**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 Acceptable Use Policy establishes the proper use of [COMPANY NAME] technology and data resources. It supports operational integrity, regulatory compliance, and the protection of organizational assets.

**2. Scope**

Applies to all personnel who use, access, or manage company-owned or managed systems and data, including:

* Workstations, laptops, servers, and mobile devices
* Networks, cloud platforms, email, and SaaS tools
* VPN, remote access, and authentication systems
* Storage, backup, and removable media

**3. Policy Statements**

**3.1 Acceptable Use**

* Users must use technology resources only for authorized business purposes. *(ISO 27001 A.5.10, NIST AC-1)*
* Access is limited to users with a legitimate need based on their job role. *(NIST AC-6, ISO 27001 A.5.18)*
* Devices must be locked or logged off when unattended. *(NIST AC-11, ISO 27001 A.5.18)*
* Users must safeguard company data and follow data classification rules. *(NIST MP-4, ISO 27001 A.5.12)*

**3.2. Prohibited Activities**

* Users must not attempt to access unauthorized systems or perform port scanning or penetration testing without approval. *(NIST AC-6, SI-4; ISO 27001 A.5.11)*
* Users must not engage in activities that are illegal, harassing, or damaging to the company’s reputation. *(NIST PL-4; ISO 27001 A.5.1)*
* Downloading or distributing pirated, obscene, or malicious content is prohibited. *(NIST SI-7; ISO 27001 A.5.11)*

**3.3 Internet and Email Use**

* Email and internet services must be used in accordance with business needs. *(NIST AC-17, ISO 27001 A.5.13)*
* Transmission of confidential or sensitive information must use encryption and approved communication methods. *(NIST SC-12, SC-13; ISO 27001 A.5.13, A.5.24)*
* Spam, phishing, and suspicious content must be reported and deleted immediately. *(NIST IR-6, SI-4; ISO 27001 A.5.25)*

**3.4 Software and Device Use**

* Users may only install software that is explicitly authorized by IT. *(NIST CM-7; ISO 27001 A.5.14)*
* Use of personal devices (BYOD) must comply with security standards and be pre-approved. *(NIST AC-19; ISO 27001 A.6.2)*
* USB drives and removable media must be encrypted and approved before use. *(NIST MP-7; ISO 27001 A.8.3)*

**3.5 Monitoring and Privacy**

* All system activity may be logged, monitored, and audited for compliance and security purposes. *(NIST AU-6; ISO 27001 A.5.20)*
* Users should have no expectation of privacy when using company-owned resources. *(NIST PL-4; ISO 27001 A.5.1)*

**3.6 Security and Incident Reporting**

* All suspected policy violations, data breaches, or unusual activity must be reported to the Security Team immediately. *(NIST IR-6; ISO 27001 A.5.25)*
* Users must cooperate during incident investigations and resolution activities. *(NIST IR-7; ISO 27001 A.5.26)*

**4. Roles and Responsibilities**

|  |  |
| --- | --- |
| All Users | Comply with AUP and report security issues. |
| Managers | Ensure team awareness and address violations. |
| IT/Security Team | Monitor systems; investigate and respond to incidents. |
| HR | Distribute policy and retain signed acknowledgments. |

**5. Compliance and Enforcement**

Noncompliance with 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 policy adherence.

**6. Review and Maintenance**

This policy shall be reviewed annually by the CISO or designated security officer and updated in response to legal, regulatory, or operational changes. Updates must be approved by executive leadership and communicated to all users.

**7. Acknowledgment and Agreement**

I acknowledge that I have read and understand [COMPANY NAME]’s Acceptable Use Policy. I agree to comply with its terms and understand that any violation may result in disciplinary action and/or legal consequences.

|  |  |  |
| --- | --- | --- |
| **Name (Print):**  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | **Signature:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | **Date:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **Manager/HR (Print):**  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | **Signature:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | **Date:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |