DATA HANDLING AND PROTECTION POLICY

1. Document Control

1.1. Information

Title	Classification	Version	Status
Data Handling and Protection Policy	Confidential	1.0	

1.2. Review, Verification and Approval

Name	Title	Date	Signature
Abhilash Mazumder	CTO		
Shaikh Faizan	DPO		

2. Policy Overview

2.1. Purpose

GREAT MANAGER RESEARCH & CONSULTANCY PRIVATE LIMITED to limit access to information and information processing facilities, ensure authorized user access and to prevent unauthorized access to systems and services, make users accountable for safeguarding their authentication information, and prevent unauthorized access to systems and applications.

2.2 Change, Review and Update

This policy shall be reviewed once every year unless the owner considers an earlier review necessary to ensure that the policy remains current. Changes of this policy shall be exclusively performed by the GMI Information Security team and approved by Management. A change log shall be kept current and be updated as soon as any change has been made.

3. Policy Statements

The following subsections present the policy statements in 7 main aspects:

- General Policy Requirements
- Personal Data Protection
- Rights of Data Subjects
- Privacy by Design Principle
- Transfer of Personal Information
- Privacy Notice

3.1 General Policy Requirements

Based on the data management, governance, and personal data protection strategy and plan, the GMI must develop a plan for safeguarding personal data that fulfils operational and strategic personal data protection requirements. The plan should include a roadmap outlining activities and milestones aimed at achieving and maintaining full compliance with the Personal Data Protection Policy issued by the Organisation. It should also specify the necessary resources and budget for achieving full compliance with the Personal Data Protection Policy.

All possible options for data subjects must be identified and their implicit or explicit consent obtained regarding the collection, usage, or disclosure of their data.

Disclosure of personal data to external parties should be limited to specific purposes outlined in the privacy notice for which the data subject has provided implicit or explicit consent.

Processing of personal data should be restricted to the purposes specified in the privacy notice, retaining it as long as necessary to achieve those purposes or as required by the laws, regulations, and policies in the Nation. Safe disposal methods should be employed to prevent leakage, loss, misappropriation, misuse, or unauthorized access.

Privacy controls and mechanisms should include appropriate technical means, which should be assessed by the GMI.

Personal data should be protected throughout its acquisition, transfer, processing, and disposal stages.

Collection of personal data should be minimized to the extent necessary to fulfil the specified purposes in the privacy notice.

The GMI is responsible for identifying, documenting, and obtaining approval for the storage of personal data based on the purposes for which it was collected and will be used. In cases where data collection is necessary, the reasons should be clarified, including the need for collection, categorization of personal data, business requirements, and the purpose of collecting each category of personal data.

3.1.1 Personal data should be accurately and fully retained in relation to the specified purposes outlined in the privacy notice.

3.1.2 Personal data should not be used for training or research purposes.

3.1.3 Regular review of personal data should be conducted, and data should be deleted as per operational requirements or the expiration of the retention period.

3.1.4 An initial assessment of personal data protection should be carried out by the GMI to evaluate the existing personal data protection environment. The assessment should include at minimum:

3.1.4.1 Identification of types of personal data.

3.1.4.2 Location and method of storing personal data.

3.1.4.3 Current processing and uses of personal data.

3.1.4.4 Challenges of personal data protection in compliance with the issued Personal Data Protection Policy by the Organisation.

3.1.5 Data hosting should comply with the regulations set by the Company Authority to ensure that data remains within the Nation, either on the Company's servers or with national cloud service providers.

3.1.6 The GMI is required to store and process personal data exclusively within the India. This requirement must be included in contracts or related documents with external parties. If the need arises to share personal data with a foreign entity, approval from the Organisation must be obtained.

3.1.7 The GMI within the GMI should conduct internal audits to monitor compliance with personal data protection rules. The results of these audits should be documented in a report submitted to the Data Protection Officer in the Company. In cases of non-compliance, corrective actions should be taken and reported to the regulatory authority and the Organisation.

3.1.8 In cases where data management tasks are outsourced by the GMI to external parties, compliance of the external party or any subsequent contracts they may engage in to process personal data should be verified in accordance with the personal data protection requirements of the Company.

3.1.9 The GMI should maintain an audit log for a reasonable period of no less than 24 months, which should be made available to the Organisation upon request in accordance with the Personal Data Protection Policy issued by the Organisation. The log should, at a minimum, include records of each data collection or processing activity related to any personal data.

3.1.10 Any changes or updates related to systems, laws, and regulations should be monitored and reflected in the Personal Data Protection Policy.

3.2 Personal Data Protection

3.2.1 Measures must be in place to ensure the ability to recover and access personal data promptly in the event of a physical or technical incident.

3.2.2 Data concealment and obfuscation techniques must be employed to safeguard personal data.

3.2.3 GMI must carry out effective testing and assessment of technical and organizational measures to ensure the security of personal data processing.

3.2.4 An annual risk assessment should be conducted for the operation and usage of information systems containing personal information. This assessment should encompass data collection, processing, storage, and transmission across all systems, whether performed manually or automatically. The risk assessment results should include at a minimum:

- Documentation
- Impact analysis and likelihood assessment
- Evaluation based on regulatory obligations and criticality.

3.2.5 Personal data should be sufficient, relevant, and limited to what is necessary for the intended processing purposes.

3.2.6 Personal data must be accurate, appropriate, and up to date. Appropriate measures should be taken to promptly rectify or correct inaccurate personal data relevant to the purposes.

3.2.7 If personal data is obtained from sources other than the data subject, the data subject should be informed. The GMI should also send a privacy notice to the data subject.

3.2.8 Appropriate security controls must be implemented to protect personal data from leakage, damage, loss, misappropriation, misuse, unauthorized access, alteration, or unauthorized modification – in accordance with guidelines issued by the Company Authority and the Organisation.

3.2.9 Administrative controls and technical measures adopted in the information security policies of the GMI should be employed to ensure personal data protection, including but not limited to:

3.2.10 Granting access rights to data based on roles to avoid overlapping responsibilities and minimize dispersion of authority.

3.2.11 Applying administrative and technical procedures that document the stages of data processing, allowing identification of the responsible user for each stage (usage logs).

3.2.12 Having affiliates engaged in data processing operations sign an undertaking to maintain data confidentiality and only disclose it as per the policies, procedures, regulations of the GMI, and relevant laws.

3.2.13 Selecting personnel engaged in data processing operations based on their integrity and responsibility, in accordance with the nature and sensitivity of the data and the access policy adopted by the Iissen.io.

3.3 Rights of Data Subjects

3.3.1 GMI must notify the data subject of the legal basis or actual need for collecting their personal data and the purpose thereof. Data must not be processed in a manner inconsistent with the purpose for which consent was given, whether implicit or explicit.

3.3.2 Data subjects have the right to withdraw their consent for the processing of their personal data at any time, unless there are legitimate reasons that require otherwise.

3.3.3 Data subjects have the right to access their personal data in order to review, correct, complete, update, or request the disposal of unnecessary portions. They are also entitled to obtain a clear copy of their personal data

3.3.4 Methods and mechanisms must be defined and provided through which data subjects can access their personal data for review, updating, and correction

3.4 Privacy by Design Principle

3.4.1 GMI must adopt the principle of privacy by design and ensure that privacy requirements are met in current or new systems and programs that collect or process personal data.

3.4.2 GMI must regularly conduct a privacy impact assessment for all systems that collect or process personal data. This assessment includes:

3.4.2.1 Applying principles of personal data protection.

3.4.2.2 Fulfilling responsibilities of the control unit.

3.4.2.3 Implementing security controls to protect personal information.

3.4.2.4 Ensuring the legal basis for processing personal data.

3.4.2.5 Guaranteeing the collection, use, processing, storage, and sharing of personal data according to authorized purposes specified in the privacy notice.

