# Information Security

## M&M Internal Privacy Policy

## DOCUMENT CONTROL

| | |
|---|---|
| **DOCUMENT NAME** | M&M Internal Privacy Policy |
| **DOCUMENT NO.** | ISMS-POL/Internal_Privacy/25/v2 |

## AUTHORISATION

| | **Prepared By** | **Reviewed By** | **Authorised By** |
|---|---|---|---|
| **Name** | Dhananjay Purankar | Shivani Arni | Mohit Kapoor |
| **Designation** | Principal – Governance Risk & Compliance | Enterprise CISO | Group Chief Technology Officer |
| **Date** | 22/01/2025 | 22/01/2025 | 22/01/2025 |

## SECURITY CLASSIFICATION: Internal

## VERSION HISTORY

| VERSION | DATE | PREPARED BY | CHANGES & REASONS FOR CHANGE |
|---|---|---|---|
| 1.0 | 23/01/2024 | Dhananjay Purankar | Initial |
| 2.0 | 22/01/2025 | Dhananjay Purankar | Policies Revamped |

## DISTRIBUTION LIST

| Sr. # | Location | Department |
|---|---|---|
| 1 | Infosec Portal | All M&M Users and Group Companies under ISMS Scope |
| | | |

# Table of Contents

## 1. Purpose

This policy sets out the guidelines that must be followed to protect the privacy of Mahindra' s entities and Personal Data (also referred to as "PII") that is processed by Mahindra of its clients, customers, employees, contractors, vendors (collectively called as "Data Principals"), and to perform any action with regards to personal data, whether in whole or in part, such as collecting, recording, organizing, storing, modifying, using, disclosing, transferring, monitoring or deleting in its capacity as a Data Fiduciary and a Data Processor. This policy ensures that Mahindra implements the industry best practices, meets the legal, statutory, and regulatory requirements, and demonstrates compliance with the Digital Personal Data Protection Act, 2023 (DPDPA). This policy acts as a guiding framework to ensure Mahindra is compliant to the Digital Personal Data Protection Act, 2023.

## 2. Scope

The scope of the policy extends to all the locations of M&M and its group companies under the scope of ISMS.

## 3. Applicability

This policy applies to all Personal Data collected, processed, stored, transferred, or retained by Mahindra for all the information collected from a Data Principal directly or indirectly either in a or electronic form. This policy also applies where data is shared/transferred with third parties and Mahindra acts as a Data Fiduciary or a Joint Data Fiduciary. Various sections of this policy only apply where Mahindra processes Personal Data on the instructions of a Data Fiduciary and acts in the capacity of a Processor. The scope of this Policy extends to Mahindra and Mahindra Limited including but not limited to all employees/staff, third party vendors, contractors who deal with and have access to Personal Data.

## 4. Terms and definitions

| Terms | Definitions |
|---|---|
| Applicable Data Protection Laws | Digital Personal Data Protection Act (DPDPA) 2023 and any other data protection laws, rules, regulations, standards, and codes of conduct applicable to Mahindra, that address Data Breaches or issues relating to a Data Breach. |
| Board | Board means the Data Protection Board of India, established by the Central Government. |
| Consent | Consent of the Data Principal means any freely given, specific, informed, unconditional and unambiguous indication of the Data Principal's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of her personal data for the specified purpose. |
| Consent Manager | Consent Manager means a person registered with the Data Protection Board who acts as a single point of contact to enable a Data Principal to give, manage, review, and withdraw her consent through an accessible, transparent, and interoperable platform. |
| Data Fiduciary | Data Fiduciary means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data. |
| Data Principal | Data Principal means the individual to whom the personal data relates. |

| | |
|---|---|
| Data Privacy Team | Data Privacy Team means one or more team members who have been tasked to identify and comply with applicable data privacy requirements within the organization. |
| Data Processor | Data Processor means any person who processes personal data on behalf of a Data Fiduciary. |
| Data Protection Officer | Data Protection Officer means an individual appointed by the Significant Data Fiduciary, who shall represent the Significant Data Fiduciary under DPDPA, be based in India, be responsible to the Board of Directors or similar governing body and be the point of contact for the grievance redressal mechanism. |
| Personal Data | Personal Data means any data about an individual who is identifiable by or in relation to such data. |
| Personal Data Breach | Personal Data Breach means any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data. |
| Profiling | Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location, or movements. |
| Pseudonymisation | Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific Data Principal without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. |
| Significant Data Fiduciary | Significant Data Fiduciary means any Data Fiduciary or class of Data Fiduciaries based on assessment of relevant factors such as the volume and sensitivity of personal data processed, risk to the rights of the Data Principal, potential impact on the sovereignty and integrity of India, risk to electoral democracy, security of the State, and public order. |

