Justin Lew

Acceptable Use Policy (AUP)

1. Purpose

The purpose of this Acceptable Use Policy (AUP) is to establish guidelines for the appropriate and secure use of the organization’s information systems, networks, and resources. This policy aims to protect the confidentiality, integrity, and availability of company assets while ensuring compliance with legal and regulatory requirements.

2. Scope

This policy applies to all employees, contractors, vendors, and third-party users who access the organization's systems, networks, or data. It also applies to any device, whether company-owned or personally owned, that connects to the company network or accesses company data.

3. Policy Statement

3.1 Acceptable Use

- Users must access company resources only for authorized business purposes.
- Users must maintain strong passwords that meet complexity requirements and follow identity verification protocols.
- Personal use of company resources should be minimal and must not interfere with business operations.
- All network traffic and system activities are subject to monitoring and logging to ensure compliance.
- Users must follow data handling procedures for different data classifications, including Public, Internal, Confidential, and Restricted data.

3.2 Prohibited Activities

- Unauthorized access, modification, or destruction of data.
- Use of company resources for illegal activities, including but not limited to hacking, unauthorized software installations, and data breaches.
- Sharing login credentials, passwords, or authentication tokens.
- Downloading or distributing copyrighted material without proper authorization.
- Connecting unauthorized devices, such as personal USB drives or unapproved cloud storage, to company systems.
- Circumventing or attempting to bypass security controls such as firewalls, intrusion detection/prevention systems, or endpoint protection.

3.3 Security Measures

- Employees must report any suspicious activity or potential security incidents to the Security Operations Center (SOC) immediately.
- Devices accessing company networks must be secured with up-to-date antivirus software, endpoint protection solutions, and security patches.
- Multi-factor authentication (MFA) is required for all remote access and privileged account access.
- All company data stored on personal devices must be encrypted and protected per company security guidelines.
- Access control measures, such as role-based access control (RBAC), must be enforced to ensure users only have access to the data necessary for their job functions.

3.4 Monitoring & Enforcement

- The organization reserves the right to monitor, audit, and log user activities on company networks and systems.
- Violations of this policy will be investigated by the SOC, IT Security, and HR teams.
- Consequences of non-compliance include disciplinary action up to and including termination of employment, legal action, and potential criminal prosecution.
- The SOC maintains an **incident escalation matrix**, defining response procedures and timeframes for different severity levels of policy violations.

4. Compliance & Regulatory Considerations

This policy aligns with industry best practices and regulatory frameworks, including:

- **ISO 27001**: Information Security Management System
- **NIST 800-53**: Security and Privacy Controls for Federal Information Systems
- **GDPR**: General Data Protection Regulation (if applicable)
- **HIPAA**: Health Insurance Portability and Accountability Act (for healthcare-related data)
- **CMMC**: Cybersecurity Maturity Model Certification (for organizations working with the U.S. Department of Defense)
- **SOC 2**: Trust Services Criteria for Security, Availability, and Confidentiality

5. Roles & Responsibilities

- **Employees & Users**: Adhere to this policy and report security incidents.
- **IT Security Team**: Implement and enforce security measures.
- **SOC Analysts**: Monitor, investigate, and respond to security incidents.
- **Management**: Ensure policy compliance and provide necessary training.
- **Third-Party Vendors & Contractors**: Comply with contractual security obligations and adhere to the AUP.

- **Security Compliance Team**: Conduct audits, track policy adherence, and ensure regulatory alignment.

6. Incident Response & SLA Considerations

- All security incidents must be reported to the SOC within 15 minutes of detection.
- Incidents are classified based on severity (Critical, High, Medium, Low), and response times are governed by predefined **Service Level Agreements (SLAs)**.
- The SOC follows **Incident Response Playbooks** to ensure rapid containment and mitigation of threats.
- Post-incident analysis and reports are required for all **High** and **Critical** severity incidents to prevent recurrence.

7. Review & Updates

This policy will be reviewed annually or as needed to reflect changes in technology, legal requirements, or business operations.

Approval & Acknowledgment
By accessing company resources, users acknowledge they have read, understood, and agreed to abide by this Acceptable Use Policy.

Effective Date: (Date)
Last Reviewed: (Date)
Approved by: (Name/Title)