3.4.2.6 Adopting the privacy by design principle for all new or modified systems and processes.

3.4.3 The Head of Cybersecurity Management must implement appropriate techniques for identity concealment of data and encryption to protect personal data.

3.4.4 GMI must fulfil the following documentation requirements and make them accessible through data subjects' records regarding personal data processing activities:

3.4.4.1 Objectives of processing personal data.

3.4.4.2 Processing activities conducted on personal data.

3.4.4.3 Processing categories of personal data.

3.4.4.4 Agreements and mechanisms for transferring personal data to and from other organizations after obtaining consent or a request from the data subject.

3.4.4.5 Retention schedules for personal information.

3.4.4.6 Existing security controls to protect personal information.

3.5 Transfer of Personal Information

3.5.1 Any transfer of personal data must be based on the consent or request of the data subject.

3.5.2 Before transferring personal data outside the office, a privacy impact analysis must be conducted.

3.5.3 Appropriate notifications, including recipients' details and the purpose of each disclosure, must be sent to the data subject before transferring personal data to them. This notification should include the date, nature, and purpose of each disclosure, as well as the names and addresses of the recipients to whom the personal data has been disclosed.

3.5.4 Data protection measures must be ensured at the receiving party, including the following details:

3.5.4.1 Name of the organization and relevant details.

3.5.4.2 Objectives of processing personal data.

3.5.4.3 Categories of individuals and processing of personal data.

3.5.4.4 Categories of recipients of personal data.

3.5.4.5 Agreements and mechanisms for transferring personal data.

3.5.4.6 Retention schedules for personal information.

3.5.4.7 Relevant technical and organizational controls implemented in the office.

3.6 Privacy Notice

3.6 1 The GMI must identify, document, approve, and implement the requirements for providing a privacy notice to the data subject regarding the following:

3.6.2 Activities that affect the privacy of personal data, including collection, use, sharing, retention, and disposal.

3.6.3 How the GMI uses personal data and the consequences of exercising or not exercising those options.

3.6.4 The right to access and correct personal data if necessary.

3.6.5 The types of personal data collected by the GMI and the purpose for which that information is collected.

3.6.6 How the GMI uses personal data.

3.6.7 If the GMI shares personal data with external entities, the categories of those entities and the purposes of such sharing.

3.6.8 How individuals can access or obtain their personal data.

3.6.9 The GMI must identify, document, approve, and implement the requirements for providing a privacy notice to the data subject regarding the following:

3.6.10 Activities that affect the privacy of personal data, including collection, use, sharing, retention, and disposal.

3.6.11 How the GMI uses personal data and the consequences of exercising or not exercising those options.

3.6.12 The right to access and correct personal data if necessary.

3.6.13 The types of personal data collected by the GMI and the purpose for which that information is collected.

3.6.14 How the GMI uses personal data.

3.6.15 If the GMI shares personal data with external entities, the categories of those entities and the purposes of such sharing.

3.6.16 How individuals can access or obtain their personal data.

3.6.17 How personal data is protected.

3.6.18 The duration for which personal data will be stored.

3.6.19 The right to request access, correction, erasure, or restriction of processing of personal data, as well as the right to object to its processing and the right to data portability.

3.6.20 The right to withdraw consent at any time.

3.6.21 The right to lodge complaints, ask questions, or express concerns to the GMI, and to file a complaint with the supervisory authority.

3.6.22 Whether the provision of personal data is legally required or contractually necessary, and if the data subject is obligated to provide personal data and has been informed of the potential consequences of not providing this data.

3.6.23 Changes in practices or policies affecting personal data or changes in activities affecting privacy, before or as soon as possible after the change.

3.6.24 The GMI must inform the data subject before lifting processing restrictions if processing is restricted by the data subject. Personal data must only be processed, excluding storage, with the consent of the data subject.