## 5. Roles and Responsibility

| Roles | Responsibilities |
|---|---|
| Consent Manager | • Ensure Data Principals provide valid, informed, and specific consent for the collection and processing of personal data.<br>• Keep accurate records of consents obtained and ensure they are retrievable.<br>• Manage the process for Data Principals to withdraw their consent at any time.<br>• Facilitate Data Principal requests related to consent and processing. |
| Data Fiduciary | • Ensure all data processing is lawful, based on a valid legal basis (e.g., consent, contract, legal obligation).<br>• Ensure all data processing is lawful, based on a valid legal basis (e.g., consent, contract, legal obligation).<br>• Ensure third-party vendors (Data Processors) comply with privacy laws and contractual agreements.<br>• Oversee and conduct DPIAs when needed for high-risk processing activities. |

| | |
|---|---|
| Data Protection Officer | • Ensure the organization complies with data protection laws and internal policies.<br>• Provide guidance on data protection and ensure privacy regulations are followed.<br>• Support the organization in responding to Data Principal requests and complaints.<br>• Ensure that data breaches are reported in accordance with legal timelines. |
| Data Principal | • Give valid consent for the collection and processing of personal data and withdraw it when desired.<br>• Request access, correction, or erasure of personal data and lodge complaints if needed.<br>• Nominate a legal heir or representative in the event of death or incapacity to manage their data. |
| Data Processor | • Process personal data only as instructed by the Data Fiduciary.<br>• Implement necessary security measures to protect personal data.<br>• Promptly inform the Data Fiduciary about any data breaches.<br>• Help the Data Fiduciary respond to Data Principal requests, such as access or erasure. |

# 6. Internal Privacy Policy

## 6.1 Privacy Reporting and Cooperation

- The Internal Data Privacy Team / Infosec Team should develop, disseminate, and update the regulatory bodies and other oversight bodies, as appropriate, with suitable reports to demonstrate accountability with specific statutory and regulatory privacy program mandates.
- The Internal Data Privacy Team / Infosec Team shall assist/ support group companies when interacting with the regulatory bodies on issues relating to data privacy matters.
- The Internal Data Privacy Team / Infosec Team should demonstrate compliance to applicable privacy requirements and apprise the MD/ executive management/ steering committee regarding the same.
- If Mahindra is classified as a Significant Data Fiduciary by the Board, then it shall comply with the additional obligations of the Significant Data Fiduciary as mentioned in the DPDPA.

## 6.2 Data Identification and Inventory

- **Data Identification**
  - Business Owners should be responsible for identifying, classifying, and documenting information assets, that contain Personal data either in the physical form or electronic form.
  - The IT Team should support the Business Owners by providing secure storage means for personal data, basis their identification and classification.
  - Business Owners should be accountable for implementing Data Identification and Classification requirements as defined in this policy document, as well as **Mahindra's Information Asset Classification Policy and Procedure.** The Business owners shall consult the **Internal Data Privacy Team / Infosec Team** in case of any queries regarding the same.

- **Data Classification**
  - All Personal Data should be handled as per the policies defined in this document.
  - The classification shall be performed basis the following classification categories:

**Confidentiality:** Under confidentiality, the information shall be classified as Highly Confidential/Confidential/Internal/Enterprise Public/Public.
**Integrity:** Under integrity, the information shall be classified as Very High Accuracy/Accuracy/Medium Accuracy/Low Accuracy/Not Required.
**Availability:** Under availability, the information shall be classified as Interoperable Disruption/Immediate/Priority/Routine/Not Required.

- The Internal Data Privacy Team / Infosec Team should be responsible for ensuring that all Information categorized as Personal Data marked with Privacy as classification label.
- The Internal Data Privacy Team / Infosec Team shall inform personnel dealing with personal data within the organization to use appropriate classification labels when dealing with personal data i.e., data at rest or in transit.
- For detailed guidance on data classification and labelling, please refer to **Mahindra's ISMS Information Asset Classification and Media Handling Procedure** as well as **Mahindra's Labelling Schema for Information Guidelines.**

- **Collection/Processing of Personal Data**
  - Mahindra must collect, use, store, process, transfer or disclose personal data for reasonable, specific, and lawful purposes only, as defined in this policy.
  - Mahindra should use secure methods for the collection of personal data. These methods should be evaluated and selected by respective Business Owners in consultation with the Data Privacy Team.
  - Mahindra must classify all the personal data that is collected or processed in accordance with the Privacy classification mentioned in this policy and must adhere to the principles of privacy while processing the personal data.
  - Data Privacy Team should take reasonable/ feasible efforts to ensure that the personal data collected is accurate, and where necessary and possible, kept up to date.
  - The Internal Data Privacy Team / Infosec Team must be accountable to demonstrate compliance with respect to the above processing requirements.
  - Where Mahindra acts as a processor, steps must be taken to ensure data collected on behalf of the Data Fiduciary is in line with the contractual agreements maintained with the Data Fiduciary.

- **Asset Management**
  - Mahindra should follow the Information Asset guidelines mentioned in the '**Mahindra ISMS Information Asset Classification and Media Handling Policy and Procedure**' for assets containing personal data.
  - All assets containing personal data should be protected from unauthorized access and be made available all the time. Refer to '**Mahindra ISMS Access to Information and System Policy and Procedure**'.
  - Controls shall be implemented, where feasible to mitigate risks related to asset thefts and asset loss.
  - Employee shall receive adequate training to report any loss of devices or assets used for storage of personal data. Refer '**ISMS Reporting and Management of IT Security Incidents, Malfunctions and weaknesses**' and/or '**ISMS Reporting and Management of Non-IT Incidents Procedure**' for procedures related to reporting of any loss of devices or assets.
  - Employees shall exercise complete caution while using portable devices for managing personal data. Refer '**Mahindra ISMS Information Asset Classification and Media Handling Procedure**' for guidance related to handling of removable media.

