Copying documents and other materials shall be strictly prohibited when the use of said materials is not within the parameters of disclosure specified by the manager of the information owner division. | | |
|  | Scope of disclosure designation\*5 | Internal disclosure | Define scope of disclosure | Designated internal individuals only whom the manager of owner division has already authorized. | Designated internal individuals or divisions that the manager of owner division already authorized. | Widely disclosed within the company without designating disclosure scope\*6 |
| External disclosure | Prior approval of disclosing department manager and NDA | (1) When disclosing confidential corporate information is required, the manager of the information owner division shall be noticed and authorize it, in advance. Intellectual property or other assets, which are defined treatment procedures (especially for disclosure), shall be treated appropriately, according to the procedure.  (2) When confidential corporate information is to be disclosed to a third party, a contract concerning non-disclosure shall be conducted with the party\*7. | | |
| Taking documents out of the office | | Precautions for taking documents out of the Company\*8 | When a document is to be taken out of the offices, limit the confidential corporate information to be removed to the bare minimum and the immediate manager shall authorize it according to the designated procedure. | | |
| Storage | | Storage management of confidential corporate materials | In principle, store in cabinet, etc., and ensure that materials classified as “Secret” or higher are managed in locked storage. | | |
| Disposal | | Disposal of confidential corporate information no longer required | (1) For confidential corporate information for which the confidentiality valid term has expired, review whether they need to be stored or not. If not, they shall be disposed of If they are necessary to be kept, their "corporate confidentiality valid term " shall be re-assigned.  (2) When a document becomes unnecessary, it shall be disposed of through shredding, burning, dissolving or other appropriate method that leaves no trace.  (3) When disposal of confidential corporate information documents is to be outsourced, conclude a non-disclosure agreement in advance and obtain a certificate of disposal. | | |

**Table 4-3: Handling of Electronic information**

| Type | Action | | Implementation Summary | Corporate Confidentiality Classification | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Top Secret | Secret | | Confidential |
| Electric document files | Designation of corporate confidentiality classification \*1 | | Indication of corporate confidentiality classification\*2, corporate confidentiality valid term \*3, owner's name, disclosure target, etc.  (The corporate confidentiality classification shall be indicated in each document.) | "Top Secret" shall be indicated on cover page. Other attributes (corporate confidentiality valid term, owners' name and disclosure target) shall also be specified.\*3 | "Secret" shall be indicated on cover page. Other attributes (corporate confidentiality valid term, owners' name and disclosure target) shall also be specified\*3. | | "Confidential" shall be indicated on cover page. Other attributes (corporate confidentiality valid term and owners' name) shall also be specified\*3. |
| Copy\*3 | | Rules on copying files | Copying documents and other materials shall be strictly prohibited when the use of said materials is not within the parameters of disclosure specified by the manager of the information owner division. | | | |
| Scope of disclosure designation\*5 | Internal disclosure | Define scope of disclosure | Designated internal individuals only whom the manager of owner division already authorized. | Designated internal individuals or divisions that the manager of owner division already authorized. | | Widely disclosed within the company without designating disclosure scope\*8. |
| External disclosure | Prior approval of disclosing department manager and NDA | (1) When disclosing confidential corporate information is required, the manager of information owner division shall be noticed and authorize it, in advance. Intellectual property or other assets, which are defined treatment procedures (especially for disclosure), shall be treated appropriately, according to the procedure.  (2) When confidential corporate information is to be disclosed to a third party, a contract concerning non-disclosure shall be conducted with the party.\*7 | | | |
|  | Taking out of the company | | Caution when taking outside the company | To prevent confidential corporate information leakage, loss, or damage, remove only the bare minimum information and obtain approval from the immediate manager in advance via prescribed procedures. | | | |
|  | Transmissions | Transmissions within the Company | Transmit within the scope of disclosure | In principle, any "Top Secret" file should not be transmitted by e-mail. However, if the manager of the disclosing division approves it, then create an email attachment, encrypt that attachment, and send via a method that leaves an electronic record of approval from the direct supervisor (electronic workflow, etc.) | | Inside the company, file transmission shall be conducted with confined scope which has been authorized by the manager of information owner division.  Personal data shall be encrypted in transmission. | |
| Transmissions outside the Company | Prior approval of disclosing department manager and NDA | Data should be encrypted.  Encrypt data before sending. However, if security is being maintained through the use of a dedicated line or equivalent line (Mitsubishi Electric Group intranet, etc.), then normal transmission is allowed. (Encrypt if containing personal data.) | |
| Send via a method that leaves an electronic record of approval from the direct supervisor. |  |
| Storage  (on Servers) | | Electronic files stored in server with access controls. | In principle, encrypt and store centralized on a server with individual access right management for each folder. | In principle, centralized storage at server shall be conducted. Set access privileges for each individual / folder.\*9 | | Centralized storage at server shall be conducted. Set access privileges for server folders for each individual / division |
|  | Disposal | | Disposal of confidential corporate information no longer required | For confidential corporate information documents for which the confidentiality valid term has expired, review whether they need to be stored or not. If not, they shall be deleted. If they are necessary to be kept, their "corporate confidentiality valid term " shall be re-assigned.  Routinely delete all unnecessary files on your computer.\*11 | | | |
| e-Mail | Designation of confidentiality classification | | Confidentiality classification on e-mail\*10 | Indicate "Top Secret" at the top left of the text body or in the subject line | | Indicate "Secret" at the top left of the text body or in the subject line | Indicate "Confidential" at the top left of the text body or in the subject line |
| Transmissions of e-mail with attachments within the Company | | | Same as internal transmission of electronic documents. | | | |
| Transmissions of e-mail with attachments outside the Company | | | Same as internal transmission of electronic documents. | | | |
| FAX | FAX messages | | Confirm recipient | When sending confidential corporate information by FAX, check the number carefully prior to sending. Furthermore, confirm the destination person to receive it or not, in principle. | | | |
| Recording device (DVD, USB memory sticks, etc.) | Designation of confidentiality classification | | Indicate the corporate confidentiality classification on each device | Indicate "Top Secret" on each device | | Indicate "Secret" on each device | Indicate "Confidential" on each device |
| Storage | | Store these devices securely | In principle, materials shall be stored in storage spaces such as cabinet and devices classified as “Secret" or higher shall be kept under lock and key. | | | |
| Taking devices out of the company | | Precautions prior to taking devices out of the Company | To prevent confidential information leakage, loss, or damage, information to be taken out shall be minimized. Follow prescribed procedures and obtain approval from your immediate supervisor.  When taking devices out of the company, implement measures to prevent information leaks, including using encryption tools to encrypt confidential corporate information. | | | |
| Disposal | | Disposal methods and precautions | (1) For confidential corporate information for which the confidentiality valid term has expired, review whether they need to be stored or not. If not, they shall be disposed of If they are necessary to be kept, their "corporate confidentiality valid term " shall be re-assigned.  (2) When disposing of storage media, data shall be completely deleted or the device shall be physically destroyed.  (3) When disposal of confidential corporate information documents is to be outsourced, conclude a non-disclosure agreement in advance and obtain a certificate of disposal | | | |

