education

DEPARTMENT: EDUCATION
MPUMALANGA PROVINCE

Private Bag X 11341
Nelspruit 1200
Government Boulevard
Riverside Park
Building 5
Mpumalanga Province
Republic of South Africa

Litiko leTemfundvo   Umnyango weFundo   Departement van Onderwys   Umnyango wezeMfundo

EXAMINATIONS SECURITY POLICY

I, *Mahlasedi Mhlabane*, Head of Mpumalanga Department of Education, after consultation with the Senior Management, hereby declare examination security policy to regulate examination operations in a manner that seek to uphold the integrity of examinations and assessment administration processes.

This policy must be read in conjunction with the Norms, Standards and Procedures for Printing Packing and Distribution of Question Papers; Regulations Pertaining to the Conduct, Administration and Management of Assessment and Examinations; Minimum Information Security Standards (MISS) 1996; and existing security regulations.

MRS. MOC MHLABANE
HEAD OF DEPARTMENT

DATE: 13\14\11

TABLE OF CONTENTS

Contents	Page
1. Introduction	2
2. Overarching Objective	2
3. Purpose	2
4. Examination security policy direction	2
5. Distribution List	3
6. Legal Mandate	3
7. Definitions	4
8. Personnel security	5
9. Document Security	5
10. Communication Security	6
11. Physical Security	6
12. Security incidents/breaches reporting	11
13. Strong room security measures	11
14. Conclusion	12

1. Introduction

The management and administration of examinations is required to be performed by persons with integrity using security competent systems and infrastructure. Lax security controls may compromise the integrity of the examinations in the country in general and dent the reputation of province in particular. Confidence in the examination administration processes in the province is paramount and critical for the public and mostly learners.

The province must have the capacity to detect potential risks and mitigate such to avert possible risk factors may erode the credibility of examination administration systems.

2. Overarching Objective

Entrench excellence, integrity and security competence in the management of examinations administration.

3. Purpose

The purpose of the examination security policy is to provide clearly defined guidelines pertaining to security controls for compliance by exam clients; suppliers; service providers; public examination staff and social partners. The security policy seeks to eliminate security breaches and enhance physical and personnel security competence.

4. Examination security policy direction

Strengthen security systems for the management of examinations and treat all potential, inherent and residual security threats that may undermine the integrity and credibility of examinations.

Examination Security Measures seek to entrench security competency of all officials working in exams; create a secure environment for operations and management of examinations; document procedures and processes to guide examination operations; Provide advanced Information Technology (IT) security enhancements to secure operations; create systems to avert and treat potential threats to the examination administration and create effective communication strategies.

The Department supports security functions and encourages all staff members to support any measures implemented to fulfill security function, such as access control, security patrols and security breaches investigations.

The Department of Education will not be sympathetic towards any fraud and corruption or any action that threatens to bring the department into disrepute.

No strikes or any form of work stoppages that are contrary to Chapter IV of the Labour Relations Act, 1995 will be tolerated. Theft or unauthorized possession of department property/assets/confidential material may lead to dismissal of employee found guilty of such.

5. Distribution List

The examination premises security access control measures relate to security protocol. This guides expected conduct requisite for elimination of security breaches that may lead to the undermining of the physical security competence of premises or areas temporarily or permanently designated for exam administration. Hereunder is list of staff and social partners who are expected to familiarize themselves with prescripts advocated by the provincial examinations security policy.

4.1. Security service providers for examinations/assessment related responsibilities.
4.2. Examination and all departmental staff.
4.3. Examination clients.
4.4. Examinations service providers
4.5. Organized labour and learner formations
4.6. School governing bodies
4.7. Provincial examination board

6. Legal Mandate

6.1. The Control of Access to Public Premises and Vehicles (Act 53 of 1985)
6.2. The Trespass Act (Act 6 of 1959)
6.3. Promotion of Access to information Act, (Act 2 of 2000)
6.4. Firearms Control Act (Act 20 of 2000)
6.5. The Constitution of the Republic of South Africa (Act 108 of 1996)
6.6. Protection of Information Act (Act 84 of 1982)
6.7. Criminal Procedure and Law of Evidence (Act 51 of 1977)
6.8. Occupational Health and Safety (Act 85 of 1993)
6.9. Compensation of Occupational injuries & Diseases (Act 61 of 1997)
6.10. Minimum Information Security Standards (MISS) 1996
6.11. The Code of Conduct for Public Servants
6.12. Private Security Industry Regulatory Act, 2008 (Act No. 56 of 2001)
6.13. National Strategic Intelligence Act, 1994 (Act 39 of 1994)
6.14. Intelligence Services Act, 2002 (Act 56 of 2002)
6.15. Public Service Act 1994, (Act103 of 1994)
6.16. Employment of Educators Act, 1998 (Act 76 of 1998)

7. Definitions

7.1. Access Control

This is a process in which several measures are applied to ensure that any object or person requiring access to the premises has bona fide reasons to gain entry. Such a person with cogent grounds for entry should be authorized thereof and the institution or its employees should not be exposed to danger or breaches of security during the presence of such a person/object.

