Government Security Regulator

GOVERNMENT SECURITY
REGULATOR
(GSR)

MINIMUM PHYSICAL
SECURITY STANDARDS
(MPSS)

FOREWORD:

MINIMUM PHYSICAL SECURITY STANDARDS (MPSS) 2009

Government ultimately is responsible for ensuring both the 'freedom and security' of the person as stated in Section 12 of the Constitution. In doing so, government must take cognisance of a variety of factors and ensure the existence of relevant legislation. The South African Police Service therefor is mandated by the Constitution and secure lives of SA citizens and property.

In 2000 Cabinet further enhanced the role of SAPS and specifically/explicitly mandated us to regulate physical security in the government, parastatals as well as National Key Points. In response to this, the SAPS formed the Division: Protection and Security Services (PSS) to focus on all security and protection functions. PSS is now the cornerstone in coordinating and supports the implementation of physical security standard and administration of the National Key Points Act 103 of 1980. PSS is a catalyst to synchronize the provision of physical security, regulate security within Government sector and National Key Points and harness the multi disciplinary approach in order to align all physical security operations to the legislative framework.

The South African Police Service has through a consultation process with the affected stakeholders, compiled: Minimum Physical Security Standards for implementation by all organs of state. The Minimum Physical Security Standards provide guidance on the required minimum levels of physical security. Also, provided herewith is annexures designed to provide guidelines on the different types of installations and security requirements.

Whilst the minimum are not legally enforceable, they are necessary. Furthermore minimum standards are a starting point towards regulations which will be enforceable and binding. Minimum standards therefor are import in ensuring that institutions are able to properly gear themselves for compliance once the regulations have been promulgated.

The Minimum Physical Security Standards are some cornerstones of our security, when implemented, they will represent a solid first line of defence. The attached annexures will be reviewed annually, it is expected that minor changes will be effected to ensure that they are in line with existing security developments.

The Minimum Physical Security Standards will be reviewed every five years to ensure that they remain consistent with our security measures.

The Minimum Physical Security Standards are promulgated by the National Commissioner of the South Africa Police Service for implementation within the Government Sector, Parastatals and National Key Points. Security is an operational responsibility of every institution. Institutions must continuously conduct vulnerability and security risk assessment in order to mount equivalent protection and security. Furthermore, government departments as well as municipalities are also required to continue to take important steps that will identify risks and assure the protection of municipal buildings.

I wish to thank all the stakeholders that provided inputs when the Minimum Physical Security Standards were compiled as well as the Government Sector Security Council who consolidated and ratified the final standard.

I urge all organs of state all Security Managers to use these standards and also to participate in the processes set to review the Minimum Physical Security Standards.

ACTING NATIONAL COMMISSIONER: SOUTH AFRICAN POLICE SERVICE
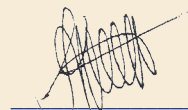DEPUTY NATIONAL COMMISSIONER

EDITORIAL:

MINIMUM PHYSICAL SECURITY STANDARDS (MPSS) 2009

In 2000 Cabinet enhanced the role of SAPS and specifically/explicitly mandated Protection & Security Services to regulate physical security in the government, parastatals as well as National Key Points. It was our approach to first develop the Minimum Physical Security Standards to be promulgated by the National Commissioner of the South African Police for implementation within Government Sector, Parastatals and National Key Points.

Government Security Regulator has through a consultation process with the affected stakeholders compiled Minimum Physical Security Standards to provide guidance on the required minimum levels of physical security. Also reference here is made to researched annexures designed to provide guidelines on the different types of installations and security requirements. The annexures will be reviewed annually and the Minimum Physical Security Standards every five years. The annexures will be available on request and any other information on the annexures can be directed to SAS@saps.org.za Tel: 012 400 6054 Fax 012 400 7053. As the chairperson of the Government Sector Security Council, I wish to extend our gratitude to the council for the work and assistance to ensure the final approval of the MPSS.

Regards

_____ ASSISTANT COMMISSIONER
CHAIRPERSON: GOVERNMENT SECTOR SECURITY COUNCIL
T KULU

PREFACE

In the course of 2003, the South African Cabinet approved the mandated functions and broad structure of the new Protection and Security Services Division of the SAPS. These functions led to the establishment of the Component: Government Security Regulator (GSR) component. The GSR functions will be to regulate the service of all existent and newly identified Strategic Installations and the administration of the National Key Points Act.

