INFORMATION SECURITY MANAGEMENT SYSTEM POLICY

Purpose

Sofstica Solutions (PVT) Ltd. (Sofstica) is committed to safeguarding the confidentiality, integrity, and availability of all data and information assets. We recognize that effective information security management is fundamental to preserving client trust, meeting contractual obligations, and ensuring business continuity

Scope:

The scope of Sofstica's Information Security Management System (ISMS) is in alignment with ISO/IEC 27001:2022 and forms the cornerstone of our strategic security posture.

Policy Statement

Sofstica Solutions is committed to safeguarding the confidentiality, integrity, and availability of all data and information assets. We recognize that effective information security management is fundamental to preserving client trust, meeting contractual obligations, and ensuring business continuity. Our Information Security Management System (ISMS), in alignment with ISO/IEC 27001:2022, forms the cornerstone of our strategic security posture. Key tenets of our policy include:

Risk-Based Information Security Management: We identify and evaluate information security risks and establish controls to mitigate these risks. Our approach involves continuous risk assessment and monitoring to adapt to the rapidly changing threat landscape.

Data Protection and Privacy: We are committed to ensuring the protection of all data, including personal, customer, and employee data. Compliance with applicable data protection laws is strictly enforced.

Access Control and Authorization: Information access is restricted to authorized personnel only, based on business needs and the principle of least privilege. Robust mechanisms for authentication, authorization, and logging are enforced to prevent unauthorized access and data breaches.

Incident Response and Resilience: Our incident response process ensures swift detection, containment, and resolution of information security incidents. We conduct regular tests of our business continuity and disaster recovery plans to maintain operational resilience.

Awareness and Training: All employees receive regular training and updates on information security risks, policies, and responsibilities to ensure vigilance and adherence to security protocols.

Compliance with Legal and Contractual Obligations: Our ISMS is designed to comply with applicable legal, regulatory, and contractual requirements to ensure the protection and management of information security risks.

Communication and Review: This policy is communicated across all levels of the organization, contractors, and relevant stakeholders and is reviewed periodically, or when significant changes occur, to maintain its continued relevance and adequacy.

APPROVED