EMAPTA

Physical Security Manual

PROTECTED

DOCUMENT CONTROL NO.: EVSI.ITD.00.00
EFFECTIVITY DATE: June 2024

TABLE OF CONTENTS

1. OVERVIEW

1.1. The Physical Security Manual outlines EMAPTA's commitment to protecting its physical assets, infrastructure, personnel, and sensitive information through structured security measures. This manual is designed to establish and maintain comprehensive guidelines, procedures, and protocols to safeguard against unauthorized access, breaches, and other security risks. By defining clear responsibilities and implementing effective security practices, the manual aims to ensure a secure and safe environment for employees, visitors, and stakeholders. It serves as a foundational document for all physical security-related activities and provides a framework for compliance with legal, regulatory, and organizational requirements.

2. OBJECTIVE

2.1. The purpose of the Physical Security Manual is to establish comprehensive guidelines, procedures, and protocols to safeguard the physical assets, infrastructure, personnel, and sensitive information of EMAPTA. By defining clear security measures and responsibilities, this manual aims to mitigate risks, prevent unauthorized access or breaches, ensure compliance with legal and regulatory requirements, and maintain a secure and safe environment for employees, visitors and stakeholders across all operational areas.

3. SCOPE

3.1. The Physical Security Manual shall apply to all EMAPTA leased and managed physical offices.

4. DEFINITION OF TERMS

4.1. **Access Control:** Measures and systems used to regulate who can enter specific areas or use particular resources within EMAPTA's premises.

4.2. **Biometric Scanner:** A security device that uses unique physical characteristics, such as fingerprints or facial recognition, to grant or deny access.

4.3. **Clean Desk Policy:** Guidelines designed to ensure workspaces are kept clear of non-essential items, confidential information, and other materials to prevent security risks and enhance productivity.

4.4. **CCTV (Closed-Circuit Television):** A system of video cameras and monitors used for surveillance and security monitoring of premises.

4.5. **Facilities Site Manager:** An individual responsible for overseeing and implementing physical security policies, maintaining security systems, and managing facility-related security operations.

4.6. **Incident Response:** The process of identifying, managing, and mitigating security incidents observed through monitoring systems.

4.7. **Information Security Team:** A group responsible for the development, implementation, and oversight of information security policies, controls, and training within EMAPTA.

4.8. **Physical Access Control:** Systems and protocols used to manage and restrict entry to physical locations based on job roles and security clearance levels.

4.9. **Secure Storage:** Areas or methods designated for the protection of sensitive or confidential physical documents and materials.

4.10. **Visitor Badge:** An identification pass issued to visitors, indicating their access permissions and details of their visit.

4.11. **Workstation:** An employee's designated area for performing job-related tasks, including a desk, computer, and other work-related equipment.

5. ROLES AND RESPONSIBILITIES

5.1. Facilities Site Manager

5.1.1. Develop and implement physical security policies and procedures in collaboration with security and management teams.

5.1.2. Oversee the design, installation, and maintenance of security systems such as CCTV, access control and alarm systems.

5.1.3. Conduct regular security checks and inspections to identify vulnerabilities and recommend corrective actions.

5.1.4. Coordinate with security vendors and contractors for security system upgrades or repairs.

5.2. Information Security Team

5.2.1. Assist in policy creation and implementation of security controls, including education of EMAPTA core and talents through ISAT and regular mailers or awareness drives.

5.2.2. Validate the regular security checks and assist in collating the evidence for external audits.

5.2.3. Perform random security checks to validate effectiveness and compliance with security policies and procedures.

5.3. Facilities Team

5.3.1. Install, configure, and troubleshoot security hardware such as CCTV, access control panels and alarm systems.

5.3.2. Conduct routine maintenance checks on security systems to ensure proper functioning and reliability.

5.3.3. Coordinate with external service providers for specialized security system maintenance or repairs.

5.3.4. Assist in testing and implementing security system upgrades or integrations with other facility systems.

5.3.5. Manage the issuance and revocation of physical access and credentials for employees and contractors.

5.3.6. Coordinate with HR and IT to ensure timely updates to access permissions based on the employee status changes.

5.4. Emergency Response Coordinators

5.4.1. Develop and maintain emergency response plans for various scenarios such as fire, natural disasters, or security breaches.

5.4.2. Conduct regular drills and training sessions for employees on emergency evacuation procedures and crisis communication protocols.