The Government Security Regulator will perform these functions at national and provincial departments (excluding NIA, SASS and the SANDF), Public Entities, Parastatals and private entities which are classified as National Key Points.

The Government Security Regulator (GSR) was mandated to compile and implement the Minimum Physical Security Standards (MPSS) as an official document on minimum physical security standards, which must be maintained at all departments / institutions.

Any comments and/or recommendations in respect of this standard should be forwarded in writing to the Chairperson of the Government Sector Security Council (GSSC). All the representatives to the GSSC are responsible for ensuring that the document and feedback is received from all of their cluster members.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.1   STATEMENT OF PURPOSE

The primary purpose of this directive is to provide guidance to the security managers of the departments and institutions with regards to the implementation and compliance in respect to minimum physical security standards required. The standards is designed to assist security managers in coordinating and managing compliance within the minimum physical security standards as required in internal physical security policy, procedures, overall efficiency and effectiveness of the physical security programme of the department or institution.

1.2   SCOPE

The MPSS is aimed for use at all Government Department, National Key Points and Strategic Installations. The guide will assist all security managers in reviewing their physical security related aspects on their respective departments or institutions. All organizational resources, i.e. people, assets and physical protection of information, are covered in this document.

1.3   LEGISLATIVE REQUIREMENTS AND DIRECTIVES

1.3.1   South African Police Services Act, 1995 (Act No 58 of 1995)
1.3.2   National Key Point Act, 1980 (Act No 102 of 1980)
1.3.3   Control of Access to Public Premises and Vehicle Act, 1985
              (Act No 53 of 1985)
1.3.4   Protection of Information Act, 1982 (Act No 84 of 1982)
1.3.5   Public Finance Management Act, 1999(Act No 1 of 1999
1.3.6   Constitution of the Republic of South Africa, 1996 (Act No 108 of 1996)
1.3.7   Public Service Act and Regulations 2001
1.3.8   Criminal Procedure Act, 1977 (Act No 51 of 1977)
1.3.9   Private Security Industry Regulation Act, 2001 (Act No 56 of 2001)
1.3.10   Firearm Control Act, 2000 (Act No 60 of 2000)
1.3.11   Occupational Health and Safety Act, 1993 (Act No 85 of 1993)
1.3.12   Minimum Information Security Standards

CHAPTER 2

DEFINITIONS AND ABBREVIATIONS

2.1   IN THIS DOCUMENT, UNLESS THE CONTEXT OTHERWISE INDICATES:

2.1.1   **Business Continuity Planning**, includes the development of plans, measures, procedures and arrangements to ensure minimal or no interruption of the availability of critical services and assets.

2.1.2   **Classified information**, means sensitive information which, in the national interest, is held by, produced or is under the control of the state, or which concerns the state and which must by reasons of its sensitive nature be exempt from disclosure and must enjoy protection against compromise.

2.1.3   **Criminal Record Check**, means an investigation to determine the criminal record of an individual to determine his/her criminal record status.

2.1.4   **Compromise**, means disclosing, destroying, removing, modifying or interrupting assets without the necessary authorization.

2.1.5   **Comsec**, means the institution identified as Electronic Communication Security (Pty) Ltd established in terms of section 2 of the Electronic Communications Security Act, 2002 (Act No 68 of 2002).

2.1.6   **Defensive Counter Intelligence**, means proactive measures conducted to neutralize the effectiveness of foreign intelligence operations to protect classified information and terrorism aimed at or against personnel, strategic installations and resources of the Republic of SA in accordance with the National Strategic Intelligence Act, 1994 (Act No 39 of 1994).

2.1.7   **Directives**, means the Minimum Physical Security Standard (MPSS).

2.1.8 **Institution**, means any organ of state as defined in section 239 of the Constitution, 1996 (Act No 108 of 1996), including, but not limited to, any public entity as defined in section 1 of the Public Finance Management Act, 1999 (Act No 1 of 1999).

