VERMEG Information Security Policy Statement & Objectives

VERMEG is committed to safeguarding the confidentiality, integrity and availability of its information assets at all times to enhance trust, reliability and confidence among all stakeholders, including end users, suppliers, customers and regulatory authorities.

This policy applies to all aspects of information security, including physical security, and covers all forms of information, whether stored on-premises or in cloud environments, transmitted across networks, printed or written on paper, stored on computers or removable devices, or communicated verbally or via telephone

Everyone at VERMEG is responsible for protecting the security of information. Understanding and accepting these responsibilities is crucial to the effective implementation of this policy.

The overall objectives for VERMEG Information Security are the following:

- Ensure confidentiality, integrity and availability of information assets, through cost effective and consistent information security infrastructure.
- Maintain an Integrated Management System (IMS) covering both Information Security Management System (ISMS) and Privacy Information Management System (PIMS).
- Protect clients' Personally Identifiable Information (PII) by implementing security best practices and ensuring compliance with applicable privacy laws, regulations, and industry standards.
- Provide a mechanism to detect and mitigate risks associated with information security domain.
- Ensure that all staff adhere to information security and privacy principles by providing training during their onboarding and regularly updating and assessing their knowledge through ongoing training and awareness programs.
- Strengthen operational resilience strategy through robust business continuity planning and regular assessments to ensure the ability to withstand and recover from disruptions, while providing assurance to top management, stakeholders, and customers about its effectiveness.
- Ensure compliance with the applicable laws, regulations, and contractual obligations in the domain of information security, privacy, Artificial intelligence and digital operational resilience.
- Safeguard personnel, information, equipment, IT infrastructure, and company facilities through effective physical security measures.
- Ensure the ethical, responsible and secure use of Artificial Intelligence (AI).
- Commit to the continual improvement of the IMS to address evolving threats, regulatory changes, and advancements in technology.

The success of the Integrated Management System IMS will be evaluated based on its ability to meet these overall objectives.

Mousser JERBI

COO

DocuSigned by:
182F92EE905140A...