7.2. Visitors Register

A book that serves as a record of all visitors, that enter and exit a security controlled premises.

7.3. Authorized Officer

In terms of "Control of Access to Public Premises and Vehicles Act 53 of 1985", an authorized officer refers to either the owner of the premises or any person who is delegated by the owner, but for the purpose of this document, authorized officers will refer to Exams Security Service providers appointed by the Mpumalanga Department of Education.

7.4. Random Search

An approach used to, without prejudice, select a vehicle/person to be searched at any time and especially during peak hours.

7.5. Peak Hours

This is the time of heavy traffic through the main entrance at the start and end of business hours.

7.6. Forbidden Items

Items such as firearms, ammunitions, bombs, intoxicating substances or illicit drugs, cameras etc, that are prohibited from the examinations premises or areas designated for examination administration.

8. Personnel security
8.1 Security Clearance

    a. Officials having access to classified information must be vetted in accordance with the level of security clearance allocated to the post in which they occupy and subjected to the need to know principle.

    b. All service providers rendering services to the department must submit their details to security division for screening/vetting purposes.

8.2 Confidentiality Declarations

    c. All officials handling examination material are expected to sign the confidentiality declarations at the beginning of every exam cycle.

    b. All those involved in examinations should also disclose if their next of kin are writing the examinations.

9 Document Security

    c. The responsibility for the grading and regrading of a document rests with the Head of Department or duly authorised designee.

9.1. Question papers and Memorandums

    d. Handling, dispatching, transmitting, sealing and transportation of a question papers and memorandums must be in accordance with the norms and standard for the handling of a national question papers.

    e. Question papers in transit must be highly secured by security escorts. All electronic copies must be kept in a safe and must be soft-blocked with access password.

    f. All confidential data saved on a computer hard drive must cleared after operations.

9.2 Certificates

    g. Certificates application must be processes strictly by those who are authorized for that purpose.

    h. All certificates must be kept in a secured environment.

    i. Tracking system must be in place to allow trace of all certificates issued and confirm receipt by recipients (registered mail can also be used)

    j. Certificate register must be used at every level of receipt and dispatch.

9.3 Confidential examination material

    k. All classified documents that are no longer in use must be destructed in such a manner that the reconstitution of such documents is impossible. If the service is outsourced the destruction certificate must be supplied to the owner of such documents.

    l. The answer books, wrappers, script & question paper satchels remain the property of the department and must not used for another purpose without authorization by Mpumalanga department of education.

    m. Confidential examination material waste must only be disposed after the finalization of examinations and must be kept in safe place that has restricted access during examinations.

10. Communication Security

10.1. Information Communication Technology Security (ICT)

10.1.1. Operations

No one must pose as another especially when using e-mails.

10.1.2. Communication gadgets (data and voice recording devises)

a. Passwords are highly confidential and sharing of passwords is strictly forbidden
b. **No password** will be reset telephonically when forgotten.
c. When a password is lost or forgotten, users must avail themselves to IT managers and fill-in **request form to reset password**.
d. Computer must be lock-off when the user is not in front of his/her computer.
e. Users can keep computers locked by for example: *CRT+alt+Del*, *window+l* or by means of password activated screen saver.
f. All computers must be switched off when knocking-off so that no one may work on it without user knowledge.
g. No one must send e-mails on behalf of anyone except secretaries
h. All computers have an audit on its own, it keeps records of whom logged in/out, when, where and the time.

10.1.3. Telephone/Fax/Email
Maintenance and repairs of the systems must be done by a vetted service provider.

11. Physical Security

11.1. Access Control for Staff

11.1.1. Identification

(a) All accredited personnel will be issued with the official identification cards.
(b) The cards serve as access cards for the motorists' main gate and pedestrian turnstiles.
(c) Biometric system will be utilized at the reception turnstile to gain access.
(d) Staff must use identification cards each time they enter or leave the premises and they must be displayed at all the times.
(e) The department shall ensure that name tags are made available to all personnel and will be displayed at all times as a form of identification when on duty both within premises and elsewhere on official capacity.
(f) Outside clients will not be permitted to enter the designated areas. Authorized visitors will be collected by those visited.
(g) Access to restricted areas will only be allowed to authorize staff.