2.1.9 **Strategic Installation**, means any institution which has been declared by the minister.

2.1.10 **MISS**, means the minimum information security standards as approved by cabinet on 4 December 1996.

2.1.11 **Owner**, means the HOD/CEO of department/institution municipal manager.

2.1.11 **Physical Security**, means the use of physical measures to prevent and delay unauthorized intrusion and to protect assets and personnel, detect any attempt or actual break in the physical security environment.

2.1.12 **Risk**, means the likelihood of a threat materializing by exploitation of an event or incident to create vulnerability.

2.1.13 **Physical Security implies**, but is not limited to:-

1. Physical security measures for the protection of information
2. Personnel security awareness of physical security matters
3. Contingency planning
4. Criminal Record check
5. Dealing with security breaches relating to physical security matters
6. Security investigations
7. Auditing and compliance checks to ensure security standards.

2.1.14 **Physical Security Grading** different levels of physical security measures of the structure.

2.1.15 **Security breach**, means the negligent or intentional transgression or failure to comply with physical security measures.

2.1.16 **Security evaluation**, means the process to determine the security threat analysis encompassing physical security appraisal, topographical analysis and security appreciation analysis.

2.1.17 **Security Policy**, means a formal set of rules that governs the security of an institution's premises, assets, technology and information assets.

2.1.18 **Threat**, means any potential event or act, deliberate or accidental, that could cause injury to persons, compromise the physical security or could cause the loss of or damage to assets.

2.1.19 **Threat and Risk Assessment**, means the process of doing a security threat analysis, encompassing physical security appraisal, topographical analysis and security appreciation analysis.

2.2 ABBREVIATIONS

2.2.1	**CEO**	-	Chief Executive Officer
2.2.2	**COMSEC**	-	Communication Security/ Electronic Communication Security.
2.2.3	**GSR**	-	Government Security Regulator
2.2.4	**GSS**	-	Government Sector Security
2.2.5	**GSSC**	-	Government Sector Security Council
2.2.6	**HOD**	-	Head of Department
2.2.7	**MISS**	-	Minimum Information Security Standards
2.2.8	**MPSS**	-	Minimum Physical Security Standards
2.2.9	**NIA**	-	National Intelligence Agency

2.2.10	**NKP**	-	National Key Points
2.2.11	**PSIRA**	-	Private Security Industry Regulatory Authority
2.2.12	**SAPS**	-	South African Police Service
2.2.13	**SAS**	-	Security Advisory Service of SAPS
2.2.14	**SASS**	-	South African Secret Service
2.2.15	**SANDF**	-	South African National Defense Force

CHAPTER 3

FUNCTIONS, ROLES AND RESPONSIBILITIES ON APPLICATION OF SECURITY MEASURES

3.1   THE ROLE AND RESPONSIBILITIES OF SOUTH AFRICAN POLICE SERVICE

3.1.1.   The SAPS will issue Minimum Physical Security Standards to support institutions in the protection of their installations (including Parastatals, Public and Private Entities).

3.1.2.   SAPS is responsible for assisting institutions (including parastatals, public/private entities that fall under the National Key Points environment) in establishing effective physical security within their own environments and to monitor the physical security compliance/ adherence as stipulated in the Minimum Physical Security Standards. To achieve this the SAPS must do the following:

3.1.2.1   Advise institutions with regard to the implementation of Minimum Physical Security Standards and any physical security related issues.

3.1.2.2   Audit physical security through conducting evaluations and assessments as part of security appraisals, in order to:

1.   Determine the overall standard of physical security and security awareness as far as it relates to physical security.
2.   Determine whether the extent to which the aspects of the security policy of the institutions are consistent with the directive of the Minimum Physical Security Standards.
3.   Implementation of the security policy and its effectiveness.
4.   Support the establishment of a physical security emergency reaction capability.

NB: Any intelligence and information security-related issues detected by SAPS (breaches of information security) must be referred to NIA (Advisory Section) for further handling.

3.2   THE ROLE AND RESPONSIBILITIES OF NATIONAL INTELLIGENCE AGENCY

3.2.1   The National Intelligence Agency is mandated by legislation to coordinate between itself, the South African Secret Services, the South African Police Services and the South African National Defense Force regarding the implementation of defensive counter - intelligence measures at institutions.

3.2.2   The Agency is responsible for assisting and providing guidance to institutions within its legislative mandate to establish effective information security within their own environments and to monitor their adherence to Minimum Information Security Standards.
In fulfilling this, the agency will:

3.2.2.1   advise institutions on how to identify information that falls within the broader categories of classified information and, therefore, require special protection through classification.

3.2.2.2   advise institutions on the implementation of and adherence to Minimum Information Security Standards.

3.2.2.3   assist institutions in ensuring that their security policies include Minimum Information Security Standards.

3.2.2.4   advise, co-ordinate, audit and exercise control with regard to information security in the public, parastatal and private environment in South Africa (with the exclusion of SAPS, SASS and SANDF responsibilities).

NB: Any physical security-related issues (breaches, non-compliance) must be referred to the SAPS for further handling.

3.3   THE ROLE AND RESPONSIBILITIES OF NATIONAL DEPARTMENT OF PUBLIC WORKS

3.3.1   When providing facilities for institutions, the National Department of Public Works must:

3.3.1.1   ensure that the requirements of physical security directives relating to contracting are complied with.

3.3.1.2   ensure that reliability checks are completed by the relevant National Intelligence Structures of private institutions, companies and individuals who may require access to protected and classified information and assets.

3.3.1.3   ensure that physical security measures as prescribed by SAPS Security Advisory Services for installations of the department/institution, as part of the contracting process, is adhered to.

3.3.1.4   ensure that security assessments of facilities or drawings/architectural designs thereof are undertaken by the SAPS (SAS) and NIA before any agreement is entered into to procure the property for an institution and all recommendations of the SAPS (SAS) are implemented.

3.3.1.5   involve the SAPS in all structural improvements done to maintain the minimum physical security levels of the institutions.

3.4   THE ROLE OF COMSEC (Electronic Communications Security (Pty) Ltd)

3.4.1   Electronic Communication Security must:

3.4.1.1   advise and assist institutions on the implementation of the minimum standards relating to communication security contained in the Minimum Information Security Standards, and

3.4.1.2   assess and report on the application of communication security technical devices in both the public and private sectors.

3.5   THE ROLE AND RESPONSIBILITIES OF GOVERNMENT SECTOR SECURITY COUNCIL (GSSC)

3.5.1   The Government Sector Security Council is a consultative structure for regulating physical security training and security provisioning in the Government Sector (including Public/Private Entities, Parastatals and NKPs).

3.5.2   The functions of the GSSC are the following:

3.5.2.1   Consolidate the implementation of Government Sector Security through co-ordinating functions and activities that relate to physical security.

3.5.2.2   Enhance the monitoring and evaluation initiatives of physical security in the government.

3.5.2.3   Facilitate thorough and effective physical security in government sector buildings and build co-operation between members of the public sector and private sector.

3.5.2.4   Co-ordinate contingency planning exercises and create a platform for communicating the management of physical security incidents and breaches.

3.5.2.5   Integrate and co-ordinate related functions, especially the inspections and audits of the different security agencies i.e. NIA, SAPS, PSIRA.

3.5.2.6   The Council will also enhance understanding of the role of different security agencies such as PSIRA, NIA and SAPS. The GSSC will create an appropriate platform for the liaison of all security managers in the public sector and private sector.

NB: *Included in the membership of the GSSC are the representatives of the regulatory bodies i.e. National Nuclear Regulator, NERSA, Rail Safety Regulator, PSIRA, Armaments Co-operation of South African (Ltd), SASSETA and NIA.*

3.6   THE ROLE AND RESPONSIBILITIES OF THE OWNER OF DEPARTMENT OR INSTITUTION

3.6.1   **"The owner of department or institution in this regard refer to Head of Department, Chief Executive Officer and Municipality Manager".**

3.6.1.1   The owner of the department/institution is accountable for the overall physical security under his/her control.

3.6.1.2   The owner must oversee the development, implementation and maintenance of the security policy as per the needs of the department/institution.

3.6.1.3   The owner must ensure that a manager is appointed to manage all security functions and ensure implementation/adherence to Minimum Physical Security Standards.