Note:

1. Designation of confidentiality classification

"Designation" refers to clarifying that a document is confidential corporate information, such as by clearly indicating the confidentiality classification as "Top Secret," "Secret," or "Confidential" on the document cover. As necessary, detailed subject names for confidential documents and information requiring confidentiality classifications shall be stipulated in relevant company regulations as necessary. Note 1Individual and specific confidentiality designations are determined by the manager of the information owner division.

1. Indication of confidentiality classification

The confidentiality classification shall be displayed as a measure to satisfy the objective recognizability required by the Unfair Competition Prevention Act.

1. Regarding electronic data, in order to quickly understand the increase in damage caused by cyber attacks, the confidentiality classification will be displayed not only on the cover page but also on the file and folder names\*. Regarding folders, if the security level is displayed in the top folder of the folder that actually contains confidential corporate files, there is no need to display the security level in lower folders. Files that correspond to personal data assets are displayed in the file name so that it can be seen that they are personal data assets. Example) File name: SECRET\_XXXXX.docx,SECRET\_Personal\_XXXXX.docx,Folder name: //SECRET\_YYYYY/ZZZZ.

Further, the security level displayed in a lower folder cannot display a higher level of security than the security level of the upper folder in which the security level is displayed. In addition, files with higher level of confidentiality cannot be stored in the lower folder. Note that if folder/file names are restricted for business reasons or if operations are affected, the confidentiality classification and personal data may be excluded from display.

1. Applies when the email body itself contains information commensurate with the confidentiality classification. It is not mandatory to write in the subject line, as indicated in the upper left corner of the text or in the subject line, but if you wish to write in the subject line, where space is limited, only the confidentiality classification may be sufficient. In this case, if it is necessary to state the scope of disclosure, etc., it may be stated clearly in the text.
2. For paper documents, if the security level is indicated on the cover, it is not mandatory to display the security level on the file of the paper document containing the relevant information. Regarding assets from the past, if there is a confidentiality classification indicated on the paper document file or server folder, the information contained therein can be considered to fall under the definition of confidential corporate information, then each piece of information must indicate a confidentiality classification. However, it is desirable to display the confidentiality classification on each cover, and when extracting and using some information from a file or folder, be sure to display the confidentiality classification.\*The requirement to display the confidentiality classification in file names is only applied when changing existing measures or when creating or modifying a new file, and does not apply immediately to all existing documents. The security level should be displayed in the folder name only for the top-level folder where the security level should be displayed as soon as possible.

2) Confidentiality valid term’

The confidentiality period can be specified as “until contract expiration”, “until public relations announcement from XX month, XX day, XX time”, “until designation cancellation notice”, “3 years”, etc. Note 3 Unless otherwise specified, the following shall apply

.a. "Top Secret": 2 years

b. "Secret": 1 year

c. "Confidential": 5 years

When the confidentiality period has expired, it is determined whether or not storage or retention is necessary, and the information is promptly deleted, or the confidentiality classification and confidentiality period are reset as necessary. The confidentiality classification will continue until it is reviewed. Review it when you realize that it has expired.

Be sure to specify the specific confidentiality period for information obtained from outside the company. Regarding the handling of confidential corporate information whose confidentiality valid term has expired in the department receiving disclosure, if the information is no longer needed, it should be destroyed taking care to prevent information from leaking, being lost, or being damaged. If necessary, the principle is to contact the information owner division. If inquiries cannot be made to the information owner division due to reorganization, etc., the information will be further managed as the information of the disclosed department.

(2) Reproduction

1) The scope of disclosure of confidential corporate information is determined in advance, and copying for purposes outside the scope of disclosure is prohibited. If there is a need for reproduction for the purpose of use outside the scope of disclosure for business reasons, please follow Article 15 of Company Regulations 1307 (Disclosure for Business).

2) Even if it is communicated to related parties that is permitted by “clarification of the scope of disclosure,” copying should never be done easily, and only the necessary parts should be communicated verbally at meetings, etc., or only those who have access should be limited, measures such as managing it as a common file must be taken.

3) If the head of the information owner division knows in advance that it will be necessary for the department receiving disclosure to copy confidential corporate documents, etc., and recognizes the necessity, the head of the information owner division must notify the recipient in advance that the copying is permitted, or notify the document in advance. (e.g., ``Copying of this document is permitted only for the minimum number of relevant persons necessary.'') When making copies with the permission of the information owner division head, the information owner division head makes copies after clarifying the responsibility for reproduction management by clearly indicating the approver's approval date, job title, and name on confidential corporate documents, etc. All possible measures must be taken to manage the documents, including disposal.

(3) Scope of disclosure designation

1) Designating the scope of disclosure for "Top Secret" and "Secret" means deciding to which department head the information will be disclosed, and if it is a document, it is usually indicated in the address.

2) Also, if necessary, specify the range of information to be communicated from the head of the department to be disclosed, such as “only your position,” “directly related parties only,” “GM only,” “managers only,” etc. However, when copying confidential documents, etc., permission is required from the head of the information owner division.

3) If the information owner division head does not specify the scope of disclosure within the disclosed department, it is the responsibility of the disclosed department head to disclose (transmit) the information to the minimum necessary range to the minimum number of subordinates necessary for business to be carried out. Regarding copying, same as above.