3.6.25 The GMI must notify any correction, erasure, or processing restriction of personal data to each recipient to whom the data has been disclosed, and the controller must inform the data subject upon request.

3.7 Privacy Violations

3.7.1 The GMI must develop, document, approve, and implement a privacy incident response plan and execute it when necessary.

3.7.2 The GMI must prepare and document the necessary procedures for managing and addressing privacy violations. This includes specifying tasks and responsibilities related to the specialized team and determining the cases in which regulatory authorities and the GMI should be notified, based on the administrative hierarchy and the severity of the impact.

3.7.3 If a privacy violation occurs, the GMI must follow the incident response plan and procedures and notify the Head of Cybersecurity Management.

3.7.4 The GMI must develop, document, approve, and implement procedures for notifying data subjects about privacy violations without delay.

3.7.5 The GMI must notify the regulatory authority in case of a personal data breach within the timeframe specified in the Data Protection Policy issued by the Organisation. The specified timeframe for notification is 72 hours.

3.7.6 The GMI must document the process of managing data breaches for immediate management and resolution of personal data protection violations. This documentation is crucial for determining the functions and responsibilities of the relevant team. The data breach management process should include, at a minimum:

3.7.6.1 Conducting an incident review

3.7.6.2 Formulating an immediate response to the incident

3.7.6.3 Implementing a permanent corrective action

3.7.6.4 Conducting tests on corrective measures to verify the effectiveness of personal data protection solutions.

3.8 Awareness and Training

3.8.1 The GMI must develop a comprehensive awareness and training program, document it, gain approval for it, implement it, and regularly update it. The purpose of this program is to ensure that affiliates are knowledgeable about their responsibilities and privacy procedures. It includes basic privacy training as well as targeted privacy training based on the roles of affiliates who are responsible for personal data or engaged in activities involving personal data.

3.8.2 The training program should include, at a minimum, the following topics:

3.8.2.1 The importance of protecting personal data, its impacts, and consequences for the organization and/or data subjects.

3.8.2.2 Definition of personal data.

3.8.2.3 Data subjects' rights.

3.8.2.4 Responsibilities of the GMI and data subjects.

3.8.2.5 Notifications: When to notify the organization or data subjects, and how to handle requests for collection, processing, and sharing of personal data.

4. Information Deletion

4.1 Policy Statement:

The purpose of this policy is to establish guidelines and procedures for the secure and timely deletion of information. This policy ensures that obsolete, redundant, or unnecessary information is appropriately identified, securely deleted, and disposed of to prevent unauthorized access and mitigate risks associated with data retention.

4.2 Policy Overview:

4.2.1 Identification of Information: Designated personnel shall regularly review and identify information that is no longer required for business purposes or legal obligations. This includes both electronic and physical records.

4.2.2 Classification of Information: Information shall be classified based on its sensitivity and regulatory requirements to determine the appropriate deletion method and retention period.

4.2.3 Deletion Procedures: Secure deletion methods, such as overwriting, degaussing, or physical destruction, shall be employed to ensure irretrievable removal of information from storage media and systems.

4.2.4 Retention Periods: Information shall be retained only for the duration necessary to fulfil business needs, legal obligations, or regulatory requirements. Once the retention period expires, information shall be promptly deleted.

4.2.5 Documentation and Records: Records of information deletion activities, including the date, method, and reason for deletion, shall be maintained in accordance with record management policies and regulatory requirements.

4.2.6 Employee Training and Awareness: Personnel handling information deletion activities shall receive training on proper deletion procedures, data classification, and the importance of secure information disposal.

4.2.7 Monitoring and Auditing: Regular audits and monitoring shall be conducted to ensure compliance with information deletion policies and procedures. Any deviations or non-compliance shall be promptly addressed and remediated.

