TECH THAT MATTERS

Elevaite365

Physical Security Policy

Version 1.0

PURPOSE

The Physical Security Policy defines the requirements for granting, controlling, monitoring, and removing physical access to the Elevaite365 (herein referred to as “the Organization”) facilities. This policy protects the Organization’s physical assets, sensitive information, and personnel from unauthorized access, theft, damage, and other physical threats.

SCOPE

This policy applies to the organization and all individuals with authorized access to any of the Organization’s facilities, including employees, contractors, and third-party service providers.

DEFINITIONS

- **ISG**: Information Security Group
- **CISO**: Chief Information Security Officer – The executive overseeing the Organization’s information and data security strategies and implementations.
- **Access Control**: Security techniques and policies regulate who can view or use resources in a physical environment.
- **Restricted Facility**: Areas within the Organization’s premises that contain sensitive information, critical infrastructure, or valuable assets requiring enhanced security measures.
- **Visitor**: Any individual who does not have regular authorized access to the Organization’s facilities but requires temporary access for business purposes.
- **Access Card/Key**: Physical devices used to enter restricted areas within the Organization’s facilities.
- **Surveillance Cameras**: CCTV or other types of cameras monitor and record activities within and around the Organization’s facilities.
- **Alarm Systems**: Systems designed to detect unauthorized access or other security breaches and alert security personnel.
- **Visitor Badge**: Temporary identification credentials are issued to visitors to access certain areas within the organization’s facilities.
- **Uninterruptible Power Supply (UPS)**: A device that provides emergency power to a load when the input power source fails, ensuring continuous operation of critical systems.

RESPONSIBILITIES

Information Security Group (ISG) and Chief Information Security Officer (CISO)

1. **Policy Implementation**: Develop and enforce the Physical Security Policy in collaboration with relevant departments.
2. **Monitoring and Compliance**: Conduct regular audits and inspections to ensure adherence to the policy and report non-compliance to top management.
3. **Training and Awareness**: Conduct training sessions to educate employees and contractors about best practices for physical security and their roles in maintaining security.
4. **Incident Response**: Coordinate responses to physical security breaches or incidents, including investigation and remediation efforts

Facilities Management Team

1. **Access Provisioning**: Manage the issuance and collection of access cards and keys. Ensure that only authorized personnel receive access based on their roles.
2. **Visitor Management**: Oversee visitor access protocols, including sign-in/out procedures and accompaniment by authorized personnel.
3. **Facility Inspections**: Conduct regular inspections of physical security measures, such as locks, surveillance systems, and access points, to ensure they are functioning correctly.
4. **Incident Reporting**: Promptly report any lost or stolen access cards/keys or suspicious activities to the ISG and IT team.

POLICY

Physical Access

1. **Documentation and Management**: Physical access to all the Organization's restricted facilities must be documented and managed through a centralized access control system.
2. **Proportional Protection**: All Information Resource facilities must be physically protected in proportion to the criticality or importance of their function.
3. **Access Justification**: Access to Information Resources facilities must be granted only to Organization personnel and contractors whose job responsibilities require access to that facility.
4. **Approval Process**: The process for granting card and/or key access to Information Resource facilities must include the approval of the person responsible for physical facility management.
5. **Access Agreements**: Everyone granted access rights to an Information Resource facility must sign the appropriate access and non-disclosure agreements.
6. **No Sharing Policy**: Access cards and/or keys must not be shared or loaned to others.
7. **Return of Access Devices**: Access cards and/or keys that are no longer required must be returned to the person responsible for Information Resource physical facility management. Cards must not be reallocated to another individual without proper return.
8. **Reporting Lost/Stolen Access Devices**: Lost or stolen access cards and/or keys must be reported immediately to the person responsible for Information Resource physical facility management.
9. **No Identifying Information**: Access cards and/or keys must not have identified information coded into them.
10. **Visitor Tracking**: All Information Resources facilities that allow access to visitors must track visitor access with a sign-in/out log.
11. **Service Charges**: A service charge may be assessed for access cards and/or keys lost, stolen, or not returned.
12. **Record Keeping**: Access card records and visitor logs for Information Resource facilities must be kept for routine review based on the criticality of the Information Resources being protected.
13. **Access Revocation**: The person responsible for Information Resource physical facility management must remove the card and/or key access rights of individuals who change roles within the Organization or are separated from their relationship with the Organization.
14. **Accompaniment of Visitors**: Visitors in card-access controlled areas of Information Resource facilities must always be accompanied by authorized personnel.
15. **Periodic Review**: The person responsible for Information Resource physical facility management must periodically review access records and visitor logs for the facility and investigate any unusual access.
16. **Access Rights Review**: The person responsible for Information Resource physical facility management must periodically review the facility's ard and/or key access rights and remove access for individuals who no longer require it.
17. **Signage**: Signage for restricted-access rooms and locations must be practical, yet minimal evidence of the location's importance should be displayed to deter unauthorized access.

Physical Data and Clear Desk Security

1. **Secure Information Storage**: Employees must ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be away for an extended period.
2. **Workstation Security**: Computer workstations must be screen-locked when the workspace is unoccupied. Unlocked hibernation or sleep modes are not sufficient.
3. **Non-Accessible Information**: When the desk is unoccupied and at the end of the workday, any internal or confidential information must be removed and locked in a drawer.
4. **File Cabinet Security**: File cabinets containing internal or confidential information must be closed and locked when not in use or attended.
5. **Key Security**: Keys to access internal or confidential information must not be left at an unattended desk.
6. **Laptop Security**: Laptops must not be left unsecured in offices overnight.
7. **Password Security:** Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
8. **Printer Security:** Printouts containing internal or confidential information should be immediately removed from the printer.
9. **Document Disposal:** Internal and/or confidential documents should be shredded in official shredder bins upon disposal.
10. **Whiteboard Security:** Do not leave internal or confidential information on whiteboards in rooms commonly used by the public.
11. **Mass Storage Device Security:** Treat mass storage devices such as USB drives as sensitive and secure them in a locked drawer if they contain internal or confidential data.

12. **Screen Privacy:** Computer screens must be positioned so outsiders cannot see information.
13. **Confidential Information Display:** Internal and confidential information must not be displayed on a computer screen where the screen cannot be viewed by those not authorized to view the information.

Equipment Security

1. **Warranty and Service Contracts:** The Organization must ensure that information assets are covered by warranty or service contracts.
2. **Regular Inspections:** Equipment must be inspected regularly, and tests to verify its proper functioning must be performed to reduce the risk of malfunction or failure.
3. **Chain of Custody**: Implement a chain of custody for off-premises equipment transferred among individuals and third parties to ensure accountability and security.
4. **Asset Transfer Procedures:** When shipping, repurposing, or disposing of physical assets, asset owners must leverage a ticketing system and update appropriate asset inventories.
5. **Authorized Personnel:** Only individuals authorized by asset owners should be permitted to move assets off-site. Details of the individual's identity and role should be documented and returned with the asset.
6. **Protection from Physical Threats:** Equipment must be protected from physical and environmental threats, including unauthorized access, theft, fire, water damage, and power failures.
7. **Environmental Controls:** Ensure that equipment is sited or protected to reduce the risks from environmental threats, hazards, and opportunities for unauthorized access.
8. **Utility Protection:** Protect equipment from power failures and other disruptions caused by failures in supporting utilities.
9. **Authorization for Off-Site Movement:** Equipment, information, or software should not be taken off-site without prior approval.
10. **Network Cabling Security:** Network cabling must not run through non-secured areas unless only public data (e.g., extended wiring for an Internet circuit) or supporting information services are protected from interception or damage.

Version Details

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