3.6.1.4   The owner must ensure that all institutions under him /her have been security evaluated/assessed by SAPS Security Advisory Services.

3.6.1.5   The owner must ensure that employees and service providers (contractors/consultants) are subjected to reliability record checking process conducted by NIA.

3.6.1.6   The owner must conduct training and awareness programmes with regard to adherence to the Minimum Physical Security Standards.

3.6.1.7　The owner must ensure that the security section is exposed to appropriate security-related training to empower them in the performance of their functions.

3.6.1.8　The owner must ensure that a Security Committee is established within his/her department/institution.

3.6.1.9　The owner must see to it that a correct reporting structure is in place with regard to reporting of Security breaches.

3.6.1.10 The owner must approve budget as advised by the Security Committee for the recommendations on the security assessment conducted by SAPS (SAS) in the department/institution.

NB: *With the assistance of the Security Committee, the owner of the department/institution must ensure that there is a continuous monitoring of the compliance with this Minimum Physical Security Standards by instituting internal departmental policy or directives.*

3.7　RESPONSIBILITIES OF SECURITY MANAGER

3.7.1　The Security Manager must:

3.7.1.1　Manage all matters relating to the administration and organization of security at the department/institution.

3.7.1.2　Draft security policy for approval by security committee and head of the institution.

3.7.1.3　Manage the security component of the department/institution.

3.7.1.4　Continually monitor all physical security related contracts at the department/institution to ensure compliance with the contract specifications.

3.7.1.5　Ensure that security assessments/evaluations/threat and risk assessments of the installations are conducted by the SAPS at institutions.

3.7.1.6　Enhance the awareness of the staff regarding physical security in the department/institution.

3.7.1.7　Ensure that security audits are conducted every three years.

3.7.1.8　Analyze the audit results, make recommendations to the head of the department/institution to improve physical security measures and prepare a report for the head of the department/institution for submission to the SAPS regarding the findings.

3.7.1.9　Consult with the SAPS on any new developments or changes in the physical security environment.

3.7.1.10 Ensure that applications for criminal record checks are correctly completed before submission to the SAPS.

3.7.1.11 Act as chairperson of the security committee of the department/institution.

3.8.　FUNCTIONS OF THE SECURITY COMMITTEE

3.8.1　The Security Committee must do the following:

3.8.1.1　Recommend the security policy of the department/institution after having taken the advice provided by SAPS and NIA into account.

3.8.1.2　Make recommendations to the head of institution regarding the implementation and maintenance of security measures.

3.8.1.3   Regularly review the security policy of the department/institution, its prioritization thereof as well as information and advice provided by the SAPS and NIA.

3.8.1.4   Forward the draft policy and any review thereof to the SAPS and NIA for endorsement.

3.8.1.5   After endorsement by SAPS and NIA, submit the policy or any review thereof to the head of the department/institution for approval.

3.8.1.6   Ensure the communication of the approved policy to all staff members and relevant consultants and contractors.

3.8.1.7   Make recommendations to the head of the department/institution regarding directives to be issued by the head of the department/institution to ensure the implementation of the security policy and any review thereof.

3.9.   FUNCTIONS AND RESPONSIBILITIES OF PSIRA

The Private Security Industry Regulatory Authority (PSIRA) was established in terms of section 2 of the Act. The primary objects of the Authority are to regulate the private security industry and to exercise effective control over the practice of the occupation of security service providers in the public and national interest of the private security industry itself. Other objects include, inter alia, the following:

3.9.1   To promote a legitimate private security industry which acts in terms of the principles contained in the Constitution and other applicable laws.

3.9.2   To ensure that all security service providers act in the public and national interest in the rendering of security services.

3.9.3   To determine and enforce minimum standards of occupational conduct in respect of security service providers.

3.9.4   To promote high standards in the training of security service providers and prospective security service providers.

3.9.5   To promote the protection and enforcement of the rights of security officers and other employees in the private security industry.

3.9.6   To ensure that compliance with existing legislation by security service providers is being promoted and controlled through a process of active monitoring and investigation of the affairs of security providers.

