Physical Security Management Policy

Auxiliary Services

Version 1.0

Table of Contents

ACRONYMS AND TERMINOLOGY

ACRONYM	DESCRIPTION
SASSETA	Safety and Security Sector Education Training Authority
EMCS	Executive Manager Corporate Services
CEO	Chief Executive Officer
OHSA	Occupational Health and Safety Act 85 of 1993
PSIRA	Private Security Industry Regulations Act 56 of 2001
DEFINITIONS	**DESCRIPTION**
Employee	Any person in the employ of the Safety and Security Sector Education Training Authority) who is permanent or on long term or short-term fixed contract, receives remuneration, and on the approved organisational structure.
Authorized Person	SASSETA employee or any other person declared by the CEO as such.
Designated Security Official	A skilled individual in terms of PSIRA.
Visitors	Any person (including SASSETA Stakeholders) who accesses SASSETA premises with the aim of engaging with SASSETA staff either on formal work-related matters or socially.

1. Policy Statement

The SASSETA considers the safety and security of its employees, stakeholders and assets of prime importance and therefore takes necessary precautionary measures to prevent security related incidents and will not compromise the set security standards and procedures in pursuit of other business priorities.

In conjunction with the Occupational Health and Safety program, the SASSETA adopts an error free and zero tolerance approach to unsafe acts and conditions with zero safety and security incidents being the aim. SASSETA assumes all the accountability and responsibility for the safety and security of all in its premises, however, all Executive Managers, Managers, employees and stakeholders have a responsibility to ensure that all their activities are carried out with the acceptable level of risk to themselves, assets and those persons around them.

To ensure effectiveness and continuous improvement, the SASSETA will ensure a consultative environment in which management work together with employees to improve safety and security in the workplace.

2. Purpose of the Policy

The purpose of this policy is to:

2.1. Articulate standards and procedures regarding the security of SASSETA's human capital, physical assets, and stakeholders.

2.2. Guide the implementation of such security standards and procedures.

2.3. Ensure continuous assessments of security risks and timeous implementation of recommended corrective actions; and

2.4. Ensure the allocation of adequate resources for the necessary deterrent methods.

3. Scope of Policy

3.1 This policy is applicable to all permanent and non-permanent (Temporary staff; Leaners and Interns) employees of the SASSETA as well as the relevant stakeholders, clients and guests who visit SASSETA premises.

4. General Principles

4.1. SASSETA views Physical Security Management as one of the key pillars for a safe, facility and believes that it has a direct and indirect impact on employee working conditions as well as organizational performance.

4.2. SASSETA strives to maintain a risk-free environment for persons and its assets; it also upholds the principles of high vigilance by individuals to avoid potentially hazardous situations and that of exercising a supreme judgement to maintain personal safety and wellbeing.

4.3. The policy is a dynamic document and will be amended as required, depending on new directives and policies that may have a bearing thereon, or based on new practices and procedures.

4.4. Failure to adhere to this policy by any employee or stakeholder will result in corrective measures being instituted or referral to the law enforcement authority where circumstances warrant such.

4.5. This Policy should be read together with the SASSETA Occupational Health and Safety Policy.

5. Legislative Mandate

This policy is aligned to the following, the list below is however not exhaustive:

5.1. Public Finance Management Act, Act 1 of 1999.

5.2. Private Security Industry Regulations Act 56 of 2001

5.3. The Occupational Health and Safety Act 85 of 1993

5.4. The SASSETA Code of Conduct.

5.5. Control of Access to Public Premises and Vehicles Act 1985 (Act 53 of 1985

5.6. Fire-arms Control Act 2000 (Act 60 of 2000) and regulations

5.7. Trespass Act, 1959 (Act 6 of 1959)

5.8. The Disaster Management Act, 2002 (Act No. 57 of 2002)

6. Security Management Team

6.1. The Auxiliary Services Practitioner is responsible for oversight function of security services within SASSETA.

6.2. The Security Management function is primarily performed by the outsourced security services provider reporting directly to Auxiliary Services.

6.3. In the absence of the Auxiliary Services Practitioner, functions related thereto will be delegated in writing to another employee.

6.4. The designated security officials will assist in various day-to-day security related activities including but not limited to the following:

a) monitoring physical barriers, security lighting, intrusion detection, access control, visitors escort etc.

b) Liaising with service providers for outsourced security services.

c) Conducting routine patrols, inspection and testing of detection (incidents).

d) Implement vehicles' keys management system, that is, the driver of a vehicle that is returned to the office after hours/weekends, deposits the keys in a locked safety box.

e) Safeguarding SASSETA's assets; etc.

f) Keeping and maintaining emergency contact details prominently at strategic locations within the building.

g) Assisting the Chairperson of the OHS Committee to facilitate the emergency preparedness program.

7. Physical Measures

Daily Access

7.1 All visitors must report to the security reception desk of the organization building for security personnel to process such visits. Visitors must remain at the reception area from where the host will collect and return the visitors.

7.2 Visitors are to be restricted from gaining access to open plan offices and sensitive areas. Visitors should be limited to Consulting/Boardrooms.