- Employees shall protect such devices against loss or theft and shall immediately report any such instances to the IT Helpdesk.

## 6.3 Lawfulness and Data Control

- **Principles for Processing Personal Data**

  Mahindra is committed to processing data in accordance with the following principles:

  - **Lawfulness, fairness, and transparency:** Mahindra processes data only on an identified legitimate use. The purpose of collection will be specified not later than at the time of data collection, or on each occasion of change of purpose. Mahindra is committed to process data fairly and honestly and complies with the transparency obligations of the right to be informed. It makes readily available to individuals, specific information related to management of Personal Data.
  - **Purpose Limitation:** Mahindra collects data only for specified, explicit and legitimate purposes and does not further use Personal Data in a manner that is incompatible with the initial purposes. As a Processor, it collects data only on the instructions of the Data Fiduciary.
  - **Data Minimization:** Mahindra collects data that is relevant and limited to what is necessary to fulfil the purpose.
  - **Data Quality/Accuracy:** Mahindra takes all reasonable steps to ensure the personal data it holds is not incorrect or misleading and the accuracy, validity, quality is maintained.
  - **Retention Restriction/Storage Limitation:** Mahindra holds the data only for the time it is required to complete the business activity and no longer than it is necessary.
  - **Integrity and Confidentiality:** Mahindra uses appropriate technical or organizational measures to ensure security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage.
  - **Accountability:** Mahindra understands its accountability and responsibility for any Personal Data that it may receive, use, process, store as part of its business. Accordingly, it will ensure that the authorities, responsibilities, and accountabilities for all policy, controls, and activities are clearly defined and adhered. Everyone shall take ownership of the respective activities; have appropriate procedures, guidelines, records and other measures to be able to demonstrate that Personal Data is used / stored / processed / retained / disposed / transferred in compliance with applicable Data Protection laws; ensure the availability of Mahindra's policies, procedures and contacts for management of personal information.

- **Lawfulness of Processing Personal Data**
  - Any processing of personal data that is carried out within Mahindra must be supported by one of the following legitimate uses of processing

  a) the Data Principal has given consent to the processing of his or her personal data for one or more specific purposes.
  b) processing is necessary for the performance of a contract to which the Data Principal is party or to provide goods and services to the Data Principal.
  c) processing is necessary under any law for the time being in force made by the Parliament or any State Legislature or for compliance with any judgment or order of any Court, quasi-judicial authority or Tribunal in India.
  d) processing is necessary for the performance of any function of the State authorized by law.
  e) processing is necessary to undertake any measure to provide medical treatment or health services to any individual during an epidemic, outbreak of disease or any other threat to public health.

f) processing is necessary for reasonable purposes which may include prevention and detection of any unlawful activity including fraud; mergers, acquisitions, any other similar combinations, or corporate restructuring transactions in accordance with the provisions of applicable laws; recovery of debt; processing of publicly available personal data; and the above purposes are subject to the legitimate interest of the data fiduciary in processing for that purpose; whether the data fiduciary can reasonably be expected, and it is practicable to obtain the consent of the data principal; any public interest in processing for that purpose; the degree of any adverse effect of the processing activity on the rights of the data principal; and the reasonable expectations of the data principal having regard to the context of the processing.

- The Data Privacy Team should, in consultation with the Internal Data Privacy Team / Infosec Team, select a relevant legitimate use for each of their processing activities, based on the processing activity and the applicable privacy laws and regulations, and document the selected legitimate use against each processing activity.
- The decision of the Internal Data Privacy Team / Infosec Team should be considered final in the determination of an appropriate legitimate use of processing.
- Mahindra should perform profiling or automated decision making only if the processing will not affect the rights and freedoms of its Data Principals, and in cases where –

a) It is necessary for entering into, or performance of, a contract between Mahindra and the Data Principal; or

b) Mahindra is authorized by the regulatory authorities to perform such processing under suitable measures that safeguards Data Principal rights and their legitimate interests; or

c) The Data Principal has provided their explicit consent to the processing.

- Mahindra shall not carry out profiling, tracking or behavioral monitoring of, or targeted advertising directed at, children and undertaking any other processing of personal data without a verifiable consent of the parent.
- The Business Owners shall consult the Internal Data Privacy Team / Infosec Team prior to performing any Profiling or Automated Decision Making.
- The Business Owner shall ensure that the Data Principal is aware of the outcome of profiling and the impact it may have on the services provided to them.
- The Business Owners along with the Data Protection Team should implement technical and organizational measures **(see 'Annexure A')** to safeguard the rights, freedoms, and the legitimate interests of the Data Principal.

- **Retention/Archival of Personal Data**
  - All Personal data should be retained as per applicable laws and/or customer contracts. For more information, refer to '**Mahindra's Data Retention Policy'**.
  - Mahindra shall not retain any personal data beyond the period necessary to satisfy the purpose for which it is processed and shall delete the personal data at the end of such period.
  - Mahindra shall undertake periodic review to determine whether it is necessary to retain the personal data in its possession.
  - Mahindra shall retain personal data only for the following purposes, after the purpose for processing has been fulfilled:

a) If explicitly consented to by the Data Principal

b) For compliance with a legal obligation

c) For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

  - The Business Owners should consult the Internal Data Privacy Team / Infosec Team/Legal Team to identify the retention period as per applicable regulatory requirement/laws in its own country.

- Mahindra must also notify the Data Principal, the duration for which their data has been retained, via the Privacy Notice.
- Mahindra should ensure that necessary organizational and technical measures such as Anonymization and Pseudonymization have been implemented to protect the retained/archived data from unauthorized access/disclosure.
- Mahindra shall consider all contractual requirements with Data Fiduciary for defining the retention periods for personal data.

- **Disposal/Destruction of Personal Data**
  - Mahindra must dispose/destroy all personal data if the purpose for which personal data was collected is fulfilled and personal data is not required for further processing.
  - Mahindra should ensure that any personal data that is disposed/destroyed cannot be recovered back in its original form:

a) Physical copies should be disposed/destroyed using paper shredders
b) Electronic copy or in external media should be disposed/destroyed using special external media degaussers and data wipe tools

  - The Internal Data Privacy Team / Infosec Team/Legal Team should be consulted if for any reason the data cannot be destroyed/deleted and the said personal data should be anonymized.

## 6.4 Communication and Awareness

- **Privacy Notice Requirements**
  - Mahindra must publish a Privacy Notice on any external facing website/application or any other platform, as per the requirements of the applicable privacy laws and regulations in the region where it will be accessed, to inform the Data Principal about the processing of their personal data.
  - The Privacy Notice must include the following information, at minimum:

a) The purposes for which the personal data is to be processed
b) The nature and categories of personal data being collected
c) The identity and contact details of the data fiduciary and
d) The contact details of the Internal Data Privacy Team / Infosec Team, if applicable
e) The right of the data principal to withdraw his consent, and the procedure for such withdrawal, if the personal data is intended to be processed on the basis of consent
f) The basis for such processing, and the consequences of the failure to provide such personal data
g) The source of such collection if the personal data is not collected from the data principal
h) The individuals or entities including other data fiduciaries or data processors, with whom such personal data may be shared, if applicable
i) The information regarding any cross-border transfer of the personal data
j) The period for which the personal data shall be retained or where such period is not known, the criteria for determining such period
k) The existence of and procedure for the exercise of rights and any related contact details for the same
l) The procedure for grievance redressal
m) The right to file complaints to the Board
n) Where applicable, any rating in the form of a data trust score assigned by Data Auditor

- The Business Owners in consultation with the Data Privacy Team shall be responsible to draft the Privacy Notice and for reviewing and updating the same on a periodic basis to reflect any changes in services or usage of personal data by Mahindra
- The Internal Data Privacy Team / Infosec Team should consult the Legal Team to obtain their inputs on the Privacy Notice and must review and approve the Privacy Notice before publishing it

- **Choice/Consent Notice Requirements**
  - Where the legitimate use of processing has been identified as consent, Mahindra must develop appropriate consent mechanisms to obtain and record consents of Data Principals. It must appoint a Consent Manager, who shall be registered with the Board in such manner and subject to such technical, operational, financial, and other conditions as may be specified by regulations.
  - The following consent requirements are mandated under the DPDPA:

  a) Consent shall be obtained freely, meaning not caused by coercion, undue influence, fraud, misrepresentation, or mistake.

  b) Consent shall be informed, specific and clear

  c) Consent shall be capable of being withdrawn

  - Data Principals may give or withdraw their consent to the Data Fiduciary either directly or through Consent Manager. Where the Data Principal gives or withdraws consent through a consent manager, such consent, or its withdrawal shall be deemed to have been communicated directly by the Data Principal.
  - If Mahindra processes any personal data of children (below the age of 18 years) in India, then it must obtain a verifiable consent of his parent or lawful guardian prior to processing the child's data.
  - While Mahindra is a Data Fiduciary, the burden of proof that the consent has been given by the data principal for processing of the personal data lies on Mahindra.
  - Mahindra must provide the Data Principals with the feasibility and procedure of withdrawing their consent at any time during the processing of personal data.

- **Cookies**
  - Mahindra must publish a cookie policy and a cookie consent banner requesting Data Principals to accept or reject cookies on the external facing website/applications/platforms; explicit consent should be obtained where personal data is collected from the Data Principals in the form of cookies and consent is the legitimate use of processing of those cookies.
  - The Business Owners in consultation with the Data Privacy Team shall be responsible to draft the Cookie policy and for reviewing and updating the same on a periodic basis to reflect any changes/additions to capturing of Cookies.

- **Training & Awareness**
  - The Internal Data Privacy Team / Infosec Team must be responsible for creating awareness and training of employees involved in processing operations and privacy audits.
  - The Company Office for Data Privacy should identify the privacy training requirements for Mahindra and communicate the training needs to the relevant stakeholders and Business Owners
  - The Internal Data Privacy Team / Infosec Team should develop privacy training programs for all employees handling personal data and provide an approval on the training objectives.