4) If the scope of disclosure is not specified, the scope of disclosure shall be deemed to be within the information owner division.

5) The scope of disclosure of "confidential" information is, by definition, Mitsubishi Electric, so it is not required to designate the scope of disclosure, but if disclosure is to the Mitsubishi Electric Group or a specific other company, the recipient should be specified.

For example, when disclosing to the Mitsubishi Electric Group: “Scope of disclosure: Mitsubishi Electric Group” When disclosing to specific other companies: “Scope of disclosure: Includes XX company” added. Note that the above is just an example and does not require this exact notation.

6) When disclosing confidential corporate information to a third party, conclude a Non-disclosure agreement with the third party. However, a non-disclosure agreement is not necessarily required with a person who is legally or under an equivalent system (\*) obligated to maintain confidentiality regarding information obtained in the course of their profession, such as a lawyer or certified public accountant.

\*Example: When an organization of nationally qualified persons has the disciplinary power to suspend or revoke the nationally qualified person's national qualification due to the leakage, loss, or damage of confidential corporate information learned in the course of one's work). When disclosing business secrets to a third party, conclude a Non-disclosure agreement with the third party. If possible, conclude a Non-disclosure agreement with a licensed business worker such as a delivery company. However, if confidentiality can be confirmed through the terms and conditions, it is not necessary to require a contract.

(4) Taking outside the company

1) Taking outside the company refers to physically taking confidential corporate information out of the office. Prescribed procedures are required for taking things outside the company, but if the risk of losing confidential corporate information outside the company, such as taking them to an adjacent business office across the street, or leaving the company only when crossing the road, is minor, then the prescribed procedures may be omitted.

2) Prescribed procedures basically mean using the "Corporate Confidential/Personal Information Removal Management Workflow."

3) There is no need to apply to remove cache information that remains on the PC. Cached information may contain confidential corporate information, but it is stored without the person who brought it being aware of it, it is not easy to identify what kind of information is cached information, and security management measures such as encryption are used to protect the information. Even if lost, there is no risk of leakage, loss, or damage, so it will not be subject to an application for removal. Please note that confidential corporate information that are intentionally taken out by the person concerned are subject to an application for removal.

4) Smartphones managed by terminal management tools were subject to management of trade secrets and personal data because their cache contains trade secrets, but there is no possibility of trade secrets being leaked, lost, or damaged from the corporate domain; Since the owner cannot control the cache, no application is required to take it out. However, if you intend to take out business secrets, you will need to apply for the removal of the confidential information.

5) It is not mandatory to wear a strap for mobile phones/smartphones. It is difficult to require that people wear a strap and keep phones on their body 24 hours a day, so consider thorough follow-up safety management measures will prevent the leakage, loss, or damage of confidential corporate information. Please note that this does not preclude requests for straps to be worn at BA/headquarters/locations for material management reasons. Please note that you must wear a strap when using USB memory.

6) It is prohibited to store or take out confidential corporate information on personally owned devices, but some exceptions may be made for storage or removal of using personally owned smartphones (BYOD smartphones, BYOD: Bring Your Own Device) managed using MDM designated by the company. Allowed in exceptional cases. Use it appropriately according to the company's instructions.

7) Downloading confidential corporate information during remote work may not require an application for removal, assuming that it will be deleted after the work is completed.

(5) Transmission

Transmission outside the company refers to all disclosures of confidential corporate information outside the company, such as email attachments, information sharing via shared sites, and information input to Internet sites.

1) Sending by email attachment

- When sending confidential company information as an attachment to an email, encrypt it before sending. However, if security can be maintained by using a dedicated line or equivalent line (MELIT network, etc.), unencrypted text is accept able (personal data must be encrypted).

- Use company standards for encryption software. Establish an encryption usage policy, manage passwords, and store records so that they can be decrypted during valid terms. Also, when encrypting and transporting data overseas, comply with the laws and regulations of the relevant country or region.

- Information that is classified as "Secret" or higher will be sent using a method that allows the supervisor's approval procedure to remain electronically (such as Kumon Workflow). However, this does not apply if separate operational rules are established and applied based on the contract, etc. concluded with the destination. For example, if a development project involves employees of affiliated companies, it is possible to define the scope of disclosure in the project charter or project plan.

2) Information sharing through sharing sites

When using an internal/external file sharing service to share confidential corporate information with an external party, receive prior approval from the information owner division. Keep external disclosure recipients to the minimum necessary, and make sure to confirm disclosure recipients and disclosure period settings. Note 15

3) Inputting information to the internet site

In principle, entering confidential company information into Internet sites (search sites, translation sites, chat-style automatic conversation programs (e.g. ChatGPT)), etc. is prohibited. For Internet cloud services that are operated and managed within the Group and whose users are limited to the Group, the handling of c confidential corporate information may be decided with the site administrator and information disclosure department if the following conditions are met:

a. Input information will not be disclosed outside of the specified scope of disclosure.

- Use settings that a vendor cannot obtain via an opt-out request.

- Entered information will not be saved on the cloud.

b. System users should not enter "personal data" or "top secret" data.

c. Do not use input information for data learning.

d. Define the confidentiality classification of the generated results and manage them based on that confidentiality classification.

- If "secret" is input, the generated result will be "secret" in principle. However, depending on the processing method, etc., it may become "confidential".

e. Appoint a system administrator and operate the system appropriately.

- Keep usage history

- Monitoring for unauthorized access, etc.

- Manage users

f. Comply with other regulations such as export control, information systems (including cloud usage standards, etc.), and intellectual property rights.

g. When entering "Secret", do the following. (Excluding cases of "confidential")

- Obtain permission from the head of the information owner division, and do not disclose it outside the scope of disclosure.

Encrypt the communication path and encrypt the storage area (excluding temporary storage)

(6) Storage

Servers that store confidential corporate information must comply with the requirements (access rights settings, trail management, etc.)" Do not store files with a high security level in folders with a low security level.

Electronic data that is classified as “Secret” or higher will be encrypted and stored. This excludes cases where encrypting information such as information incorporated into a business system would make it impossible to perform the business. To prevent cases of failing to apply encryption, if a folder has an automatic encryption function, it is recommended to use it (this general storage enhancement measure replaces the important information protection measures developed as a countermeasure against cyberattacks).