7.3 Hosts receiving visitors are required to exercise access control beyond the security access points.

7.4 Visitors who elect to bring personal equipment i.e., laptops, onto SASSETA premises, are required to declare same on entry point and to complete the relevant declaration form.

7.5 Visitors will be searched. The search will be done with strict regard to decency and privacy and within the confines of the law.

7.6 Should any person (official, visitor or contractor) refuse to be searched he/she may be denied access.

7.7 Visitors who are suspected of being under the influence of alcohol, will not be allowed in the building.

7.8 All dangerous objects found in the possession of visitors, contractors and staff members will be confiscated and based on the risk it holds for the SASSETA, be dealt with in terms of this policy. No firearms will be allowed on any SASSETA premises.

After Hours Access

7.9 Should the need arise for contractors/consultants to work later than 18:00 during the week, or over the weekend, the Auxiliary Services Unit must be informed by email.

8. Issuing of Access Cards

The following procedures shall apply as the first point of security control on entering the SASSETA premises:

8.1 All access cards are issued by the Auxiliary Services Unit. Cards issued as such remain the property of SASSETA.

8.2 Each authorized employee will be issued with one access card except in those instances where more than one access control system is use.

8.3 Officials leaving SASSETA for whatever reason e.g. resignation; must hand their cards over to Auxiliary Services on the last day of service.

8.4. The Auxiliary Services Unit needs to be informed in writing in the event of an employee's name changing to ensure records reflect the correct details of all employees.

9. Use of Access Cards

Staff:

9.1 Each cardholder shall use his/her access card every time on entering and exiting an access point. Same will apply in case of biometric finger reader where the index finger is scanned.

9.2 Under no circumstances are registered users (biometric or card holders) permitted to provide access to another person, swipe for another person and/or allow another person to tailgate at any access point. Persons found to do so compromise the safety and security systems of SASSETA and may be subjected to corrective measures.

9.3 Lost or stolen access cards must be reported to the Practitioner: Auxiliary Services Unit to disable the card. In addition, stolen cards must be reported to Security Personnel.

9.4 Lost/stolen access cards will only be re-issued after a receipt of payment for the replacement cost payable at Finance Unit, is produced.

9.5 The cardholder will use the finger biometric while Auxiliary Services is in the process of issuing another access card.

9.6 The cost of replacing a lost card is as determined by the Landlord and processed through the Finance Department.

Contractors/Consultants

9.7 The Head of the unit where the contractor/consultant is appointed must furnish a letter to the Auxiliary Services Unit containing the following information:

9.5.1 The areas where the contractor/consultants will perform their activities.

9.5.2 A short description of the task that must be performed.

9.5.3 The duration, nature, and expiry date of the contract.

9.5.4 Full names, surnames and ID numbers must be indicated.

9.8 Contractors/Consultants must report and register at Reception on a daily basis for the duration of their stay at SASSETA.

10. Closed Circuit Television (CCTV)

10.1 A comprehensive CCTV and 24-Hour Armed Response has been installed to trigger response when other forms of security have been breached. This system includes deterrent features such as loud 24-Hour alarms to notify intruders that their presence has been detected.

10.2 The purpose of CCTV is to protect life and property and to prevent crime. It is used for no other purpose. The images captured are recorded and retained in the event they are needed as evidence of criminal activity.

10.3 In the interest of confidentiality and privacy, the CCTV is running in the background with no security official viewing same, except in the basement parking area.

10.4 Random review of CCTV tapes shall be conducted for possible suspicious dealings/activities.

11. Basement Parking

11.1 Access to the basement is primarily for parking purposes and under no circumstances shall visitors be allowed to park and enter the building through the basement.

11.2 Parking bays for staff shall be on a first come, first serve basis with exception to parking pays for the Executive and Management Team.

11.3 Staff who travel for work purposes may leave their vehicles over-night at the basement parking. Staff are however discouraged from leaving their vehicles for extended periods in the basement parking.

12. Risk Assessment

12.1 The Auxiliary Services Practitioner in consultation with the Executive Manager Corporate Services, shall ensure that comprehensive security risk assessments are conducted annually.

12.2 The identified risks and their potential impact shall be rated. Adequate controls shall be devised and integrated into the organizational risk profile. Progress monitoring and reporting on implementation of controls shall be in accordance with the organizational risk management procedures.

12.3 Corrective actions shall be effected timely by the Auxiliary Services Practitioner to avert risk recurrence. Where the levels of security risks are escalating, extra measures which may include sourcing in external expertise, shall be employed. The Auxiliary Services Practitioner shall seek permission from the CEO to in-source a security expert for a predetermined period to assist in addressing such risks.

13. Deviations

No deviations to this policy will be entertained however in cases where issues not covered by the policy arise, the final written approval will be granted by the Chief Executive Officer.

14. Policy Review

This policy shall be reviewed every 2 years unless there are significant changes to legislation or business operational requirements.

15. Approval

Document Name	Physical Security Management Policy
Approval	
Year of Current Review	2022/2023
Year of Next Review	2025/2026
Revie process championed by the Chief Executive Officer	
Name of the CEO	Mr. Thamsanqa Mdontswa
Signature	Date:
Approved by the Board	
Name of the Chairperson	Mr. Chris Mudau
Signature	Date: