elevaite365

TECH THAT MATTERS

Elevaite365

Acceptable Usage Policy

Version 1.0

PURPOSE

This policy defines the acceptable and responsible use of the organization’s information systems, IT assets, and resources. It ensures alignment with the organization’s information security objectives, compliance with legal and regulatory standards, and safeguarding proprietary and sensitive information from unauthorized use or disclosure per the Information security policy of Elevaite365 (herein referred to as organization).

SCOPE

This policy applies to all users, including employees, contractors, vendors, and third parties, who access the organization’s IT assets, networks, or information systems. It encompasses all devices and environments, including organizational and personal devices used on-premises, remotely, or in hybrid configurations.

DEFINITION

- **Information Security Group (ISG):** The team overseeing the organization’s information security measures, including this policy.
- **Unacceptable Use:** Any activity that violates organizational policies or applicable laws while utilizing the organization’s resources.
- **IT Resources:** All hardware, software, networks, applications, and data owned or managed by the organization.
- **Blogging and Social Media Activities:** Public or semi-public communication platforms, including personal blogs, social media posts, and forums.
- **IT Resources:** Includes all hardware, software, systems, networks, applications, and data owned, managed, or accessed by the organization.
- **Unacceptable Use:** Any action that violates this policy, organizational standards, or applicable legal and regulatory requirements while utilizing IT resources.
- **Confidential Information:** Any data designated as proprietary or sensitive, including but not limited to trade secrets, intellectual property, Personally Identifiable Information (PII), and internal business communications.

RESPONSIBILITIES

1. **Information Security Group (ISG):**
    a. Ensure the enforcement of this policy.
    b. Regular training and awareness programs on acceptable use should be conducted.
    c. Monitor and audit IT resource usage for compliance.
2. **Department Heads and Managers:**
    a. Ensure their teams adhere to the policy.
    b. Approve exceptions and report violations promptly.
3. **End Users:**
    a. Comply with this policy when using organizational resources.
    b. Protect their credentials and promptly report any suspicious activity or policy violations.

POLICY

Acceptable Use

The organization’s IT resources must only be used for legitimate business purposes and in alignment with organizational goals, policies, and legal obligations. Acceptable use includes:

- Performing tasks and activities directly supporting the organization’s business operations and strategic objectives.
- Accessing, processing, and sharing information as required for job roles, ensuring compliance with data classification and handling policies.
- Using IT resources responsibly to prevent harm to the organization’s reputation, resources, or data.

Permissible Personal Use:

Personal use of IT resources is permitted on a limited basis, provided it:

- Does not interfere with work responsibilities or organizational productivity.
- Do not compromise system security, consume excessive resources, or violate this policy or applicable laws.

Unacceptable Use

The organization prohibits activities that misuse IT resources, jeopardize security, or violate ethical or legal standards. Below is an expanded list of prohibited activities.