Furthermore, when personal data classified as "Secret" or higher is retrieved from the storage location, it must be encrypted using a cryptographic code with usage rights. Supervisors regularly check access records.

To prevent information from be becoming inaccessible due to future changes in technology, establish procedures for ensuring data accessibility (readability of media and file format) throughout the storage period. Also, stipulate procedures for the storage and handling of records having given consideration to the possibility of media deterioration.

(7) Disposal

1) Documents whose confidentiality designation has been cancelled as a result of reviewing the confidentiality period shall be disposed of using the methods listed in the "Disposal" column of Tables 4-2 and 4-3, or managed as general documents.

2) Regularly delete unnecessary files from the trash can, desktop, download folder, etc. on your PC. The purpose is to prevent the possibility that unnecessary files may have been stolen in the event of infection with malware.

**4.4 Taking Materials Out of Office**

Employees and their respective Functional Heads will ensure that, while taking any materials including confidential corporate information and personal information (such as PC, printed paper, recording devices and so on) out of the offices shall ensure the following:

* Confidential corporate information and personal information taken from the office shall be limited to the bare minimum information and shall require prior approval from an immediate manager.
* Confidential corporate information to be taken from the office via recordable or other media must be encrypted.
* Take proper security measures against leakage to the third party when we work outside with the taking materials including confidential corporate information and personal information

The respective functional heads & above will also ensure that confidential information in either form if needs to be taken/sent out of factory (for business purposes only), then the same is to be sent out by adopting certain information Security measures.

* + - 1. If the document is a MS-office document (Word/Excel/PowerPoint) and small in size, the password can be given in the program itself.
      2. In case the document size is big or other than Microsoft office document where password cannot be assigned, please follow the below procedure to compress it and assign a password.

The General encryption procedure for file/folder is in Windows operating system

1. **Compressing file/folder through encryption software**

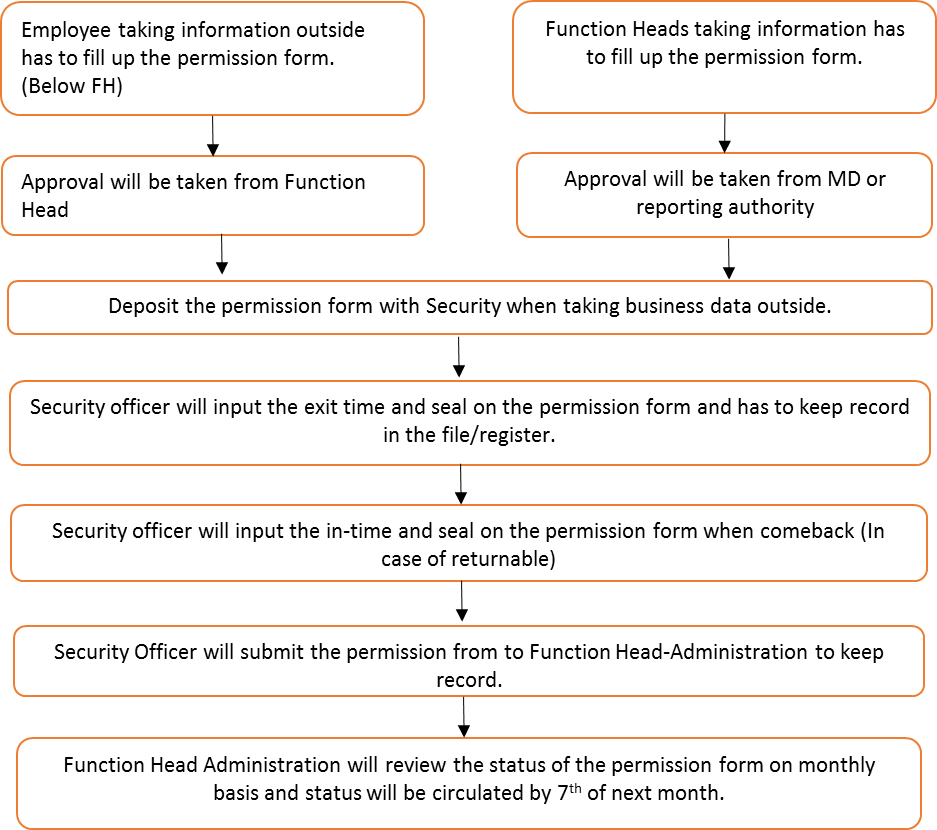
**Encryption Process**

**Decryption Process**

* + - 1. Password will be communicated separately.
      2. Legal or other statutory documents can be sent as per government rules and policies.
      3. If the document is taken out in floppy, CD or in any media, the same is to be routed through permission slip requirements (Format attached in next page) and following points should be taken care.

1. When taking confidential information out of office premises on a storage media, password protect the data.
2. When sending confidential information via the Internet, send the data after it is password protected, and inform the receiver of the decoding password in a separate mail
3. When receiving a document that is scanned using a multifunction printer (scanner) through a network, do not use a shared folder, but instead use an individual/group mailbox so that the scanned data cannot be read by a third party

The following approval hierarchy will be followed in case permission for taking data outside



When taking laptops or any other electronic device outside the company premises needs to get approval as per **Annexure 1 (General Baseline).**

If any laptop is not encrypted in general, it cannot be taken out. In case of emergency it should be recommended by function head IT and approved by Managing Director.

Any employee, who is taking the laptop outside has to ensure that the system is properly shutdown before leaving the office premises.

**Employees having VPN connection in their laptop:** Laptop can be connected with secured Wi-Fi devices or internet and then immediately connect the same with VPN.

**Employees not having VPN connection in their laptop:** Laptop should not be connected with home/or other places Wi-Fi devices or internet

Also, see “Taking documents out of the office” or “Taking out of the company” in Table 4-2, 4-3 for reference

**4.5 Security measures during remote work**

- When working outside the office, such as working remotely or on business trips, take security measures based on the assumption that you will be working in an area that is shared with third parties.

- Even when you are working from home, the use of an individually owned PC for business purposes is prohibited. Be sure to use a PC specified by the company.

After connecting to the Internet, immediately connect to the company network using VPN.