- The Company Office for Data Privacy should also conduct periodic trainings within their respective companies.

## 6.5 Vendor Due-diligence and Cross border data management

- **Third Party Vendor Management**
  - Mahindra may share personal data collected by it, with third parties, to aid the processing of the personal data or for additional services. Where such third parties are appointed, the third-party agreement must clearly define if Mahindra is a Data Fiduciary or processor and shall contain the following at a minimum:

a) Clearly defined purpose for processing personal data.
b) Clearly defined the scope of the processing activities.
c) Types of Data Principal.
d) Jurisdictions where personal data may be processed.
e) Documented Organizational and Technical measures meeting Mahindra and regulatory obligations.
f) Secure destruction or return of the data when requested.
g) Responsibilities and process are clearly defined in the Data Breach event.
h) Clearly defined responsibilities for the breach notification.
i) Protecting the confidentiality of personal data.
j) Establish a process for Data Principal request management; and
k) Establish an audit mechanism for personal data protection.

  - The Internal Data Privacy Team / Infosec Team/Legal Team should have the final authority in the interpretation of personal data transfer to a third party and should provide approval before the execution of any agreement involving the processing of personal data
  - The Legal Team should be responsible for conducting vendor audits related to Privacy on a periodic basis as per the binding agreement; wherever applicable.
  - As a processor, Mahindra shall obtain written consent or approvals from the Data Fiduciary before engaging any third parties for processing personal data on its behalf, and shall ensure the following:

a) Maintain valid and updated Data Protection Agreements with third parties (sub-processors), and include controls as stringent as those present in Mahindra' s contract with the Data Fiduciary
b) Obtain an assurance of the technical and organizational measures implemented by the third-party to ensure personal data protection
c) Inform the Data Fiduciary of any changes in the services provided by the third-party (sub-processor)

- **Data Transfer Mechanisms – Cross Border Transfer**
  - The Data transfer requirements may change basis the applicable privacy law requirements. All Employees should validate the same with The Internal Data Privacy Team / Infosec Team prior to cross border transfer of personal data.
  - The Internal Data Privacy Team / Infosec Team should be notified prior to the selection of any of the above transfer mechanisms and should review and validate the cross-border transfer mechanisms, in consultation with the Legal team.
  - The Internal Data Privacy Team / Infosec Team/Legal Team should be the final authority in deciding the cross-border transfer mechanism.

## 6.6 Request, Incident and Breach Management

- **Data Principal Request**
  - Mahindra must provide the Data Principals the freedom to exercise their Data Principal Rights, as per the DPDPA.
  - Following are the rights are available to the Data Principals -

a) Right to Access Information
b) Right of Grievance Redressal
c) Right to Nominate
d) Right to Correction and Erasure
e) Right to Withdraw Consent

  - The Data Principal will now be able to exercise his or her right to decide how their data will be handled in case of casualty or death by nominating a legal heir or representative.
  - The Data Principal rights are governed by the legitimate use for which the data is being processed by Mahindra **(Refer to 'Annexure B')**
  - The Data Principal, for exercising any right, shall make a request in writing to Mahindra either directly or through a Consent Manager.
  - Mahindra must provide clear communication channels such as E-mail or Web Form, through which the Data Principals can send a Data Principal request. The same must be communicated via the Privacy Notice to external Data Principals and via internal notices to internal Data Principals (e.g., employees).
  - The Data Privacy Team must validate the identity of the Data Principal raising the Data Principal request. If required, additional personal data can be requested to validate the identity of the Data Principal; should validate the Data Principal request to check if it is a valid request. Requests can be validated against the applicable privacy laws in the region of the Data Principal and the legitimate use of processing used; should maintain a record of the Data Principal requests received
  - As per industry best practices, the time taken to respond to Data Principal requests is 30 days from the receipt of such requests, except where such request involves complexity; extensions must be communicated to the Data Principals within a month of receipt of the request.
  - Mahindra, as a Processor must assist the Data Fiduciary in fulfilling its obligation of responding to Data Principal Rights.
  - In its capacity as a Processor, Mahindra will respond to the request of Data Principals directly if so, required by the contractual obligations. Otherwise, Mahindra will only support its clients, in their capacity as a Data Fiduciary, with request processing in accordance with directions received from the Data Fiduciary.
  - The Business SPOC should inform the Data Processors/Third-Party Vendors about the requests from Mahindra' s Data Principals, where applicable, without any undue delay.
  - Mahindra shall have the right to refuse to act on the request if the requests are excessive because the request is complex or repetitive in nature, or the processing is in interests of national security, or the processing is as directed by the applicable law. If the request is refused, Mahindra shall provide the Data Principal the reasons in writing for such refusal and shall inform the Data Principal regarding the right to file a complaint with the Board against the refusal.

- **Complaints/Grievance Redressal**
  - Data Principals have the right to lodge a complaint with the Board to seek judicial remedy. Mahindra shall inform the Data Principals about the same and provide information regarding the means to lodge the complaint. The Internal Data Privacy Team / Infosec Team should be responsible to communicate with the Board regarding the complaint.

