Tavio Corporate Policy Directory

1.0 Introduction

This document is the official directory of Tavio's corporate policies. Its purpose is to provide all employees, contractors, and relevant stakeholders with a clear, at-a-glance summary of each policy's core function, ensuring easy navigation and understanding of the company's governance framework.

2.0 Policy Summaries

This collection of policies is of strategic importance to the company's success and integrity. These documents collectively define the operational, security, ethical, and compliance standards that govern Tavio's activities. Adherence to these policies is mandatory and fundamental to protecting the company, its employees, and its clients, thereby fostering a secure and trustworthy business environment.

Application Change Management
Tavio has adopted this policy to provide an overview of the application change management program of the Company.

Asset Management
This policy outlines the safeguarding measures for Tavio's intellectual property (IP) and assets. It applies to both Tavio's and others' IP, as well as all technology assets, including systems, hardware, and data sets directly used in business operations.

Bring Your Own Device (BYOD)
The Bring Your Own Device (BYOD) Policy governs personally owned devices used for work purposes.

Business Continuity and Disaster Recovery (BCDR)
This policy outlines the requirements Tavio has set to ensure the least downtime possible to services and systems provided to customers and that support critical business functions.

Cloud and Network Security
This policy governs the management of Tavio's cloud hosting environment where it hosts its web application. This policy must be followed by the individuals assigned to managing or accessing this environment, excluding those who only access via Tavio's online application interface.

Code of Conduct
This policy outlines the behavior, ethics, and security standards all employees and contractors must follow at Tavio.

Cryptography
To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information. This policy establishes requirements for the use and protection of cryptographic keys and cryptographic methods throughout the entire encryption lifecycle.

Data Management
This policy defines practices to secure and manage data throughout its lifecycle. It includes data encryption, data retention, data classification, disaster recovery, data backups, key management, data flow management, and non-repudiation practices.

Endpoint and Configuration Management
This policy provides guidance for all endpoints that access other systems and data, including workstations, servers, and cloud computing devices, including all endpoints owned, leased, or otherwise controlled by Tavio.

Governance
This policy explains Tavio's information governance program. It gives an overview of the organization's mission and objectives for privacy and security and outlines the key roles and responsibilities related to data privacy and information security.

Human Resource Security
This policy outlines Tavio's human resources requirements concerning information security and data privacy at each stage of employment or engagement.

Identity and Access Management (Access Control)
This policy defines the requirements of Tavio, governing acceptable methods of determining a user's identity and how access control is managed for these identities on networks and services.

Incident Reporting
This policy aims to guide all employees and contractors of Tavio on how to identify, report, and assist in the prompt resolution of any security or privacy incidents.

Incident Response for Security Team
This policy provides guidelines for swift resolution of security and privacy incidents within Tavio.

Information Security
The purpose of this policy is to communicate our information security policies and outline the acceptable use and protection of Tavio's information and assets.

Mobile Device Management
This Mobile Device Management (MDM) policy outlines the guidelines and standards for the use of mobile devices (e.g., smartphones, tablets, laptops) that are owned or used by employees of Tavio to access company data and systems.

Operations Security
To ensure the correct and secure operation of information processing systems and facilities.

Privacy Policy
This privacy policy explains how Tavio processes information that can be used to directly or indirectly identify an individual (“Personal Data”) collected through use of its website and platform in accordance with the applicable regulation and standards.

Privacy Program
This policy covers handling personal information collected by Tavio or its customers, including data that is stored, processed, or otherwise shared with Tavio, its systems, employees, and contractors.

Remote Working
This policy outlines how Tavio protects information accessed, processed, or stored at remote working sites.

Risk and Compliance Management
This policy governs Tavio’s risk management program. This policy specifies when to perform risk assessments of Tavio equipment, systems, and data systems.

Secure System Development
This policy outlines Tavio’s secure software development strategies and provides an overview of the organization’s approach to developing software securely.

Third-Party Management
This policy governs Tavio’s third-party vendor management activities.

Vulnerability and Patch Management
This policy includes the activities, tools, and strategies that are employed to identify, monitor, report, and resolve vulnerabilities in systems and software.

This directory serves as a high-level guide to Tavio's governance framework. All employees and contractors are accountable for reading, understanding, and adhering to the full text of the policies relevant to their specific roles and responsibilities to ensure company-wide compliance.