**Acceptable Use Policy (AUP)**

**Policy ID:** SEC-AUP-001  
**Version:** 1.0  
**Approval Date:** [Insert Date]  
**Next Review Date:** [Insert Date + 12 months]  
**Owner:** Chief Information Security Officer (CISO)  
**Applies To:** All employees, contractors, vendors, and authorized third-party users

**1. Purpose**

This policy outlines the acceptable use of organizational information systems, networks, applications, data, and computing resources. It is designed to protect employees and the company from exposure to security risks, legal liabilities, and operational disruptions resulting from improper use of technology.

**2. Scope**

This policy applies to all individuals and entities who access, use, or manage any information system or data asset owned or operated by the company. This includes:

* Company-issued devices (e.g., laptops, phones)
* Company-managed cloud services (e.g., email, SaaS tools)
* Internal networks and wireless connections
* Remote access environments

**3. Policy Statements**

**3.1 Authorized Use**

* Information systems must be used solely for legitimate business purposes.
* Personal use must be incidental, infrequent, and not conflict with business operations or policies.
* All access and activity must be conducted through company-managed tools and approved channels.

**3.2 Prohibited Activities**

* Users may not engage in unauthorized access, port scanning, penetration testing, or attempts to bypass system controls.
* Users must not access, create, or distribute materials that are discriminatory, harassing, illegal, or offensive.
* Users may not use company assets for personal commercial gain, political campaigns, or non-approved charitable causes.

**3.3 Data Handling**

* Confidential and sensitive data must be accessed only when required and must not be stored on unauthorized devices or platforms.
* Use of personal USB drives or external storage media is prohibited unless explicitly authorized and encrypted.

**3.4 Software and Services**

* Installation of unapproved software, browser extensions, or cloud services (e.g., Dropbox, Google Drive) is prohibited.
* Only company-authorized IT staff may configure systems or install software.

**3.5 Authentication and Access**

* Users must follow password and MFA requirements defined in the Access Control Policy.
* Sharing passwords or access credentials is strictly prohibited.
* All user activity may be logged and monitored for compliance and security.

**3.6 Physical and Remote Access**

* All unattended systems must be locked when not in use.
* Remote access must occur through company-approved tools such as VPN or MDM-enforced SSO.

**3.7 Incident Reporting**

* Users must immediately report any suspected security incident, data breach, or policy violation to the security team.
* Failure to report may result in disciplinary action.

**4. Roles and Responsibilities**

| **Role** | **Responsibility** |
| --- | --- |
| All Users | Understand, acknowledge, and comply with this policy |
| HR | Include AUP in onboarding; retain signed acknowledgments |
| IT/Security | Enforce technical restrictions, monitor usage, investigate abuse |
| Managers | Ensure team compliance and escalate violations |

**5. Compliance and Enforcement**

Violations of this policy may result in disciplinary action, up to and including termination of employment or contract, as well as legal action. The company reserves the right to monitor and audit use of systems to ensure compliance.

**6. Review and Maintenance**

This policy shall be reviewed annually by the CISO or designated security officer. Updates must be approved by executive leadership and communicated to all users.

**7. Framework Mappings**

| **Standard** | **Clause / Control** |
| --- | --- |
| **NIST SP 800-53 Rev. 5** | AC-1 (Access Control Policy), PL-4 (Rules of Behavior), AU-6 (Audit Review), IR-6 (Incident Reporting) |
| **ISO/IEC 27001:2022** | A.5.1 (Policies for Information Security), A.5.6 (Acceptable Use of Assets), A.6.1.1 (InfoSec Responsibilities) |

**8. Acknowledgment**

All users must sign an acknowledgment form indicating that they have read, understood, and agreed to comply with this policy. HR is responsible for record retention.