TECH THAT MATTERS

Elevaite365

Mobile Device and Teleworking Policy

Version 1.0

PURPOSE

This policy aims to define the requirements for the appropriate use and configuration of mobile computing and teleworking. These measures are necessary to protect data belonging to Elevaite365 (herein referred to as “the Organization”) and its clients from unauthorized access or disclosure.

SCOPE

This policy applies to the organization and its employees, contractors, and third parties. It applies equally to all individuals with authorized access to any of the Organization’s information assets, regardless of the device or location from which access is obtained.

DEFINITION

1. **Mobile Device:** A handheld computer, usually small enough to be carried in one hand. Examples include laptops, tablets, smartphones, and similar devices.
2. **Teleworking:** All forms of work conducted outside of the office, including non-traditional work environments such as telecommuting, flexible workplaces, remote workplaces, and virtual work environments. Teleworking safeguards protect client information, intellectual property, and other sensitive data.
3. **ISMS**: Information Security Management System

RESPONSIBILITIES

Information Security Group (ISG)

1. **Policy Implementation:** Responsible for implementing this policy in coordination with the IT team.
2. **Awareness and Training:** Ensure all employees understand and undertake their responsibilities regarding teleworking.
3. **Compliance Monit responsibilitiesoring:** Monitor adherence to this policy and report non-compliance to top management.
4. **Incident Response:** Manage and respond to security incidents related to mobile devices and teleworking.

IT Team

1. **Technical Support:** Provide technical support and ensure all mobile devices meet security requirements.
2. **Configuration Management:** Ensure proper configuration of mobile devices and teleworking setups to comply with this policy.
3. **Security Controls Implementation:** Implement and maintain security controls such as encryption of mobile devices, antivirus, and firewall protections on mobile device computing.

Policy

General Use of Mobile Devices and Removable Media

1. **Business Necessity:** Mobile devices and removable media must only be used when there is an identified business need relevant to job responsibilities and approved by the top they have been engaged
2. **Data Storage Restrictions:** Under no circumstances should client data be stored on mobile devices that are not owned or managed by the Organization or do not meet the security requirements outlined in this policy.
3. **Authorized Devices:** Only authorized mobile devices and removable media may be used for the Organization’s business purposes.

Mobile Devices and Removable Media Protection Controls

1. **Access Protection:** Access to mobile devices or any applications used to access organizational information must be protected using a password that meets the requirements outlined in the Access Control Policy.
2. **Antivirus Software:** Any mobile device capable of using antivirus software must comply with the Antivirus Policy.
3. **Firewall Activation:** Where supported, firewall software should be installed and activated on mobile devices.
4. **Encryption Requirements:**
    a. **Confidential Data Storage:** Mobile devices and removable media used to transmit store, or process data categorized as “Confidential” must encrypt the entire device or provide a separate, encrypted container for all organizational data.
    b. **Data Transmission Encryption:** All confidential data transmitted to or from the device must be encrypted using methods approved by the IT Head by the Encryption and Key Management Policy.

5. **Security Patches:** Establish and implement procedures to ensure that all security patches and updates relevant to mobile devices or installed applications are promptly applied in compliance with the Patch and Vulnerability Management Policy. Automation of the patching process is recommended where possible.
6. **Prohibition of Stored Credentials:** Storage of user IDs and passwords that allow access to the Organization's network or systems on mobile devices is prohibited, except for approved password management software.
7. **Primary Data Source:** Mobile devices and removable media should not be used as the primary source. The primary copy of source data should reside only in the Organization-managed central repository to ensure controlled backup and security.
8. **Data Synchronization:** Mobile devices and removable media used to store data that is designated as "Confidential" must only synchronize data with Organization-owned workstations, laptops, or other approved devices.

Physical and Environmental Protection of Mobile Devices and Removable Media

1. **Device Ownership Responsibility:** The assigned owner of the device or media is responsible for its physical protection against loss, damage, abuse, or misuse.
2. **Return Protocol:** All Organization-owned mobile devices must have a method of return if lost.
3. **Device Security:** Mobile devices must not be left unattended and should be locked away or physically secured when not in use.
4. **Public Usage Care:** Exercise reasonable care when using mobile devices in public places to avoid accidental disclosure of information.
5. **Device Sharing Restriction:** Authorized mobile devices must not be shared with others without prior written approval from the IT Head.
6. **Data Removal Before Disposal:** Before disposing, all data must be removed from locally owned mobile devices used to synchronize organizational email or access company data; all data must contact the IT team to disable synchronization and assist in data removal.
7. **Device Return Upon Termination:** Employees terminating their relationship with the Organization must return any Organization-owned mobile devices by their last date of employment. Employees using personal devices for organizational access must ensure all organizational data is removed.
8. **Loss or Theft Reporting:** Any suspected the IT team must be immediately notified of any loss of a mobile device used with organizational systems or information must be immediate**ly**

Teleworking Requirements

1. **Protection of Teleworking Site:** Implement suitable protection of the teleworking site against theft, unauthorized disclosure, unauthorized remote access, and misuse of facilities.
2. **Authorization and Control:** Teleworking must be managed to authorize and control teleworking properly. Security arrangements and controls are in place.
3. **Equipment Usage:** Only Organization-owned equipment may be used to access the corporate network. If personal devices are used, they must comply with the BYOD Policy.
4. **Security Arrangements Compliance:** Teleworking activities are authorized only if security arrangements comply with the Information Security Policy.

Considerations for Teleworking
The following factors must be considered to ensure secure teleworking:

1. **Physical Security:** Evaluate the existing physical security of the teleworking site, including the building and local environment.
2. **Teleworking Environment:** Assess the proposed teleworking environment for security adequacy.
3. **Communications Security:** Ensure remote access to internal systems is secure, especially when handling sensitive information.
4. **Threat of Unauthorized Access:** Mitigate risks of unauthorized access from other individuals in the teleworking environment, such as family or friends.
5. **Protective Monitoring:** Implement results from the protective monitoring policy.
6. **Hardware and Software Support:** Ensure necessary software support and maintenance.
7. **Backup and Business Continuity:** Establish procedures for data backup and business continuity.
8. **Audit and Security Monitoring:** Conduct regular security audits and identify vulnerabilities.

Teleworking Security Measures

1. **Unattended Equipment Policy:** Equipment must not be left unattended and unsecured. Devices should be locked away when not in use or physically secured.

2. **Document Security:** Organizational documents must not be left unattended or unsecured. Implement a clear desk policy when leaving the working area.
3. **Device Ownership:** All devices remain the Organization's property and must only be used by authorized employees. Access by non-employees is strictly forbidden.
4. **Unauthorized Connections Prohibition:** Employees must not connect unauthorized equipment to Organization devices or use personal removable media on Organization equipment.
5. **Pre-Work Authorization:** Managers must ensure appropriate physical documents and IT security controls are in place before individuals begin teleworking.
6. **Home Security Measures:**
    a. **Asset Protection:** Protect assets entrusted to teleworkers.
    b. **Separation of Matters:** Maintain separation between personal and official matters.
    c. **Dedicated Workspace:** Designate a dedicated working area.
    d. **Clear Desk Policy:** Implement a clear desk policy to prevent unauthorized viewing of sensitive information.
    e. **Log Off Equipment:** Log off IT equipment when unattended, especially when connected to the Organization's systems.

Version Details

Version	Version Date	Description of changes	Created By	Approved By	Published By
Version 1.0	Aug 29 2025	Initial Release	Borhan	Linh	Borhan