- Data Principals may make a complaint of contravention of any of the provisions of this Bill, or the rules or regulations made thereunder, which has caused or is likely to cause harm to such Data Principal, by lodging a complaint to The Internal Data Privacy Team / Infosec Team via e-mail on privacy@mahindra.com.
- The Internal Data Privacy Team / Infosec Team should be responsible to respond to any complaint made by a Data Principal within 30 days from the receipt of the complaint.

- **Incident Management**
  - All Mahindra employees should report privacy incidents (incidents involving personal data) to IT Help Desk.
  - All IT Incidents and action taken shall be recorded at IT Help Desk as per M&M Procedure for Reporting & Management of IT Incidents. Level 2 and Level 3 incidents as defined in M&M Procedure for Reporting and Management of IT Incidents, shall be escalated to data centre & Mahindra IT respectively.
  - Information Security incidents, if required to be communicated to outside authorities/ press, will only be reported by Head-Corporate Communications in consultation with Group CIO.
  - Mahindra IT shall investigate Level 3 IT incidents and take corrective steps to avoid recurrence of such incidents in future. Required evidence shall be preserved wherever necessary.
  - Learning from such incidents shall be captured, stored appropriately and be disseminated to IT Users.
  - Head Mahindra IT / Sector IT shall investigate IT incidents (As defined in M&M ISMS Reporting and Management of IT Security Incidents, Weaknesses and Malfunctions Procedure - ISMS-PRO/A1.3/RMITsec/14/V11) and take corrective steps as per M&M ISMS Corrective Action and Continuous Improvement Procedure - ISMS-PRO/A16.1.3/CACI/1/V11 to avoid recurrence of such incidents in future. Required evidence shall be preserved wherever necessary.
  - Mahindra, as a Processor must notify the Data Fiduciary about the incident along with the details such as, the nature of the breach, likely consequences and measures taken to address the breach without undue delay.

- **Breach Management**
  - The Data Breach Response Team shall follow the procedures laid down in '**Mahindra's Personal Data Breach Management Procedure'** to identify, contain, mitigate, report the data breach and shall determine if the privacy incident is an actual data breach, in consultation with The Internal Data Privacy Team / Infosec Team.
  - After becoming aware of a personal data breach, The Internal Data Privacy Team / Infosec Team must, without undue delay, notify the data protection Board within the required legal timeline. 72 hours is the duration within which data breaches must be reported to the Board as per DPDPA.
  - The notification must contain all required information such as nature of personal data which is the subject-matter of the breach; number of data principals affected by the breach; possible consequences of the breach; and the remedial action being taken by the data fiduciary for such breach.
  - The Internal Data Privacy Team / Infosec Team shall maintain the records of all breaches, likely consequences and measures taken and should verify that all agreed measures have been taken within a reasonable time to contain/mitigate the data breach.
  - Third Party Vendor Processing Personal data on behalf of Mahindra should be mandated to report any data breach within 72 hrs. of being aware of such a breach. Such mandate should be a part of the Data Protection Agreement signed with the vendor.

- Mahindra, in its capacity as a Processor must notify the Data Fiduciary about the breach without undue delay along with the required information such as, the nature of the breach, likely consequences and measures taken to address the breach.

## 6.7 Data protection and security

- **Information Security Requirements**
  - Mahindra shall have information security policies and procedures in line with industry standards such as ISO 27001 for protection of organization information.
  - Mahindra should conduct periodic risk assessments to identify the risk associated with information and implement adequate controls for protection of the same.
  - Mahindra should take into consideration specific control requirements for protection of personal information based on the application regulation or requirements.

- **Data Security (Personal Data)**
  - For the protection of personal data, Mahindra should implement security controls at the time of collection, processing, storage, transfer, and retention, to ensure that the confidentiality, availability, and integrity of the personal data is maintained throughout the data lifecycle. **(Refer: Mahindra ISMS-Asset Classification and Media Handling Procedure)**
  - Mahindra should ensure that restricted access is provided to personnel dealing with systems that involve the processing/ storage of personal data, based on the principle of least privilege and on a need-to-know basis **(Refer: Mahindra ISMS-Access to Information and Systems Policy and Procedure)**
  - Any personal data collected as a part of authorizing the Data Principal to any application should be governed by the Collection/Processing of personal data mentioned in this privacy policy
  - Physical security measures such as locks, cabinets, CCTV cameras etc. should be implemented for protection of personal data.
  - No personal data shall be collected/processed/stored on Mahindra personnel's own device i.e., mobile phones, laptops, tablets etc.
  - The Data Protection Team should implement the organizational and technical measures across Mahindra as detailed in '**Annexure A**' for the protection of personal data and to protect against risks such as data loss, unauthorized access, modification, destruction, disclosure, and misuse of Personal data.
  - The Internal Data Privacy Team / Infosec Team should be accountable to ensure to the effectiveness of organizational and technical measures.

- **System Acquisition, Development and Maintenance**
  - The Internal Data Privacy Team / Infosec Team should be consulted prior to making any changes on Mahindra processing systems affecting the collection, processing, or storage of personal data.
  - The Business Owners/Privacy champions should ensure that personal data is backed up prior to carrying out maintenance/change implementation on any systems hosting personal data to avoid any data loss.