- Check the security settings of your Internet access point (home router, etc.) in advance.

- Do not connect to unknown internet access points. Use company-standard tools for remote meetings.

- If a customer requests that you use other tools, consult with your superior. When using an external satellite office, etc., be aware that you will be working in an area that is shared with third parties (area level 0).

- Always be aware of the eyes and ears of others and do not inadvertently reveal corporate confidential information (using a private room is recommended)

- Prevent corporate confidential information from being captured on surveillance cameras installed at facilities- Printing using multifunction printers provided by the facility is prohibited in principle (violates the prohibition on connecting personal external recording media and the prohibition on connecting to the Internet without a VPN)

- Do not forget anything (this may cause an "accident" regarding the management of corporate confidential information). At the end of work, delete files temporarily saved on the device and shut down (or hibernate) rather than putting the device in standby.

In light of the current environment, Mitsubishi Electric has published “Security Measures for Remote Work,” which describes security considerations when working outside of managed locations. Each Group company is asked to appropriately formulate and update operational rules to maintain information handling standards in response to changes in their respective environments and circumstances.

**4.6 Handling of public internet websites**

During the creation and operation of an internet website, comply with instructions related to official website management distributed to individual group companies by the Mitsubishi Electric Official Website Certification Committee Furthermore, as a crisis management measure to address the risk of phenomena such as system interruptions, tampering, information leaks, loss, or damage that could interfere with the quality and maintenance of official websites, Group companies that operate official websites should comply with instructions from the Official Website Certification Committee concerning website architecture and operation.

While public websites on the Internet are extremely beneficial for the development of corporate activities and business development, accidents involving the leakage, loss, or damage of confidential corporate information can lead to loss of customer trust and social credibility and can be detrimental to a company. Such incidents also risk the survival of the company.

**Section 5: Human Security**

**5.1 Non-Disclosure Agreements with Employees**

Exchange written non-disclosure agreements with employees (including temporary workers) at appropriate times, such as when hiring, changing duties, or retiring, to clarify and conclude an agreement with employees concerning obligations related to security, including maintaining the confidentiality of information obtained during employment.

When managing confidential corporate information, the company must understand who is handling what kinds of corporate information and clarify who is in-charge of which responsibilities and do so in a manner that that is agreed upon by both the employee and the employer. It is important to form a common understanding concerning the extent of responsibilities.

MEAI concludes appropriate non-disclosure agreements with employees by having employees submit written pledges, etc. at the time of hiring, changes in work, and retirement to prevent employees from disclosing, leaking, losing, or damaging the confidential corporate information of Mitsubishi Electric to third parties without permission during their employment or after they retire. Also, make it known that violations will result in disciplinary action.

When an employee (including temporary workers) resigns or their contract ends, request the return of all company-related items. If an employee cannot return his/her borrowed things, he/she must report the reason and the influence on the confidential corporate information. However, if the above content is included in the contract concluded as an obligation of the employee, such as work regulations, there is no need to create new regulations related to information security.

* 1. **Education and training of employees**

For all employee (including top management and temporary staff), security education and training shall be conducted regularly to make them understand the approach and rules regarding information security

of MEAI.

To ensure proper handling of confidential corporate information and personal data and to transform our corporate culture, conduct employee training at the time of hiring or at the time of the employee contract, as well as periodically (once a year). Provide systematic education and training so that employees can acquire the necessary skills based on their roles in information security.

PIC of CPM shall strive to improve skills for information security management by using various educational opportunities for activity of confidential corporate information management, MEAI will have the following education program for employees about information security.

**Table 5-1: Employee Education Program**

|  |  |  |
| --- | --- | --- |
| Title | Details | Frequency |
| Confidential Corporate Information Management and Personal Data Protection education program (For all employee) | Fundamental education (Mitsubishi Electric policies, incident status, reflection on the previous year, internal fraud prevention, etc., and what each individual should be aware of regarding confidential corporate information management and personal data protection (human, physical, technical, and organizational security control measures)). | Once a year |

Topics concerning information security are repeatedly disseminated at opportune times, such as through education programs for newly hired employees, training intended for newly appointed section managers, etc. that are organized by the Corporate Human Resources Div.

Table 5-2: Domestic Group Company Meeting for PIC of CPM

|  |  |  |  |
| --- | --- | --- | --- |
| Title | rough schedule | target | Details |
| Domestic Group Company Meeting for PIC of CPM | Jun. | PIC of CPM | - Explanation of changes in common measures of group companies  - Exchange information on various measures and examples of initiatives related to corporate confidential information management and personal data protection |

Domestic Group company meeting for the person in charge of confidential corporate information and personal data protection management should be actively utilized as opportunities for training staff in charge of implementation and improving security promotion capabilities.

**Section 6: Physical Security**

**6.1 Secure Areas**

* + 1. **Definition of Area Level**

MEAI will define security area level criteria and layout keeping in view of physical securities and the security procedures and rules to be review periodically once in a year or any structure changes whichever is earlier. The security area level will be designed keeping in view of following matter according to Business environment.

Inform employees working in each area of security measures for each area.

The following table shows security area level design in Mitsubishi Electric.

1. Area and Area Level Definition
   1. Explanation criteria for each area level

**Table 6-1: Explanation criteria for area levels**

|  |  |  |
| --- | --- | --- |
| Area level | Explanation (Criteria) | Example of forecast area |
| 4 | Areas within the place of business that are usable/accessible by only a small subset of authorized employees, personnel from related companies, and the like | Special rooms, designated management project rooms |
| 3 | Areas within the place of business that are usable/accessible by only authorized employees, personnel from related companies, and the like | Server rooms, drawing/project rooms, development rooms, and rooms in which important equipment is installed |
| 2 | Areas within the place of business that are generally usable/accessible by all employees and authorized personnel (personnel from related companies, and the like) | Offices, common conference rooms (for internal use) |
| 1 | Areas within the place of business that are generally usable/accessible by all employees and personnel who have completed access procedures (personnel from related companies, suppliers, general visitors, and the like) | Site grounds, shared conference rooms (including those outside the company), and hallways |
| 0 | Outside the perimeters | Off-premises |

* 1. **Assigning area levels**

(a) As shown in Figure 6-1, area levels are generally set up in concentric circles.