CHAPTER 4

MINIMUM PHYSICAL SECURITY STANDARDS

4.1   STANDARD STATEMENT

These are minimum physical security related standards that must be adhered to during implementation process. Those standards that may impact on information security have been addressed through the Minimum Information Security Standards. If any standard contained in the Minimum Physical Security Standards document is unclear with regard to the implementation, GSR can be contacted.

4.2   PHYSICAL SECURITY

4.2.1   Physical Security Measures:

The HOD/CEO of a department/institution is responsible for the physical security of the facilities/assets of the institution and must ensure that:

4.2.1.1   The budget of the department/institution provides for the costs of implementing proper physical security measures.

4.2.1.2   The placement of personnel, assets and functions in existing and newly designed facilities is done in a manner that is conducive to the provision of effective and efficient physical security measures within the department/institution.

4.2.1.3   The integration of physical security measures occurs in the early process of selecting, designing or modifying facilities of the institution. Such integration of security measures must entail:

1.   The selection, design and modification of facilities in order to facilitate physical security measures.
2.   The demarcation and control of areas at the facilities.
3.   The installation of the necessary physical security equipment based on the assessments by SAPS-SAS.
4.   The inclusion of the necessary security specifications for tender documentation process.

4.2.1.4   The implementation of physical security measures to:

1.   Delay, detect or prevent unauthorized intrusion to a department/institution.
2.   Activate appropriate responses to such attempts or actual gaining of unauthorized intrusion.
3.   The implementation of physical security measures to safeguard employees contractors and visitors from harm.
4.   The secure storage, transportation and disposal of assets of the department/institution.
5.   The continuous review of physical security measures at facilities of the department/institution in order to reflect changes in the environment and take advantage of new cost-effective technologies.

CHAPTER 5

SECURITY POLICY

5.1   REQUIREMENTS FOR A SECURITY POLICY

5.1.1   It must be a clearly defined document that encompasses the Minimum Physical Security Standards.

5.1.2   It must cover all aspects of physical security and provide for different levels of physical security grading.

5.1.3   It must set out the obligations of the different role players with regard to the implementation of the policy.

5.1.4   The policy must clearly give a direct guide to all personnel and relevant contractors and consultants of the department/institution to adhere / comply with the Minimum Physical Security Standards.

5.1.5   The policy must clearly specify that failure by an employee to comply with the policy and the Minimum Physical Security Standards constitutes serious misconduct and that disciplinary measures must be taken against such a person.

5.1.6   Security Manager to develop operating standard to ensure that they achieve operational objectives.

NB: These can be achieved through exposing employees, contractors and consultants to physical security awareness programmes, by assigning to specific officials the responsibility to develop, co-ordinate and manage physical security training and awareness programmes, including monitoring the compliance with the Minimum Physical Security Standards.

5.2   REPORTING ON SECURITY POLICY

5.2.1   The Security Manager of a department/institution must report to the HOD/CEO of a department/institution on a quarterly basis on the extent to which the policy has been implemented and its prescripts are being complied with and identify any difficulties experienced with the implementation of the policy and make recommendations to the HOD/CEO on how to address those difficulties.

5.2.2   The HOD/CEO must take the necessary steps to address the difficulties identified in the report and must report to the SAPS, including his or her comments.

CHAPTER 6

PHYSICAL SECURITY TRAINING AND AWARENESS

6.1   DEVELOPMENT OF TRAINING AND AWARENESS PROGRAMMES

6.1.1   The security manager of the department/institution is responsible for developing and implementing physical security training and awareness programmes for the department/institution in close cooperation with:

6.1.1.1   The security committee and/or Joint Planning Committee of that department/institution.

6.1.1.2   The training component of that department/institution.

6.1.1.3   SAPS and NIA security related training and awareness programmes.

6.2   IMPLEMENTATION OF SECURITY TRAINING AND AWARENESS PROGRAMS

6.2.1   The Security Manager must:

6.2.1.1   Arrange and conduct the physical security awareness programmes within the department/institution.

6.2.1.2   Determine the needs for physical security training and awareness of personnel, contractors and consultants, make recommendations to the HOD/CEO of the department/institution in this regard and ensure that the training, as approved by the head of the department/institution, takes place.

