Data Privacy and Security Policy

# Introduction

The Data Privacy and Security Policy establishes the framework for protecting company and customer data against unauthorized access, misuse, loss, and disclosure. This policy ensures compliance with applicable laws such as GDPR, CCPA, and other industry-specific regulations, while promoting a culture of privacy awareness across the organization.

# Scope

This policy applies to all employees, contractors, consultants, partners, and third-party vendors who handle or process company or customer data in any form.

It covers all types of data, including personal information, financial data, intellectual property, and other sensitive business information.

# Data Classification

Data must be classified into four categories: Public, Internal, Confidential, and Restricted.

Public data is openly available without restrictions. Internal data is limited to employees for operational use.

Confidential data includes customer records, financial reports, and strategic plans. Restricted data is the highest classification, covering trade secrets, encryption keys, and protected health information.

Employees must apply appropriate controls and protections according to the classification.

# Access Control

Access to sensitive data must follow the Principle of Least Privilege (POLP), ensuring individuals have only the access necessary to perform their duties.

Multi-factor authentication (MFA) is mandatory for accessing systems containing Confidential or Restricted data.

Access rights must be reviewed quarterly, and any unnecessary privileges must be revoked promptly.

# Data Handling Procedures

Confidential and Restricted data must be encrypted both at rest and in transit using approved encryption standards.

Portable devices such as laptops, USB drives, and external hard drives must be encrypted and protected with strong passwords.

Data sent via email must be encrypted when containing sensitive information, and recipients must be verified before sending.

# Incident Response

All employees must report suspected or actual data breaches immediately to the Information Security Team via the Incident Reporting System.

A preliminary investigation will be conducted within 24 hours, followed by containment, mitigation, and recovery measures.

The company will notify affected parties and regulators within the legally required timelines.

# Training and Awareness

All employees must complete mandatory privacy and security training within the first 30 days of employment and annually thereafter.

Training includes phishing awareness, password hygiene, secure data handling, and incident reporting procedures.

# Compliance and Enforcement

Non-compliance with this policy may result in disciplinary action, including termination, legal action, and financial penalties.

Periodic audits will be conducted to ensure compliance, and violations will be documented with corrective actions taken.