5.4.3. Coordinate with local emergency services and agencies to ensure a timely and effective response during emergencies.

5.4.4. Maintain emergency supplies, equipment, and contact lists for quick response and recovery.

5.4.5. (Refer to Safety and Security Policy and Procedure (SSPP) for more information)

5.5. SEA Team

5.5.1. Monitor and review access logs to detect any unauthorized access attempt or anomalies.

6. PHYSICAL ACCESS CONTROL

6.1. Access to company resources will be granted based on the principles of least privilege, where employees are granted access only to the resources necessary for their job functions.

6.2. All entrance and exit doors must be kept closed at all times. Only authorized personnel are allowed to assist a visitor or any person who has no physical access to enter the common reception area to secure proper access authorization.

6.3. Access control policies for employees, contractors, and visitors

6.4. Employees:

6.4.1. Employees will be provided with company-issued identification cards.

6.4.2. Access to specific areas within the premises will be restricted based on job functions and security clearance levels.

6.4.3. New Employees: Upon hiring, HR will initiate the access request process based on the employee's job role. The employee's manager will review and approve access privileges accordingly.

6.4.4. Role Changes: Any changes in an employee's job role that require different access permissions must be approved by the employee's manager and HR.

6.4.5. Termination or Departure: HR will promptly deactivate or revoke access privileges for employees who resign, terminated, or no longer require access due to job changes.

6.4.6. Responsibilities:

6.4.6.1. Employees: Employees are responsible for safeguarding their access credentials and reporting any suspicious or unauthorized access attempts immediately.

6.4.6.1.1.1. Employees shall not allow tailgating or pass backs

6.4.6.1.1.2. Report cases of tailgating

6.4.6.1.1.3. Employees shall not assist any visitor who is attempting to enter the premises. Employees to ask the front desk receptionist to assist.

6.4.6.2. Managers: Managers are responsible for ensuring that access permissions granted to their team members align with job responsibilities and business needs. They must promptly report any access-related changes or concerns to HR and IT departments.

6.4.6.3. Human Resource Department: HR is responsible for initiating access requests, coordinating with IT and security teams to ensure compliance with access control policies.

6.4.6.4. Facilities: The facilities team is responsible for implementing and maintaining access control mechanisms, conducting access audits, and enforcing security measures related to physical access.

6.5. Contractors:

6.5.1. Contractors must obtain explicit authorization and proper credentials from the designated company representative or project manager before accessing EMAPTA facilities.

6.5.2. Access permissions will be granted based on the specific requirements of the contracted work and restricted to designated areas as necessary.

6.5.3. Prior to commencing work, contractors must undergo security awareness training provided by EMAPTA to familiarize themselves with company security policies, emergency procedures, and safety protocols.

6.5.4. Contractors must comply with all applicable laws, regulations, and company policies related to security, safety and confidentiality.

6.5.5. Contractors and their personnel must prominently display their issued identification badges while on company premises.

6.5.6. Contractors' identification should have an indicated contractor status and documented expiration dates.

6.5.7. Contractors must work under the supervision of their assigned project manager or company representative while on-site.

6.5.8. Contractors need to be escorted by EMAPTA employee while accessing restricted areas or performing critical tasks.

6.5.9. Contractors must promptly report any security incidents, accidents, or safety hazards to their project manager, or the designated company contact.

6.5.10. Contractors are responsible for ensuring the security and proper use of any equipment, tools, or materials provided by EMAPTA during the contracted work.

6.5.11. Contractors must not remove nor tamper with company property, assets, or information without proper authorization.

6.5.12. Exit Procedures:

6.5.12.1. Upon completion of contracted work or termination of the contract, contractors must return all company-issued equipment, keys, access cards, badges and any other property entrusted to them.

6.5.12.2. Access permissions for contractors will be promptly revoked upon contract completion or termination, and all physical access must be relinquished.

6.6. Visitors

6.6.1. Visitor Registration:

6.6.1.1. All visitors must register upon arrival at the designated reception or entry point.

6.6.1.2. Visitors are required to provide valid identification (e.g. government-issued ID, passport) and complete a visitor registration form.

6.6.1.3. Reception personnel will verify visitor information and issue a visitor badge or temporary access pass.

6.6.2. Escort Requirement:

6.6.2.1. Visitors must be escorted at all times while within company premises.

6.6.2.2. The host employee or assigned escort is responsible for accompanying the visitor during their visit and ensuring they adhere to company policies and procedures.