Special rooms/designated managed projects rooms

**Area level 4**

Server rooms, drawing/project rooms, development rooms

**Area level 3**

Offices, etc.

**Between area levels (3 → 4)**

**Area level 2**

**Site access**

**Between area levels (2 → 3)**

Site grounds, shared conference rooms, and hallways

**Between area levels (1 → 2)**

**Area level 1**

**Room Access**

Outside the place of business (off-premises)

**Between area levels (0 → 1)**

**Area level 0**

(b) Where at all possible, critical area levels 3 and 4 must not be adjacent to area levels 0 and 1.

(c) Direct access from Area Level 0 to Area Level 2 should be avoided wherever possible.

(d) Direct access from Area Level 0 to Area Levels 3 and 4 should be forbidden as a rule.

**3) Establishing physical boundaries**

(a) As shown in Table 6-2, physical boundaries should be established to control site or room access depending on the area levels.

**Table 6-2: Establishing physical boundaries**

Legend (Applicability to physical boundary examples Applicable: 〇, Not applicable: ― )

|  |  |  |  |
| --- | --- | --- | --- |
| Physical boundary  examples  Between area levels | Perimeter walls, fences, shuttered gates, and the like | Walls, doors, gates, fences, and the like | Partitions, elevators, and the like |
| 3→4  2→3  1→2 | ― | 〇 | 〇 |
| 0→1 | 〇 | 〇 | ― |

(b) The physical barriers shown in Table 6-2 should be constructed without gaps or places that are easy to penetrate.

(c) If there are objects near the site perimeter wall or fence that could provide a foothold, modify their height so that it is not easy to penetrate the perimeter, or add spikes or similar deterrents.

(d) Ensure the roofs, walls, and floors of facilities on the premises are structurally sound. And make sure all doors that open to the outside utilize an opening/closing control system (for example, access control equipment or keys) so that they are appropriately protected from intrusion by unauthorized personnel.

(e) Enact policies (keys, grating, surveillance systems, etc.) to prevent intrusion through windows (especially first floor windows) from the outside.

(f) Depending on area level, place security guards or install doors controlled by ID cards or biometric authentication.

* + 1. **Site and Room Access Control**

For site/room access control, introducing technologies such as entrance/exit management systems could assure success. On site/room access control, operation procedures shall be established, taking into consideration with clarification of required security clearance and accessible area levels.

Assign security personnel and install surveillance cameras to continuously monitor the inside and outside of critical facilities.

1. When employees of business location access the site
2. MEAI Employees including Contractual should enter into the office area/factory using biometric devices and related records should be kept. Records of such nature will be maintained.
3. Log identity verification or authentication access history in a ledger or access control system.
4. Personnel from related companies and the like who work at the same place of business can also be handled in the same way.
5. When business travellers (Mitsubishi Electric Group Company) access the site

In principle, the rules are the same as in "3) Visitors.

1. When visitors access the site

Have visitors (other than our employees) record their name, organization department, destination, and time of access during reception when entering or leaving. Also, if reception is unmanned, install a reception system or something like it, to summon responders (employees) who can perform verification. Following reception, visitor badges (including cards and the like) should be issued and visitors asked to wear them, so it is clear that they have completed reception.

When a visitor enters Level 3 or 4 areas, in principle, a receptionist (employee) must accompany them from the time they enter the room until they leave the room. In a Level 2 area, a receptionist (employee) will accompany them as necessary.

* + 1. **Physical access device management**

Physical access devices are keys, locks, dial locks, and ID cards (Identification cards) for entering facilities or locking server racks. Managers shall make a list of active physical access devices and regularly update the list. Managers shall physically control access of the devices and keep records of lending and returning of the devices in preparation for risk of unauthorized use or losing the devices. Managers must de-activate the corresponding locks, for example: replace them, as soon as possible when the devices are lost or are not returned for some reasons. Managers should constantly monitor places where the devices are stored by cameras or guard men if the third party can enter into the stored places We shall store the physical access devices in key boxes or lockable cabinets when using the devices and prevent losing the devices with a neck strap or so on when our moving. We must properly manage the devices in preparation for risk of unauthorized use or losing the devices when returning home outside of our secure areas.

MEAI has managed physical access devices in the following way;

Physical keys are also under management in preparation for risk of unauthorized duplicate key or out-of-date security.

(1) Physical access devices

Physical access devices for entering facilities or locking server racks include

(i) key,

(ii) dial lock,

(iii) ID card, and so on,

(2) Storage of physical access devices

The devices are stored in secure places (Area level is more than 1),

(3) Management methods of physical access devices

A list of active devices is made and the list is regularly updated,

(4) Access control for physical access devices

The devices are access controlled and used by authorized employees.

(5) Lending and Returning

Records of lending and returning of the devices are kept on the list,

(6) Handling of loss, etc.

Proper measures, for example: replacement of lock, are done as soon as possible when the device is not returned for some reasons or is lost.

## **Protection of devices storing confidential corporate information**

Protect devices and equipment storing confidential corporate information from physical and environmental risks.

In areas with devices and equipment used to store confidential corporate information, minimize access permissions, and control and monitor entry and exit.

Supply power in accordance with the handling specifications of devices and equipment used to store confidential corporate information and, as necessary, protect these facilities from power outages or other power abnormalities.

Protect from the possibility of natural disasters.

- Take measures to prevent servers, etc. from falling or moving due to earthquakes.

- Appropriately install fire extinguishing equipment.

- Install in a location with a low chance of flooding.

Also make sure to appropriately manage equipment located outside the premises.

Protect the wiring of power supply cables, data transmission cables or cables supporting information services from interception, interference or damage.

Equipment should be properly maintained to ensure that the availability, integrity and confidentiality of information is maintained.

Establish management procedures for recording media, and constantly check whether storage, removal, return, and disposal are being conducted properly

**Section 7: Incident/Accident Management**

* 1. **Reporting Incidents/Accidents**

MEAI Comply with the Personal Data Protection Guideline when including EU personal data. Furthermore, take the following measures regardless of whether or not information includes EU personal data.

