IT Acceptable Use Policy

# Introduction

This policy defines the acceptable, safe, and responsible use of company IT assets, including computers, networks, mobile devices, and software. It safeguards company data from misuse, unauthorized access, and cyber threats.

# Scope

Applies to all employees, contractors, and third parties who use company-provided IT systems.

Covers on-site, remote, and cloud-based access.

# Acceptable Use

Use IT resources for work-related tasks and authorized personal use only.

All software installations must be approved by IT.

# Prohibited Use

Accessing unauthorized systems, distributing malware, or engaging in illegal activities is strictly prohibited.

Storing company data on unapproved personal devices is forbidden.

# Data Security

Users must use strong passwords, enable MFA, and avoid sharing login credentials.

Sensitive files must be encrypted, and backups maintained according to IT policy.

# Monitoring and Compliance

The company reserves the right to monitor and audit IT usage to detect security violations.

Violations may result in disciplinary action, including termination and legal proceedings.