Information Security Policy

1. Overview & Purpose

Xavor Pakistan (Pvt) Ltd. (**XAVOR**) recognizes that protecting information assets is critical to business continuity, operational resilience, and maintaining stakeholder trust.

The objective of this policy is to establish a structured framework for securing our Information Security Management System (**ISMS**), minimizing the impact of security incidents, and ensuring the confidentiality, integrity, and availability of all data assets.

2. Scope

This policy applies to:

- All employees, management, and technical staff of XAVOR.
- All information assets, systems, applications, networks, and digital processes owned or managed by XAVOR.
- All third parties, vendors, and contractors interacting with XAVOR information or systems.

3. Our Core Security Principles

In alignment with **ISO 27001:2022**, XAVOR Top Management is committed to implementing, maintaining, and continually improving our ISMS. We adhere to the following core tenets:

Risk Management: Proactively identify, evaluate, and reduce security threats.
Compliance: Meet all legal, regulatory, and contractual requirements.
Access Control: Limit data access through role-based permissions and unique user credentials.
Asset Protection: Protect endpoints, block unauthorized software, and keep systems patched.
Continual Improvement: Regularly review security controls and strengthen our infrastructure.

- **Risk-Driven Security:** We continuously identify security risks, assess their potential impact, and implement robust mitigation controls.

- **Access Management:** Information access is strictly restricted based on job responsibilities. Every user must use unique credentials; shared accounts are prohibited.
- **Endpoint & System Integrity:** Company systems must run approved security solutions with automated updates. The installation of unauthorized, unlicensed, or peer-to-peer (P2P) software is strictly prohibited.
- **Legal & Contractual Alignment:** We safeguard internal and third-party information assets in strict accordance with legal, regulatory, and ethical guidelines.

4. Policy Governance & Enforcement

- **Review Cycle:** This policy is reviewed **Bi-annually**, or when significant changes occur in business operations, regulatory environments, or technological landscapes, ensuring its ongoing adequacy and effectiveness.
- **Availability:** This document is communicated across the organization and made available to relevant internal and external interested parties.
- **Enforcement:** Compliance is mandatory. Any violation of this policy may result in disciplinary actions, up to and including termination of employment or contract, and legal action where applicable.

Reference: ISO/IEC 27001:2022, Clause 5.2 (Information Security Policy)