* + 1. **Reporting Criteria**

Information security accidents shall refer to the loss, theft, destruction, modification, unauthorized access, or unauthorized use or disclosure of confidential corporate information. If accidents occur within the company, it is critical to request improvements and provide guidance to the workplace.

MEAI will report "Serious Accident" and "Accident" to Mitsubishi Electric. The Accident Criteria is defined as follow.

**Table 7-1: Accident classifications**

|  |  |
| --- | --- |
| Classification | Definition |
| Serious Accidents | Serious Accidents are accidents characterized by any of the following.  (a) Serious enough that a company executive (President or Director in charge) must make a direct apology to the customer.  (b) Serious enough to require a public relations announcement (public relations necessary to fulfill corporate social responsibility or to communicate widely in order to prevent secondary disasters such as large-scale data leaks,)  (c) When Group company information equivalent to "Top Secret" or "Secret" at Mitsubishi Electric being leaked, lost, or damaged in a situation where no security management measures such as encryption have been applied and there would be a significant impact on each company's business. |
| Accidents | Accidents resulting in external leakage, loss or damage to Corporate Confidential Information (treat the leakage, loss, or damage to non-public customer information as a serious accident or accident)  Furthermore, even in the case of an accident not involving the external leak of confidential corporate information, treat the incident as an accident in the case of the following.  (a) Information ("Secret" or higher for Mitsubishi Electric) that could cause the company to suffer significant losses or disadvantage if leaked to others, lost, or damaged is leaked within the company beyond the scope of disclosure, lost, or otherwise disadvantages are incurred.  (b) CCI of third party was illegally got or used by or for the organization (e.g. the company).  (c) The loss of or damage to personal data impacts the individual or, even if there is no impact on the individual, the incident fulfills the criteria for external accident reporting.  (d) Personal data residing in the EU were lost or damaged and their result had an impact on the person. |
| Minor Accidents | Minor Accidents are given below. Whether to report minor accidents should be determined based on the rules of individual locations.  (a) Accidents related to CCI that do not involve the leakage of internal information and are not equivalent to “Serious Accidents” or “Accidents” outlined above  e.g.: Sending e-mail to (a) wrong address(es) in the company excluding the above case of “Accidents” (a).  (b) Accidents where the subject of CCI has been leaked outside the company but appropriate security measures have been taken so that third parties cannot view the CCI.  e.g.: The lost or theft devices or media were so properly secured that their contents cannot be revealed to unauthorized parties, because of encryption of their data or by other security measures. The encrypted/auto-encryption-set files are downloaded by unauthorized parties who cannot decrypted the files. |
| Close Calls | Examples of Close Calls are given below. Reporting of Close Calls is not needed.  (a) Leak, loss, or damage to internal information that was not CCI and results in only minor damage.  (b) -Lost or theft of media without internal information,  -Unattended Visitors in secure area of the company,  -Malware Alarming when private device or medium was connected with facilities in the company,  etc. |

The purpose of accident reports are the following three reasons.

(a) To identify accidents related to confidential corporate information and, in the event of an accident, to minimize the expected impact on customers, economic losses, and loss of social trust.

(b) To ensure that reports of an accident are issued appropriately and rapidly, and implement internal and external measures (ascertain facts, identify cause and prevent reoccurrence, issue apology and contact customers, submit notifications to related supervisory authorities as necessary, etc.) without fail.

(c) Ascertain problem on and improve information security management.

Regarding incidents related to confidential corporate information, all accidents (when outsourcing, this includes all relevant operations by the outsourcer; the same applies to subcontractors, sub-subcontractor’s companies, etc.) are subject to reporting. If the president of the company determines that the accident classification (form: Company Confidential/Personal Data, Serious Accident/Accident/Minor Accident Report) falls under the category of a "minor accident" or "close calls," then there is no need to report but make the details of the incident known internally within the company as necessary.

Upon occurrence of any accident/incident regarding Information System Security such as computer virus or unauthorized access, please report to CSIRT of Mitsubishi Electric because of prevention of damage extension.

**7.1.2 Accident Reporting System**

"Regarding incidents related to confidential corporate information, all accidents (when outsourcing, this includes all relevant operations by the outsourcer; the same applies to subcontractors, sub-subcontractor’s companies, etc.) are subject to reporting. If the president of the company determines that the accident classification (form: Company Confidential/Personal Data, Serious Accident/Accident/Minor Accident Report) falls under the category of a "minor accident" or "close calls," then there is no need to report but make the details of the incident known internally within the company as necessary.

The user has to report incident/accident details to respective Function Head and thereafter to Function head Administration department as per the details given below.

Serious / Major Accident – Immediately after the incident/accident.

Minor - Within 24 hours maximum up to 48 hours after the incident.

In case of theft/criminal activity outside the premises, user has to report the matter to police and collect First Information Report (FIR copy) which is to be submitted to administration department. In case serious accident/incident happened inside the premises the matter may be reported to police after reviewing the gravity of incident. If "Accidents" or "Serious accidents" occur, MEAI shall report by the following route through accident report form **Annexure-2 (General Baseline).**

When Functional Head IT (FH-IT) will receive information about a security incident/accident related to the information system (service) MEAI is using, FH-IT will confirm the content and alert the user department (concern user through respective FH) based on the management ledger. Also, depending on the nature of the incident/accident, report to the CSIRT and take necessary measures.

**Reporting Route for MEAI**

A picture containing text, diagram, screenshot, font

Description automatically generated

**Reporting Route to MELCO.**

**The reporting system within Mitsubishi Electric Group**

Conduct reporting to relevant authorities as outlined in the Personal Information Protection Act, GDPR, and other relevant laws and ordinances. Each group company other than Japan shall inform Information Security managers in each region (Americas, Europe, Asia pacific and China) when sending a copy to the regional representative organization.



