GREY MATTER SOLUTIONS

V.1

INFORMATION SECURITY POLICY

DOCUMENT NUMBER:

ISO 27001:2022(ISMS)

DOCUMENT CONTROL:

Type of Information	Description
Document Title	Information Security Policy
Document Number	GMS_POL_2025_0002_V1.0
Document Status	Approved//In-Review//**Draft**
Document Classification	Internal
Release Date	Jan 02, 2026
Reviewed by	Director of Business Development
Document Custodian	Director of Business Development
Approved By	President

DOCUMENT CHANGE HISTORY LOG:

Information Security Policy					
Rev.no	**Rev. Date**	**Description**	**Prepared by**	**Approved by**	**Signature**
1.0	Jan 02, 2026	Initial Release	Director of Business Development	President	E.S.

TABLE OF CONTENTS

1. Purpose:

The purpose of the Information Security Management System (ISMS) in Grey Matter Solutions is to ensure the continuity and protection of the business processes and information assets that are considered within the ISMS scope (stated in the scope document). The information security needs and objectives are stated in this document to minimize the impact of security incidents on the operations of Grey Matter Solutions.

2. Scope:

The **Information Security Management System (IMS)** at Grey Matter Solutions encompasses the **Information Security Management System (ISMS)**. It applies to all organizational units, services, systems, and locations involved in delivering secure, high-quality IT services and solutions. The ISMS ensures the confidentiality, integrity, and availability of information, consistent delivery of IT services, aligned with ISO/IEC 27001.

3. Definition:

4.1 Availability – Property of being accessible and usable upon demand by an authorized entity.

4.2 Asset – Anything that has value to the organization.

4.3 Confidentiality – Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

4.4 Integrity – Property of accuracy and completeness.

4.5 ISMS – Information Security Management System is the part of the overall management system and required to establish, implement, maintain and continually improve the information security of the organization.

4. Corporate ISMS Policy:

The Information Security Management System of Grey Matter Solutions intends to ensure:

4.1 Integrity of all business processes, information assets, and supporting IT assets and processes, through protection from unauthorized modification, guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. The unauthorized modification or destruction of information could have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals;

4.2 Availability of all business processes, information assets, and supporting IT assets and processes to authorized users when needed, ensuring timely and reliable access to and use of information. The disruption of access to, or use of, information or an information system could have a serious adverse effect on organizational operations, organizational assets, or individuals;

4.3 Confidentiality of all information assets (information is not disclosed to unauthorized persons through deliberate or careless action). Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

The unauthorized disclosure of information could have a limited adverse effect on organizational operations, organizational assets, or individuals;

4.4 All IT-enabled processes and stakeholders shall follow the rules and regulations or circulars published in the organization;

4.5 All audit trails and logs, as decided by the Management Information Security Forum (MISF), shall be maintained and monitored by Grey Matter Solutions.

4.6 All operational and system changes shall be monitored closely; these shall adhere to the change management process;

4.7 Grey Matter Solutions complies with the laws, regulations, and contractual obligations which are applicable to the organization in general and in particular to its ISMS;

4.8 All applicable information security requirements are satisfied;

4.9 Continual improvement of the information security management system.

5. Applicability:

This policy applies to all Manager and staff of Grey Matter Solutions, contractors, and third-party employees under contract, who have any access to, or involvement with, the business processes, information assets, and supporting IT assets and processes covered under the scope of ISMS.

6. Responsibility:

Grey Matter Solutions shall ensure that all activities required to implement, maintain and review this policy are performed. All personnel, regarded as included in the ISMS scope, must comply with this policy statement and its related security responsibilities defined in the information security policies and procedures that support the corporate information security policy. All personnel, even if not included in the ISMS scope, have a responsibility for reporting security incidents and identified weaknesses, and to contribute to the protection of business processes, information assets, and resources of Grey Matter Solutions.

7. Enforcement:

Grey Matter Solutions holds the right to monitor the compliance of its personnel to this policy. Manager and staff of Grey Matter Solutions, contractors, and third-party employees, who fail to comply with this policy, may be subjected to appropriate disciplinary actions.

8. Ownership and Revision:

This policy statement is owned by the Board of Directors of Grey Matter Solutions who has delegated this task to the Chief Information Security Officer (CISO). This policy shall be revised once a year by the CISO and every time that the Board of Directors of FCI, or the MISF, decides to do so.