6.6.3. Access Permissions

6.6.3.1. Visitors will be granted access to authorized areas based on the purpose of their visit.

6.6.3.2. Access permissions may include designated meeting rooms, common areas, or specific workspaces approved by the host employee or department manager.

6.6.4. Visitor Pass

6.6.4.1. All visitors must prominently display their issued visitor pass while on-site.

6.6.4.2. Visitor passes should clearly indicate the visitor's name, date of visit, and authorized areas of access.

6.6.4.3. Visitors without valid visitor pass must be directed to reception for assistance.

6.6.5. Visitor checkout

6.6.5.1. Upon completion of their visit, visitors must return their visitor pass to reception or designated personnel.

6.6.5.2. Reception personnel will record visitor checkout times and verify that all visitors have exited the premises.

6.6.6. Restricted Areas

6.6.6.1. Visitors are strictly prohibited from accessing restricted areas such as Server rooms, IT infrastructure areas, Electrical Room secured workspaces, or other sensitive locations without prior authorization.

6.6.6.2. Access to restricted areas requires explicit approval from the host employee, department head and information security department.

6.6.7. Awareness

6.6.7.1. Employees responsible for hosting visitors or acting as escorts must be aware of EMAPTA's visitor control procedures, emergency protocols and safety guidelines.

6.6.7.2. Regular reminders and updates regarding visitor control policies should be communicated to all employees to maintain awareness and compliance.

6.6.7.3. Visible and readable signages for emergency exits must be used.

6.6.7.4. Emergency exit route map

6.7. Access Control Equipment Specifications

6.8. Access control equipment (e.g. biometric scanners and electronic locks) installed on entrance and exit doors must meet industry standards for reliability, security, and compatibility with existing systems.

6.9. All access control equipment installations must be approved and supervised by the designated facilities site lead. Information Security department will validate and check for proper sign off from facilities site lead.

6.9.1. Cable Management – Use proper cable management techniques to minimize the risk of accidental damage or interference.

6.9.1.1. Adhere to industry standards and best practices for cabling installation, including cable types, terminations, and distances.

6.9.1.2. Data cables or LAN cables should be protected from tampering or interference.

6.9.1.3. Power cables and power supply should be protected from tampering or physical interference.

6.9.1.4. Only authorized personnel are allowed to access cables for maintenance and repairs.

6.9.1.5. Ensure proper wiring and connectivity between the device, access control panels, power supply units, and network infrastructure. Use high-quality cables and connectors to minimize signal interference and ensure reliable operation.

6.9.2. Scanning tool or biometric scanner

6.9.2.1. Conduct a thorough site assessment to determine the appropriate placement of biometric access control devices. Consider factors such as door type, traffic flow, lighting conditions, and accessibility requirements.

6.9.2.2. Choose an access control device that are suitable for the specific entry door environment. Consider factors such as weather resistance, tamper resistance, and compatibility with existing access control systems.

6.9.2.3. Install the device at an appropriate height and angle for easy user access while ensuring optimal scanning accuracy. Follow the manufacturer guidelines for recommended mounting heights and angles.

6.9.2.4. Implement backup power solutions such as uninterruptible power supply (UPS) systems to ensure continued operation of access control devices during power outages.

6.9.2.5. Tamper-resistant Installation – Securely mount devices and associated components to prevent tampering or unauthorized access. Use tamper-resistant hardware and enclosures where applicable.

6.9.2.6. Integrate access control devices seamlessly with EMAPTA's access control system for centralized management of user credentials, access permissions, and audit trails.

6.9.3. Testing and Commissioning

6.9.3.1. Facilities site lead must conduct thorough testing and commissioning of installed biometric access control system to ensure all components function correctly, including biometric verification accuracy, door locking/unlocking mechanisms, and system integration.

6.9.3.2. Facilities to establish a maintenance schedule to inspect, clean, and calibrate biometric devices regularly. IT and Information Security team to assist Facilities in monitoring system logs and performance metrics to identify and address any potential issues proactively.

7. CLEAN DESK CLEAR SCREEN

7.1. Workstations should be free from personal non-work-related items, including but not limited to photographs, souvenir items, books, magazines, clothing. etc. that impede work productivity of the employees, compromise information security, or damage any EMAPTA asset.

7.2. Employees should not put out their passwords or confidential data on sticky notes, post-it notes, or unprotected files within their desktop screens.