- **Access Management**
  - Unique passwords that contain letters in both upper and lower cases, numbers, and special keys, and are ten or more characters in length.

- Effective control of Authentication, Authorization and Accounting through personalized and unique user identifications and secure authentication process.
- Access to personal data, where possible, should be provided to individual users. Where data is provided to a group of users, mechanisms shall be put in place to ensure that any changes (addition, deletion, or modification) to the personal data can be attributed to the user making the changes, hence demonstrating accountability.
- Access rights should be reviewed on a periodic basis to identify and de-provision excess rights to users who no longer require access to personal data.
- Secure mechanisms should be implemented for providing remote access to systems and applications processing personal data.

- **Authorization**
  - Administrative access to systems used for processing personal data should be strictly controlled and limited to authorized personnel. Activities of system administrative and system operator activities should be logged and monitored.
  - All logging facilities and log information should be protected from unauthorized access.
  - All the asset containing personal information should be protected from unauthorized access and be made available all the time.

- **Physical and Environmental Security**
  - Restriction of access rights to office buildings, data centres and server rooms should be provided to the minimum necessary.
  - Effective control of access rights should be implemented through an adequate locking system.
  - Measures for the prevention and detection of unauthorized access and access attempts shall be implemented (e.g., regular review of burglary protection of the doors, gates and windows, alarm systems, video surveillance, security guards, security patrol).

- **BYOD/Mobility/Portable devices**
  - Personal data shall not be collected/processed/stored on Mahindra personnel's personal device i.e., mobile phones, tablets, laptops, etc.
  - Employees shall exercise complete caution while using portable devices for managing personal data.
  - Employees shall protect such devices against loss or theft and shall immediately report any such instances to the IT Helpdesk.

## 6.8 Recover

- **Business Continuity (Availability of Personal data)**
  - Mahindra should make personal data available to all Data Principals upon request.
  - Mahindra should maintain processes, procedures, and controls to ensure the required levels of availability of personal data during adverse situations.
  - Mahindra should maintain backup of personal data to ensure its availability. When multiple copies of personal data are maintained (as backup), mechanisms such as pseudonymization of personal data and encryption of backup data shall be adopted, as feasible, to ensure personal data protection.

## 6.9 Monitoring and compliance

- **Internal Compliance Monitoring**

- The Internal Data Privacy Team / Infosec Team should review processing activities periodically to identify opportunities for data minimization, storage limitation and purpose limitation.
- The Business Owners should identify the personal data critical to their areas and shall ensure the access rights to such data are strictly controlled.
- The Data Privacy Team should conduct periodic self-assessments **(See 'Annexure C')** or due diligence of third parties to demonstrate compliance to privacy requirements.
- The Internal Data Privacy Team / Infosec Team should have the rights to monitor any computer system, network system and storage device, or personal data (stored, or in transmission), if required, as per applicable privacy laws and regulations. Such monitoring shall be carried out as preventive measures to detect any fraudulent activity and should not be a privacy violation to any employee and should be carried out after obtaining appropriate approvals.

- **Regulatory Compliance Monitoring**
  - The Internal Data Privacy Team / Infosec Team should identify the compliance review/audit requirements based on the applicable privacy laws and regulations and conduct periodic privacy compliance reviews to ensure that all the applicable privacy requirements are being implemented.
  - The Internal Data Privacy Team / Infosec Team should review any complaints/ grievances raised by the Data Principals or the Data Fiduciary to identify indications of any unlawful processing of personal data.
  - The Internal Data Privacy Team / Infosec Team should review any non-conformities identified as a part of the audit and monitor the same to closure and present the results of the privacy compliance review/audit to the Board of Directors/Management.

## 7. Measures & KPIs

| SN. | KPI | KPI Details | Accountable |
|---|---|---|---|
| **1** | Accuracy of Personal Data | No. of records updated to hold accurate personal data | Internal Data Privacy Team / Infosec Team |
| **2** | Handling of Data Principal Requests | No. of Data Principal requests on which assistance was provided | Operations Team |
| | | No. of Data Principal requests responded and closed | Internal Data Privacy Team / Infosec Team |
| **3** | Reporting Breaches | No. of data breaches reported to the Internal Data Privacy Team / Infosec Team | Data Breach Response team |
| | | No. of data breaches reported to the Board | Internal Data Privacy Team / Infosec Team |
| **4** | Diligence on 3rd party vendors | No. of data protection agreement signed with 3rd party vendors with whom personal data is shared | Legal Team |
| | | No. of Data Principal requests where assistance of 3rd party vendors was requested | Legal Team |
| **5** | Conducting Privacy Audits | No. of privacy audits conducted in every department to ensure compliance with privacy requirements | Internal Data Privacy Team / Infosec Team |

| | | | |
|---|---|---|---|
| **6** | Training & Awareness | No. of training and awareness sessions conducted across Mahindra | Company Office for Data Privacy |
| | | No. of training and awareness sessions attended | All Staff |

## 8. Contact Details

If you have any comments, questions, or concerns about any of the information in this Policy, or any other issues relating to the Processing of Personal Data by Mahindra, please contact Internal Data Privacy Team / Infosec Team in the first instance.

