Information Security & Privacy Management System (ISPMS)

Version: 1.1

Policy

Document Information

Category	Information
Document	Information Security and Privacy Policy
Version	1.1
Identifier	E4U_002_Information Security and Privacy Policy_1.1
Status	Approved
Author(s)	ISPMS
Reviewer(s)	CEO
Approver(s)	CEO
Creation Date	01/03/2023
Issue Date	10/03/2023
Effective Date	10/03/2023
Control Status	**CONTROLLED**
Distribution	TLP: WHITE
Disclaimer	This document contains general information. Do not copy this document without prior approval from EMINENT4U.

Document Revision History			
Author(s)	**Date**	**Version**	**Description**
ISPMS team and Compliance Officer	25/04/2023	1.0	Continual Improvement and data subjects updated

Table of Content

Contents

1. Information Security & Privacy Policy

1.1 Purpose

This Policy is to create, maintain and continually improve the Information Security & Privacy Management System (ISPMS) and to adhere to ISPMS practices in compliance with best practices required for information security and privacy needs of the clients.

Eminent4u works within the framework of the Local Government, while fulfilling the contractual obligation of the clients and regulatory bodies. This is to ensure the protection of data, privacy, and protection of personally identifiable information. This information security and privacy policy ensures that Eminent4u complies with data protection law and follows good practices.

1.2 Scope

This policy applies to all assets which process critical data & information as well as privacy related areas which includes systems, networks, applications, locations, and users of Eminent4u or suppliers under contract to it.

1.3 Objective

The objectives of Information Security, Privacy, and Data Protection Policy are to preserve:

1. Implementation of ISMS and PIMS Framework
2. Increase information security and data privacy awareness at organizational level to 90%
3. Reduction in security and privacy breaches by 10%
4. Ensure timely mitigation of all identified risks related to ISMS and PII
5. Perform successful DR/BCP drill

1.4 Principles

- **Confidentiality (C)** - Access to data shall be confined to those with appropriate authority.
- **Integrity (I)** – Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification.
- **Availability (A)** – Information shall be available and delivered to the right person, at the time when it is needed.
- **Privacy (P)** – Information and infrastructure shall be protected.

1.5 Policy

To achieve the objectives Eminent4u will ensure the following policy:

- Business requirements for availability of information and systems are met.
- Confidentiality, Integrity, Availability, and Privacy (CIAP) of the information is maintained throughout the process flow.
- All legal, regulatory, contractual, and business are meeting ISMS and Privacy requirements.
- All corporate assets (tangible/intangible) are in a physically and logically secure environment.
- Risks to all corporate assets (tangible/intangible) are assessed against all risks appropriate.
- Contingency and risk mitigations are defined.
- Human resources are provided with a conducive work environment.
- All personnel are trained in information security and privacy procedures awareness.
- Physical, logical, and remote access to all the corporate assets (tangible/intangible), information and physical locations are monitored and controlled.
- Business continuity plans are established, maintained, tested, and periodically updated as needed.
- Each team that handles personal PII or client data must ensure that it is handled and processed in line with this policy and data protection principles.
- The organization should address the following key areas.
    - Keeping the board updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies.
    - Arranging data protection training and advice for the people covered by this policy.
    - Checking and approving any contracts or agreements with third parties that may handle the company's or client's sensitive data.
    - Ensuring all systems, services and equipment used for storing data (cloud) meet acceptable security standards.
    - Performing scheduled checks and scans to ensure security hardware and software is functioning properly.
    - Evaluating any third-party services, the company is considering using to store or process data. For instance, cloud computing services provided by Clients.
    - Employees should keep all data secure, by taking sensible precautions and following the guidelines
    - Strong passwords must be used, and they should never be shared.
    - Personal and client data should not be disclosed to unauthorized people, either within the organization or externally.
    - When not required, the papers or files should be kept in a locked drawer or filing cabinet.
    - Employees should make sure papers and printouts are not left where unauthorized people could see them.
    - Data should be protected by strong passwords and never shared between employees.
    - Data should be backed up frequently and those backups should be tested regularly, in line with the organization backup policy stated in operations policy.

- If an individual contacts the company requesting critical and confidential information, this is called subject access request, obligations of Subject requests to be followed.
    - Subject access requests from the individuals should be made by email and they should be approved by the relevant department and log to be maintained.

- Continual Improvement:
    - Eminent4u to review and monitor the compliance and ISPMS performance in the organization.
    - Eminent4u conducts yearly Management Review Meetings to review and evaluate policies, procedures and any risks assessments.
    - Eminent4u segregate duties of Management, individuals and departments to ensure continuity and improvisation of ISMPS System implementations.
    - Eminent4u to ensure regular training and refreshers courses and sessions for the staff related to information security and privacy.
    - Related personnel (internal) to remain up to date with any latest standard updates and requirements.
    - Continuous monitoring, evaluating, measuring and fixing on the objectives of ISMS and PIMS.

This policy has been approved by the company management and shall be reviewed by the management in the annual management review meeting.