XAVOR PAKISTAN (PVT) LTD.

INFORMATION SECUITY POLICY

POLICY

Document Information:

GRC Hub System will automatically track the “Document Information”

Amendment History:

GRC Hub System will automatically track the “Amendment History”

Contents

1 OVERVIEW

Xavor Pakistan (Pvt) Ltd. is a software development and IT consulting organization with over 30 years of experience delivering mission-critical solutions to leading enterprises and Fortune 500 clients across global markets. Our service portfolio spans custom application development, AI and data services, enterprise platform implementation, managed cloud services, DevOps, and GRC advisory. The nature of these services requires that information assets, including client data, intellectual property, system configurations, and service delivery infrastructure, be protected with the highest degree of diligence and care.

The organization recognizes that its customers, partners, regulators, and other interested parties have legitimate expectations regarding the confidentiality, integrity, and availability of information entrusted to Xavor. The evolving threat landscape, increasing regulatory requirements across international markets, expanding use of cloud-based and AI-driven delivery models, and the growing sophistication of cyber threats make a structured, risk-based approach to information security not only a business necessity but a fundamental organizational obligation.

2 PURPOSE

The purpose of this Information Security Policy (ISP) is to ensure the protection of information assets within Xavor Pakistan (Pvt) Ltd. and associated environments by minimizing the risk of security incidents and reducing their potential impact.

Xavor Pakistan (Pvt) Ltd. shall maintain the confidentiality, integrity, and availability of its information assets to prevent adverse effects on operations and professional standing.

This policy shall support the strategic direction of the organization and provide a framework for establishing and achieving information security objectives.

3 SCOPE

This policy applies to:

* All employees, management, and technical staff of Xavor Pakistan (Pvt) Ltd.
* All third parties, contractors, and vendors who interact with Xavor Pakistan (Pvt) Ltd. information or systems
* All information assets, systems, applications, networks, and processes owned, managed, or operated by Xavor Pakistan (Pvt) Ltd.

All applicable personnel shall comply with this policy, related procedures, and company code of conduct.

4 REFERENCE

- ✓ ISO 27001:2022, Clause 5.2

5 ABBREVIATIONS

Abbreviation	Acronyms
XVR	Xavor Pakistan (Pvt) Ltd.
IC	Infrastructure & Cloud
POL	Policy
ISMS	Information Security Management System
MR	ISO Management Representative
NA	Not Available
ISO	International Organization for Standardization

6 POLICY

All information shall be treated as Xavor Pakistan (Pvt) Ltd. asset. Unauthorized access, disclosure, duplication, modification, diversion, loss, misuse, or theft of information is strictly prohibited.

Top Management of Xavor Pakistan (Pvt) Ltd. is committed to establishing, implementing, maintaining, and continually improving the Information Security Management System (ISMS) in accordance with ISO 27001:2022, and shall ensure alignment with the organization's strategic direction.

Following principles and requirements shall apply:

i. Xavor Pakistan (Pvt) Ltd. shall identify, assess, and manage information security risks based on their impact and likelihood.
ii. Information assets, including third-party information, shall be protected according to their sensitivity, classification, and business requirements.
iii. Access to systems, applications, and information shall be granted only to authorized users based on job responsibilities and business needs.
iv. Users shall use unique credentials and comply with defined password requirements, including password complexity and periodic updates.
v. Shared user accounts shall be prohibited unless specifically authorized and controlled.
vi. Unauthorized, unapproved, unlicensed, or prohibited software and tools shall not be installed or used on company systems.
vii. Critical systems shall be protected using approved security controls, including antivirus, endpoint protection, security patches, and automatic updates.
viii. Information assets shall be protected in compliance with applicable legal, regulatory, contractual, and organizational requirements.
ix. Any activity that violates company policies, legal requirements, or information security practices shall be strictly prohibited.
x. Information security roles and responsibilities shall be defined, assigned, and communicated throughout the organization.

xi. Adequate resources, infrastructure, technology, and competent personnel shall be provided to establish, operate, maintain, and improve the ISMS.
xii. Compliance with this policy and the effectiveness of security controls shall be monitored, measured, and reviewed regularly.
xiii. Security controls and risk treatment measures shall be reviewed periodically to ensure their continued suitability and effectiveness.
xiv. This policy shall provide a framework for establishing and achieving information security objectives and shall be communicated to relevant interested parties.
xv. The ISMS and this policy shall be reviewed bi-annually or whenever significant changes, incidents, risks, audit findings, or management review outcomes occur to ensure continual improvement.

7 ENFORCEMENT

Any employee or third party found to be in violation of this policy shall be subject to disciplinary action**,** which may include termination of employment or contract, and/or legal action as applicable.