1. **System and Network Activities**
    a. **Violation of Laws and Regulations**:
        i. Using IT systems to engage in any activity that violates local, state, national, or international laws.
        ii. Breaching intellectual property laws by using, copying, or distributing copyrighted content without proper authorization.
    b. **Introduction of Malicious Software**:
        i. Intentionally or negligently introducing malicious programs into organizational systems or networks, such as viruses, worms, ransomware, or spyware.
        ii. Engaging in phishing or other deceptive activities to compromise user credentials or systems.
    c. **Unauthorized Access and Hacking**:
        i. Attempting to bypass or compromise access controls, such as passwords, firewalls, or encryption protocols.
        ii. Using hacking tools or techniques to probe, scan, or exploit vulnerabilities in systems or networks.
    d. **Denial-of-Service and Disruption**:
        i. Engaging in activities intended to disrupt or deny access to IT systems, such as DoS or DDoS attacks.
        ii. Misusing bandwidth or system resources to degrade performance for legitimate users.
    e. **Negligence and Data Mismanagement**:
        i. Leaving devices or systems unattended without proper locking mechanisms.
        ii. Storing or transmitting sensitive data on unsecured devices, platforms, or networks.
        iii. Using public Wi-Fi to access or transmit sensitive information without a secure VPN.
2. **Email and Communication Systems**
    a. **Spam and Phishing**:
        i. Sending unsolicited emails (spam), chain letters, or advertisements through organizational accounts.
        ii. Using email systems to craft or disseminate phishing emails, whether internal or external.
    b. **Confidential Information Protection**:
        i. Transmitting sensitive or confidential information via email without encryption or prior authorization.
        ii. Auto-forwarding emails to external domains unless explicitly approved for business purposes.
    c. **Behavioral Violations**:
        i. Sending messages containing discriminatory, offensive, or harassing language.
        ii. Misrepresenting the organization or impersonating others in email communications.
    d. **Restrictions on Personal Use**:
        i. Using organizational email for non-work-related political activities, personal business ventures, or unauthorized solicitations.
        ii. Subscribing to non-work-related services, newsletters, or websites using organizational email.
3. **Social Media and Blogging**
    a. **Confidentiality and IP Protection**:
        i. Sharing organizational secrets, proprietary information, or internal documents on social media platforms.
        ii. Disclosing information about employees, customers, or vendors without prior approval.
    b. **Reputation Management**:
        i. Posting content that could harm the organization’s reputation or create legal or ethical conflicts.
        ii. Associating personal statements, opinions, or views with the organization unless officially authorized.
    c. **Ethical Online Conduct**:
        i. Engaging in online activities that could be considered unethical, such as trolling, hate speech, or participating in illegal forums.
4. **Data and Document Handling**
    a. **Data Classification Adherence**:
        i. Users must adhere to data classification policies and appropriately handle public, confidential, and sensitive data appropriately.
        ii. All sensitive information must be encrypted during storage and transmission.
    b. **Document Security**:
        i. Physical documents containing sensitive information must be securely stored when not in use.

        ii. Digital documents must not be stored on personal devices unless explicitly authorized and adequately encrypted.

5. **BYOD (Bring Your Own Device)**
    a. **Device Registration**:
        i. All personal devices used for accessing organizational resources must be registered with and approved by IT.
        ii. Devices must have up-to-date security configurations, including anti-malware protection and encryption.
    b. **Prohibited Activities**:
        i. Storing unencrypted organizational data on personal devices.
        ii. Connecting personal devices to the corporate network without prior approval and compliance checks.
6. **Physical and Environmental Security**
    a. **Device Security**:
        i. Employees must lock workstations and devices when leaving their workspace.
        ii. Lost or stolen devices must be reported immediately to the Information Security Group (ISG).
    b. **Document Security**:
        i. Printed documents containing sensitive data must not be left unattended in public or shared workspaces.
        ii. All discarded sensitive documents must be shredded or disposed of securely.

Advanced Controls for Sensitive Activities

1. **Two-Factor Authentication (2FA)**:
    a. All systems containing sensitive data must require 2FA for access.
2. **Logging and Monitoring**:
    a. All sensitive data or critical systems access must be logged and subject to regular audits.
3. **Access Control**:
    a. Access to IT resources must follow the principle of least privilege, granting users only the access necessary for their roles.

Enforcement and Consequences

1. **Monitoring**:
    a. The organization monitors all IT resource usage to ensure compliance. This includes logging activities such as system access, email usage, and internet browsing.
2. **Consequences**:
    a. Violations may result in:
        i. Temporary or permanent loss of access to IT resources.
        ii. Disciplinary action, including termination of employment or contractual agreements.
        iii. Legal action if the violation constitutes a criminal offense.

Exceptions and Policy Evolution

1. **Exceptions**:
    a. Any exceptions to this policy must be approved by ISG and documented with a clear rationale.
2. **Policy Updates**:
    a. This policy will be reviewed annually and updated to reflect technological changes, regulations, and organizational objectives.

Version Details

Version	Version Date	Description of changes	Created By	Approved By	Published By
Version 1.0	-	Initial Release	Borhan	-	-