6.2.1.3   Regularly consult with SAPS (Government Security Regulator) to determine any new developments or changes in the physical security training and awareness fields.

CHAPTER 7

PHYSICAL SECURITY BREACHES

7.1   SECURITY INCIDENTS/BREACHES REPORTING PROCESS

7.1.1   The Security Manager must ensure that all physical security breaches, including the prevented incidents/breaches, are reported to the SAPS for investigation and further handling. Recommended reporting structures stand as follows:

7.1.1.1   Crime related incidents must be reported to the nearest Police Station.

7.1.1.2   Information security related incidents must be reported to NIA.

NB: Reporting of physical security breaches as covered in all security dimensions must at all times be dealt with using the highest degree of confidentiality to protect the reporting individual from any injustice or harm.

7.1.2   The Security Manager must ensure that all staff members are informed, by means of a physical security awareness program, about the procedure that must be followed in the event of the detection of a breach or suspected breach of physical security.

7.2   PHYSICAL SECURITY INCIDENTS/BREACHES RESPONSE PROCESS

7.2.1   Every breach of physical security must be inquired into in order to:

7.2.1.1   Conduct proper investigation process.

7.2.1.2   Assess damage that was caused or could possibly have been caused.

7.2.1.3   Make recommendations regarding steps to be taken to prevent the breach from re-occurring.

7.2.2 All breaches or suspected breaches of security that constitute misconduct by an employee must be dealt with by the head of the department/institution through taking appropriate disciplinary measures against the employee concerned.

7.2.3 All breaches of physical security that may possibly constitute a criminal offence must be referred to the nearest police station for investigation.

CHAPTER 8

CONTINGENCY PLANNING

CONTINGENCY PLANNING

8.1.1 An HOD/CEO of a department/institution must have a contingency plan to provide for the continued availability of critical services and assets if a threat materializes and to provide for appropriate steps and procedures to respond to an emergency situation to ensure the safety of employees and visitors.

8.1.2 The plan must:

8.1.2.1 Set out measures to ensure the regular review and testing of the plan.

8.1.2.2 Ensure that the emergency evacuation procedures are made available for all possible emergencies.

8.1.2.3 Ensure that there is an appropriate number of trained members to assist with evacuation when an emergency occur.

8.1.2.4 Ensure that equipment is available to assist with evacuation in an emergency.

8.1.2.5 Ensure that awareness programmes include emergency evacuation.

8.1.2.6 Ensure that emergency procedures are available in all passages, control rooms and at emergency escape routes.

8.1.2.7 Ensure proper marking of emergency escape routes.

8.1.2.8 Include floor plans of the department/institution.

8.1.2.9 Ensure that assembly points are demarcated, accessible and well-known.

8.1.2.10 Ensure that signals and signs are clearly defined and communicated.

CHAPTER 9

REVIEW AND UPDATE PROCESS

9.1   REVIEW AND UPDATE

9.1.1   The Minimum Physical Security Standards will be reviewed by the SAPS (Government Security Regulator) every five years.

9.1.2   The annexure to MPSS will be reviewed annually to ensure that they are in line with the new technology.

9.1.3   Communication will take place through the GSSC to all relevant role players.

CHAPTER 10

MONITORING

10.1   MONITORING

10.1.1   Audits and inspections will be conducted by the SAPS (Government Security Regulator) monitoring compliance with Minimum Physical Security Standards.

10.1.2   Certain observations may have such a significant impact, that immediate corrective action required. In such cases the auditing shall monitor the condition until satisfactory corrective action had been taken.

10.1.3   Follow-up inspections/audits is the process by which the auditor determines the adequacy, effectiveness and timeliness of actions taken by management on reported engagement observations and recommendations made.

CHAPTER 11

ENFORCEMENT

Senior Management, Security Manager and all employees within the department/institution are responsible for enforcing these Minimum Physical Security Standards.

Non-compliance/infringement of these directives must be regarded as misconduct and must be dealt with in accordance with the disciplinary code of the relevant department/institution.

Annexures will be provided separatly as it will be reviewed annually.

Annexure a: Grading of National Key Points

Annexure b: Grading of Buildings

Annexure c: Grading of Residences

Annexure d: Grading of Newly Built Residences