📝 Acceptable Use Policy

Version: 1.0
Effective Date: April 2025

Purpose

This policy outlines acceptable use of company-owned and authorized personal devices and systems, to ensure the protection of information assets and technology infrastructure.

Scope

This policy applies to all employees, contractors, and third-party users who access company systems, data, or networks, whether onsite or remote, and whether using company-issued, CYOD (Choose Your Own Device), or BYOD (Bring Your Own Device) resources.

Policy

- All devices (company-issued or personal) used for business purposes must comply with company security standards, including antivirus, encryption, and auto-lock configurations.
- Credentials must not be shared or stored in unapproved locations. Use of MFA is required.
- Users shall not access, distribute, or store content that is illegal, offensive, or harmful.
- Installation of unauthorized software on any work-connected device is prohibited.
- Public Wi-Fi use requires connection through a company-approved VPN.
- Company systems shall not be used for personal financial gain or non-sanctioned commercial activity.

BYOD & CYOD Considerations

- Personal devices must be registered and approved before accessing internal systems.
- MDM (Mobile Device Management) tools may be deployed to ensure compliance.
- Users consent to limited monitoring on any personal device used for work.

Enforcement

Violations of this policy may result in revocation of access privileges, disciplinary action, or termination.