11.1.2. Employees who are not in possession of their identification cards

(h) Officials who are not in possession of their identification cards will be required to complete staff access control register at every security check point

(i) They will be recorded by security personnel and assisted to gain entry into the premises.

(j) Staff members are not allowed to use their cards to open for others who are not in possession of their own access cards.

(k) No staff member is allowed to use anther staff member's access card to gain entry into the premises or to pose as that staff member.

(l) All officials and examinations monitors or officials appointed for examination related responsibilities are expected to always display their identification cards within examinations designated area.

11.1.3. Lost of Identification Cards

(m) A staff member who loses his/her access card must make an affidavit at the nearest police station stating the circumstances that led to loss of the access card and will be required to pay a replacement fee.

(n) An employee who loses his/her identification card will be charged R120.00 for the replacement thereof.

(o) Worn-out and malfunctioning cards will be replaced free of charge.

11.1.4. Incoming Assets/ Private Property

(p) All staff members shall declare all incoming private furniture, equipment at the security checkpoint upon entering the premises

(q) The security officer on duty shall record such items into the relevant register.

(r) It is the responsibility of the employee to declare his/her private property to security personnel upon entry to the premises. Failure to do so will result in the property not being permitted to leave the premises and will released upon submission proof of ownership.

(s) Any instrument or equipment that may be used to record or reproduce information such as data recording device, camera or voice recorder will not be allowed in high security examination designated area.

(t) Any breach will result in the items being confiscated if found with anyone without authorization.

11.1.5. Outgoing State Property

All state assets being removed from the premises must have official removal permit. No person may be allowed to remove state property out of the premises without proof of permission.

11.1.6. Officials allocated permanently with the state laptops

A list of all officials allocated permanently with state laptops will be made available to security at access control points. The security officers will verify the serial number of the laptop in possession of the official against the one that is on the list each time on entry and exit. Any person who does not appear on register, must register the laptop every time when entering or leaving the premises.

11.1.7. Searches

(u) The intent of searching a person, vehicles, objects, article and containers is to prevent theft and unauthorized items

(v) Searches will be conducted to check cars upon entry/exit regardless of whether the person is staff member or visitor.

(w) Searches and access control measures will be stepped up whenever the risk increases to ensure that the prevailing risk is mitigated.

(x) Body search will be conducted to those who enter/exit the high security designated areas, like where storages and printing areas.

(y) Any person who refuses to be searched or refuses to allow his/her vehicle, object, article, or container irrespective of its nature to be searched will be refused admission or exit in terms of Control of Access to Public Premises and Vehicles Act (Act 53 of 1985)

11.1.8. After-Hours Access

Staff visiting offices after-hours or during week-ends will be required to complete after-hours register at security check point and must also inform the office of the security manager to activate their access rights.

No visitor must be allowed access to the premises after hours unless when accompanied by an authorized official. In such a case the visitor may be permitted within the premises but will not be allowed into the examination building. Only accredited staff with evidence of prior approval may enter the examination building.

11.1.9. Prohibited Substances/items

(z) No alcohol or illicit drugs are allowed within the premises

(aa) Firearms (including licensed firearms) and ammunitions are strictly prohibited and defaulters will be prosecuted. Only service firearms for authorized security services personnel and police are permitted.

(bb) All dangerous weapons and intoxicating substances shall be confiscated and/or not allowed into the premises.

11.2. Access Control for Visitors

11.2.1. Identification

The security personnel reserve the right to request any visitor to produce proof of identification at the security check point and the following identification documents are acceptable:

(a) RSA ID (green bar coded) or RSA Drivers' license
(b) Department's official ID card
(c) Passport

11.2.2. Visitors' Vehicles

The following information of all visitors entering premises with vehicles must be recorded at main gate:

(d) Date and time of entry
(e) Full name, address and telephone number
(f) ID number/Passport
(g) Vehicle Registration number
(h) Purpose of visit
(i) Name of host/Person to be visited
(j) Time of departure
(k) Time of arrival
(l) Signature of the visitor
(m) Signature of the Security Personnel

11.2.3. Recording and Searching

(n) The Security Officials shall ensure that the personal details of visitors are captured on the system e.g. Name, Surname, ID Number and photo. This information will be printed on a label which the visitor should wear on and the label must be visible all the time.
(o) Security personnel reserve the right to search any visitor before access into the premises is granted
(p) All visitors will be attended to at the foyer or client services office allowed further into the building with the exception of accredited service providers.