For accident reports, use **Annexure 2 (General Baseline)** as stipulated in the Mitsubishi Electric Corp. internal regulations 1307-1, “Detailed Regulations for Handling Incidents pertaining to Confidential Corporate Information Management. Use this **Annexure 2 (General Baseline)** for "prompt", "intermediate" and "final" reporting. The underlying norms are as follow: -

* When an accident occurred related to confidential corporate information is discovered, the accident shall be reported to the president of the affiliate company through appropriately designated reporting path, and initial response shall be taken to the accident immediately.
* As indicated in figure 7-1, presidents of an affiliate shall immediately +) report the occurrence (preliminary report) of an accident using Accident 2(Accident Report) going through the primary controlling division Secretariat.
* Emergencies related to personal data should be reported within 3 days regardless of whether one uses a paper or e-mail, and no matter whether it is a holiday or business day. In cases requiring urgency, it refers to accidents that require reporting to external agencies. According to the definition of Japan's Act on the Protection of Personal Information, this includes personal data containing sensitive information, personal data that may result in financial loss due to unauthorized use, personal data that may have been obtained for malicious purposes, and cases where the leakage, lost or damage of personal data of more than 1,000 individuals has occurred.
* After completion of all measures implementation, use **Annexure 2 (General Baseline)** to issue a final report. (In principle, within 30 days of the initial report). If completion will be delayed or an interim report is necessary, then submit an interim report. In case it takes quite a while to close the accident, the "final" report can be sent when permanent measures to be taken are decided.
* Refer to the attached "Confidential Corporate and Personal Information Accident Report" form for more details.
* As for cyber security incidents, MEAI allows reports written in another form defined by Mitsubishi Electric rule 1911 “Rule for cyber security incident and accident.” We obey the instruction by MELCO-CSIRT.
* Contact Details for accident reporting will be maintained in **Annexure 3 (General Baseline)** which will be reviewed and updated in April and October every year.
  1. **Preventive measures**

When information security incidents or accidents occur, immediate countermeasures shall be important to minimize the influence of such incidents/accidents. However, implementing preventive countermeasures shall be more important to prevent the similar incidents/accidents occurrence. To prevent recurrences, investigation of essential cause of the incidents/accidents and implementation of beneficial and effective permanent measures shall be conducted.

MEAI has introduced "Why Why Analysis" to develop efficient preventive measures against accidents or other security incidents.

**Table 7-4: Guidance points related to intrinsic safety**

|  |  |
| --- | --- |
| Focus | Details |
| 1. Eliminate operation | Try to eliminate the operation itself (e.g. If you use communications methods other than fax machines, wrong fax transmissions will not occur.). |
| 2. Prevent from wrong operation | Make sure only predetermined acts are possible (e.g. Only when prescribed items are completed, next stage can be provided to end-users.) |
| 3. Make easier to understand | Appeal to human cognitive features (e.g. Add company names to mail address books to make them easier to recognize; prevent erroneous operations using colors or markings). |
| 4. Facilitate operations | Make it easier to carry out operations, reduce the burden (e.g. Use friendly systems reduce fatigue and prevent loss of concentration.) |
| 5. Trigger awareness | Give warning to ensure not to make mistakes (e.g. Display message to confirm sending an e-mail before the action) |
| 6. Make users recognize/predict | Enable users to recognize/predict which situations are dangerous (e.g. Enhance sensibility to information security through KYT (Kiken Yochi (hazard prediction) Training)) |
| 7. Ensure safety first | Give people the sense of values or criteria to prioritize security (e.g. Education through slogans, posters, etc.) |
| 8. Give users capabilities | Ensure users have the ability to carry out operations safely and reliably (e.g. Education and training) |
| 9. Make users more alert | Ensure that users/teams notice errors by themselves (e.g. Alter check sequences each time so as to use a different perspective as much as possible) |
| 10. Detect | Make easier to detect errors (e.g. Ensure an alarm sounds if operations are not carried out in the correct sequence, etc.) |
| 11. Prepare | Take measures to minimize damage even if accidents occur (e.g. Encrypt) |

**Section 8. Compliance**

* 1. **Legal requirement**

For appropriate management of all confidential corporate information regarding the company's business activities, applicable law and regulation shall be identified and managed.

1. Information Technology Act, 2000
2. Indian Penal Code, 1860
3. Indian Contract Act 1872
4. Cyber Law

The respective managers have/will ensure identification/execution of all applicable laws and regulations.

If there are other specific legal requirements in each jurisdiction, MEAI will review all the feasibility to include them in this policy, if necessary. Also give due consideration to laws and regulations concerning intellectual property and encryption.

* 1. **Continual Improvement of information security management**

The ISMS rule / policy will be reviewed periodically and the schedule for review is given below.

**Table 8-1: Elimination security assessment for group companies**

|  |  |  |
| --- | --- | --- |
| Program name | rough schedule | details |
| Information security self-check program | Jan. - Mar. | By using checklist based on control list in ISMS (ISO/IEC 27002) being aligned with these Guidelines, conduct self-check for information security. |
| Information security assessment by externals | Full-year  (inspection every three years) | Be checked the information security management by third parties (primary controlling division of Mitsubishi Electric, other related group companies, etc.) |

**8.3 Collection of evidence**

For risks of information leaks, unauthorized use or unauthorized access, in addition to system administrator’s operation logs and records for taking-out/returning materials, also consider keeping access records for buildings or offices and the storage of surveillance video.

Logs of DLP (Data Leakage Protection) like Printing, USB/CD/Mobile Memory Copy, Outlook Email Upload, FTP, Skype, P2P, IM, Web Upload Data (Gmail, Yahoo, Google Drive etc.) is maintained for a period of six (6) Months applicable for all employees below General Manager Level.

**Section 9.0 Approach to information security in the event of an emergency**

Even in the event of a disaster, the same information security response as per **Clause 7. Incident/Accident management** as in normal times is required.

Maintain information security at an appropriate level even when business is interrupted or hindered due to natural disasters or cyber accidents. Evaluate information systems and consider redundancy to ensure availability in emergency situations. Regarding the exceptions for the use of personal PCs, ensure that company security measures (i.e., prohibition of storing or using confidential corporate information on personal PCs) are maintained. Each department should consider lending out company PCs as a BCP response. If the information does not qualify as "Confidential" (information related to confirming safety, business instructions that do not include confidential corporate information), it is acceptable to contact employees via mobile phone or private PC.

**Section 10.0 Revision/Amendment in Policy**

**10.1** Management reserve the right to include/amend/revise any clause/section in any part of the policy.

**10.2** This policy will be reviewed bi-annually preferably in the month of June & December or as and when required and the record of the same will maintained by HR Dept.