7.3. Lock or log out of computers, laptops, or other electronic devices when leaving the workstation unattended.

7.4. Avoid leaving portable electronic devices unattended or unlocked in the workplace.

7.5. Do not use unauthorized removable storage devices to store confidential Company or Client Data.

7.6. Employees should always secure protected, confidential, and classified information, whether in hardcopy or softcopy in accordance with the Information Security Policy.

7.7. All confidential and classified information should be stored in a secured and locked drawer or a filing cabinet.

7.8. All Employees should check their workspace before leaving the area. Workstation devices that are to be temporarily unattended should be system locked or turned off. No confidential or classified paper or document should be left out on any unsecure work area or surface; the drawer and/or the filing cabinet for such documents should be locked.

7.9. Employees should store sensitive physical documents in designated secure storage areas, such as locked cabinets or drawers.

7.10. Employees should ensure that confidential or sensitive information is not visible on screens, whiteboards, or any other display mediums when leaving the workstation unattended.

7.11. Secure printed materials in printer areas. No printed materials should be left unattended.

7.12. Employees should shred any confidential and classified paper documents once no longer required and put the shredded paper in the designated trash bin.

7.13. (Please refer to Emapta's Clean Desk Policy for a more detailed information)

8. CCTV SURVEILLANCE MONITORING

8.1. Live Monitoring: Security personnel should continuously monitor live CCTV feeds for any unusual or unauthorized activities in designated areas.

8.2. Event Monitoring: Monitoring of specific events or alarms triggered by motion detection (if applicable), door access control systems, or other integrated security systems.

8.3. Recording Management: Ensure proper recording of CCTV footage based on retention policies and legal requirements. Regularly archive and backup recorded footage to prevent data loss.

8.4. Incident Response: Immediately respond to security incidents observed through CCTV monitoring. Follow established escalation procedures, notify relevant authorities, and document incident details.

8.5. Privacy and Legal Compliance

8.5.1. Data Privacy: Ensure CCTV monitoring complies with data privacy laws and regulations. Limit access to recorded footage to authorized personnel only.

8.5.2. Footage Retention: Adhere to EMAPTA retention policies for storing CCTV footage based on legal requirements and EMAPTA company guidelines. Properly dispose of outdated footage as per data protection protocols.

8.5.3. Public Area Monitoring: Clearly define areas monitored by CCTV systems, particularly public spaces, to ensure transparency and compliance with privacy regulations.

8.6. Facilities team to conduct regular maintenance checks, inspections, and testing of CCTV cameras, monitors, recording devices, and connectivity cables.

8.7. Schedule routine calibration, cleaning, and software updates to ensure optimal performance and reliability of CCTV equipment, coordinating as necessary to IT and Security departments.

9. DOCUMENTATION AND COMPLIANCE

9.1. Any Employees found to have violated this policy may be subject to disciplinary action following the Code of Conduct.

9.2. Regularly audit physical security procedures for compliance with security policies, standards and procedures.

9.3. Audit findings will be documented, and corrective action plans be implemented as necessary.

10. POLICY REVIEW

10.1. This Physical Security Manual will be reviewed and/or updated on an annual basis or immediately following equipment changes, standard or regulatory updates.

11. EFFECTIVITY

11.1. This Physical Security Manual becomes effective immediately upon its approval and issuance by the relevant authority within EMAPTA. All employees, contractors, and visitors must adhere to the policies and procedures outlined within this manual from the effective date onwards. The manual will be reviewed and updated on an annual basis or as required by changes in security standards, regulatory requirements, or operational needs. Employees and stakeholders will be notified of any updates or amendments to ensure ongoing compliance and awareness.

POLICY/PROCESS OWNER:	**Information Security Manager**
DOCUMENT CONTROL NO.:	**EVSI.ITD.00.00**
EFFECTIVITY DATE:	**June 2024**

	NAME / DESIGNATION	DATE
AUTHOR	**Jappy Damaso – Information Security Manager**	**June 2024**
REVIEWED	**Luis Sicat III – Chief Information Security Officer (CISO)**	**June 2024**
APPROVED	**Henry Vassall Jones – Chief Information Officer (CIO)**	**June 2024**

REVIEW AND REVISION HISTORY

DATE:	ACTION	Control No. (for Revision)	DESCRIPTION / COMMENT
June 2024	*Created*	*1.0*	*A Manual for Physical Security is created. Reviewed and approved.* *-Jappy Damaso-*