4.3 Responsibilities

- Information Security Officer/ Chief Technology Officer: Responsible for overseeing the implementation and enforcement of the information deletion policy.
- IT Department: Responsible for implementing technical measures for secure information deletion.
- Data Owners: Responsible for identifying obsolete or unnecessary information within their respective areas.
- Employees: Responsible for adhering to information deletion procedures and reporting any concerns or deviations.

5 Data Masking Policy

5.1 Policy Statement

The purpose of this policy is to establish guidelines and procedures for the masking of sensitive data to protect confidentiality and privacy. Data masking ensures that sensitive information is obfuscated or replaced with realistic but fictional data, reducing the risk of unauthorized access or disclosure during testing, development, or data analysis activities.

5.2 Policy Overview

5.2.1 Identification of Sensitive Data: Designated personnel shall identify and classify sensitive data within the organization, including personally identifiable information (PII), financial data, healthcare records, and intellectual property.

5.2.2 Data Masking Techniques: Appropriate data masking techniques, such as substitution, shuffling, encryption, or tokenization, shall be applied based on the sensitivity and regulatory requirements of the data.

5.2.3 Masking Rules and Policies: Masking rules and policies shall be established to govern the masking process, including the types of data to be masked, the masking techniques to be used, and access controls for masked data.

5.2.4 Masking Procedures: Data masking shall be performed prior to the release or sharing of sensitive data for testing, development, or analysis purposes. Masked data shall replace original sensitive data in non-production environments.

5.2.5 Access Controls: Access to masked data shall be restricted to authorized personnel with a legitimate business need. Access controls shall be implemented to prevent unauthorized viewing or manipulation of masked data.

5.2.6 Data Masking Environment: A secure environment shall be established for data masking activities, with controls in place to prevent unauthorized access, tampering, or leakage of masked data.

5.2.7 Monitoring and Auditing: Regular monitoring and auditing of data masking activities shall be conducted to ensure compliance with masking rules and policies. Any deviations or unauthorized access shall be promptly investigated and remediated.

6 Data Leakage Prevention Policy

6.1 Policy Statement

The purpose of this policy is to establish guidelines and procedures for the prevention of data leakage or unauthorized disclosure of sensitive information. This policy aims to safeguard confidential data from unauthorized access, transmission, or disclosure both within and outside the organization.

6.2 Policy Overview

6.2.1 Identification of Sensitive Data: Designated personnel shall identify and classify sensitive data within the organization, including personally identifiable information (PII), financial data, intellectual property, and confidential business information.

6.2.2 Data Classification: Sensitive data shall be classified based on its sensitivity and regulatory requirements to determine the appropriate level of protection and access controls.

6.2.3 Access Controls: Access to sensitive data shall be restricted to authorized personnel with a legitimate business need. Role-based access controls (RBAC) shall be implemented to ensure that users have access only to the data necessary for performing their job functions.

6.2.4 Encryption: Sensitive data shall be encrypted both at rest and in transit to prevent unauthorized access or interception. Strong encryption algorithms and key management practices shall be employed to protect data confidentiality.

6.2.5 Data Loss Prevention (DLP) Solutions: DLP solutions shall be implemented to monitor and control the movement of sensitive data within the organization's network and endpoints. DLP policies shall be configured to detect and prevent unauthorized data transfers or leakage.

6.2.6 Endpoint Security: Endpoint security measures, such as firewalls, antivirus software, and endpoint detection and response (EDR) tools, shall be deployed to prevent unauthorized access to sensitive data stored on endpoint devices.

6.2.7 Employee Training and Awareness: All employees shall receive training on data security best practices, including the importance of safeguarding sensitive information, recognizing potential data leakage risks, and reporting incidents or suspicious activities.

6.2.8 Incident Response: Procedures shall be established for responding to data leakage incidents, including incident reporting, containment, investigation, and remediation. Incident response plans shall be regularly tested and updated to ensure their effectiveness.

GREAT MANAGER INSTITUTE
Our pathways. Your potential.

END OF POLICY