Organizational IT Security Policy Proposal Plan

1. Introduction

This document outlines the proposed IT security policies for [Organization Name]. The objective is to define processes, roles, and controls that safeguard the confidentiality, integrity, and availability of organizational information assets.

2. Purpose

The purpose of this policy plan is to establish and communicate the required standards for IT security, mitigating risks from cyber threats and ensuring compliance with regulatory requirements.

3. Scope

This policy applies to all employees, contractors, and third-party partners who access, use, or manage the organization's IT assets and data.

4. Policy Statements

4.1 Access Control

- User accounts shall require strong authentication and be reviewed regularly.
- Access to sensitive data must be restricted based on roles and responsibilities.

4.2 Data Protection

- All personal and organizational sensitive data must be encrypted in transit and at rest.
- Backups are to be performed regularly and stored securely.

4.3 Network Security

- Use of firewalls, intrusion detection and monitoring systems is mandatory.
- Remote access must use secure VPN technologies.

4.4 Incident Response

- All security incidents must be reported promptly to IT management.
- Incident response procedures shall be documented, tested, and updated routinely.

4.5 Acceptable Use

- Organizational IT resources are to be used only for authorized business purposes.
- Prohibited activities include unauthorized software installation and data sharing.

5. Roles and Responsibilities

- **IT Department:** Implement technical controls, monitor threats, coordinate incident response.
- **Management:** Support policy enforcement, allocate necessary resources.
- **Staff & Users:** Comply with policies, report security concerns.

6. Policy Review

This policy shall be reviewed annually or upon significant operational or regulatory changes.

7. Approval

____
Date: ______________________
Name & Title: ______________________