<<Relevant Team Name>>

Email id: privacy@mahindra.com

## 9. Exception

- Exceptions shall not be universal but shall be agreed on a case-by-case basis, upon official request made by the information owner. These may arise, for example, because of local circumstances, conditions or legal reason existing at any point of time.
- Exceptions to the Information Security Policy and Procedures may have to be allowed at the time of implementation of these policies and procedures or at the time of making any updating to this document or after implementation on an ad hoc basis based on business or a specific and a peculiar manifestation of circumstances which could be of temporary or permanent in nature.
- All exceptions during implementation shall be submitted by the concerned person responsible for implementation. These shall be submitted through an Exception Form and sign-off on the same shall be maintained including ad-hoc requests.
- The ISC shall review all exceptions every year for validity and continuity.
- M&M shall also list parameters to ensure that before acquiring new applications or other software and hardware, the set of applicable policies and guidelines shall be matched with the available security mechanisms of the product to ensure that the product has the necessary features. If not, then exceptions shall be approved before acquiring the desired product. Similarly, while developing new applications, the necessary security policies and guidelines must be incorporated in the application or exceptions shall be obtained for the same from the Information Security Team.

## 10. Disclaimer

- M&M reserves all rights and is the exclusive owner of all intellectual property rights over this information security policy and procedure document. This information security policy and procedure document shall not, either in part or in full, be reproduced, published, copied, displayed, distributed, transferred, stored into any media (external storage devices), and/or captured or transmitted through by any means (electronic, digital, mechanical, photocopying, recordings, video and film or photographs and otherwise) by any person without prior written consent from the Information Security Team of M&M's. The information security policy and procedure document is meant to be published on the intranet of M&M's and/or any other forum as decided by the management of M&M. Anything not specifically stated in this information security policy and procedure document shall not be considered as implied in any manner.
- For any clarifications related to this information security policy document with respect to its interpretation, applicability and implementation, please write to infosec@mahindra.com.

# Annexures

## Annexure A - Security Controls

| S.No | List of security controls | Description |
|---|---|---|
| 1 | **Logical Access Control** | Restricted access controls have been implemented i.e. only personnel requiring access is provided access to the personal data |
| 2 | **Physical Access Control** | Restricted access controls have been implemented where personal data is stored in physical files, documents, servers and accessible to personnel |
| 3 | **Data Masking (Encryption)** | Encryption is implemented at the database level or at the attribute level depending on the sensitivity of the personal data |
| 4 | **Data Masking (Anonymization)** | Anonymization is implemented to de-identify the personal data and de-link from other related attributes |
| 5 | **Data Masking (Pseudonymization)** | Pseudonymization is implemented to de-link the personal data from the data principal's identity |
| 6 | **Data Masking (UAT Data)** | Data is masked in the UAT environment if personal data is stored or copied from production to UAT instance for testing purposes |
| 7 | **Privilege Access Management** | Privilege access management is implemented for privilege user accounts to monitor the access to personal data by privileged users |
| 8 | **Application Security and VAPT** | Periodic Application security and Vulnerability assessment and penetration testing is conducted to identify vulnerabilities in the system processing personal data |
| 9 | **Log Management** | Logs related to access, security and other critical events are captured and logged |
| 10 | **Secure Data Disposal** | Personal data that should not be retained for more than the defined retention period or that needs to be disposed off is disposed securely using a tool/technology or a method |
| 11 | **Audit Trail** | Audit trails are enabled for access to applications and database where personal data is stored either by Mahindra personnel or third parties access to personal data |
| 12 | **IT Infra Disaster Recovery** | Availability of the infrastructure storing personal data has a DR plan and strategy |
| 13 | **Secure Backup** | Secure backup is maintained of all databases storing personal data securely |
| 14 | **DLP / Endpoint Protection** | DLP and Endpoint protection is implemented to detect unauthorized access and transfer of personal data |
| 15 | **SOC/ SIEM** | SOC/SIEM monitoring is carried out to detect data breach incidents related to personal data |

| | | |
|---|---|---|
| 16 | **Privacy Trainings** | All company's employees/staff and especially personnel dealing with personal data undergo privacy trainings |

## Annexure B - Data Principal rights mapping to Legitimate use

| LEGITIMATE USE | | DATA PRINCIPAL RIGHTS | | | | | |
|---|---|---|---|---|---|---|---|
| | | **Right of grievance redressal** | **Right to Access Information** | **Right to Correction** | **Right to Erasure** | **Right to Nominate** | **Right to withdraw consent** |
| | **Consent** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | **Contract** | ✓ | ✓ | ✓ | ✓ | ✓ | **X** |
| | **Legal** | ✓ | ✓ | ✓ | **x** | ✓ | **X** |
| | **Public Interest** | ✓ | ✓ | ✓ | **x** | ✓ | **X** |

## Annexure C - Privacy Audit Checklist

Privacy_Audit_Checklist.xlsx

## Annexure D – Privacy Risk Register

Privacy_Risk_Register_Template_v1.xlsx