11.2.4. Visitors with Firearms (i.e. security service personnel and police)

(q) No private firearms and ammunitions are allowed on the premises.
(r) All service firearms for authorized security service personnel and police firearms and ammunitions must be declared on entry together with proof of identity and firearm license.
(s) Details of the service firearm must be logged into the firearm register and the weapon must be made safe by removing the magazine.
(t) Both firearm and magazine with ammunitions must be placed in a safe in the presence of the Security Officer and the key of the safe must be handed to the visitor.

(u)   Firearms without license will not be accepted for safekeeping and such visitors will be denied access into the premises. The office of the Security Manager will be informed for further action.

(v)   Members of SAPS, SANDF and Security Agencies entering on official capacity are allowed to enter with their firearms in line with Control of Access to Public premises vehicles(Act 53 of 1985)

11.2.5.   Prohibited Substances

(w)   No alcohol or illicit drugs are allowed within the premises

(x)   Any person suspected to being under the influence of or in possession of any prohibited substance shall be refused access into the premises

(y)   In the case of illicit drugs being discovered during a search by the Security Officers, the person will be taken into custody and the SAPS will be notified for further handling.

11.2.6.   Types of visitors

(a)   VIP Visitors

Arrangements shall at all times be made with security management in advance whenever VIP visitors are to be received. Such visitors will be identifiable and accredited by the security manager.

(b)   Members of Emergency and Response Units

All identified South African Police Service (SAPS); South African National Defense Force (SANDF) and other government security agencies personnel have authority to enter a security controlled area without being searched if entering is in performance of their duties as per Control of Access to Public Premises and Vehicles (Act 53 of 1985). Identified Ambulance and Fire Brigade personnel will also be allowed access without being searched into the building if entering on official capacity and must be identifiable.
All these personnel should display their identity cards and must be on duty at the time of their visit. If not on official status they will be handled like any other client/visitor.

(c)   Hawkers/Sales people

No hawkers or salesperson/s will be allowed to enter the premises and it is the responsibility of the security personnel to enforce that, unless if the visit has been authorized or confirmed by the Provincial Head of examinations or the Head of Department.

(d) **Journalists**

No journalists are allowed within the exams premises without prior arrangement and approval by the Head of Department or MEC and no exception will be given. Proof of authorization must be produced and all personnel must be registered.

(e) **Members of the Public**

Members of the public who are having examination queries must be directed to the clients' services office or the district head of examinations and the following procedures must be followed by the security personnel at the reception or check point:

    i. Greet them first
    ii. Ask how they can be helped
    iii. Fill-in their information/particulars at the visitors register
    iv. Politely call the host to attend the visitor
    v. Offer them a seat
    vi. Never argue with the clients, even if they are provocative.

12. Security incidents/breaches reporting

a. Staff members must report security breaches immediately within their areas of responsibility to the Head of the Directorate/district head of examinations;
b. Potential security breaches must be deal in the highest degree of confidentiality in order to avoid the leakage of information.
c. Any potential risk must be reported immediately.

13. Strong room security measures

The strong room is one of the critical places where safety should be guaranteed at all times. All question papers must always be securely kept in a strong room

a. The strong room must have double-lock system and keys to the strong room handled by two senior officials.
b. Two officials must be physically responsible for controlling access to the strong room. Each official must be in possession of only one of the two keys to the storage.
c. An updated question paper register for all question papers kept in the strong room must be maintained.
d. A register that records every access to the storage indicating purpose and time spent accessing the strong room must be used.
e. A strong room should always have functional surveillance cameras that record movement and access to the storage.
f. The strong room must be have ventilation and have sufficient light.

g. Separate small safes must be used by designated officials to lock in the keys to the strong room and high security areas
h. The director for public examinations/district head is the only official responsible for safe keeping of spare keys.
i. A strong room must not unnecessarily be kept open for a long time nor left unattended while open

14. Conclusion

Access control is one of the most important measures in the physical protection systems, and it can decisively influence the effectiveness of the entire security system. Due to the nature of security expected for confidentiality of examinations material, security personnel consciousness is critical in the daily security operations. The success of the departments' business depends on the level of security astuteness among all personnel involved in examinations related responsibilities in execution of their assigned tasks.

Security vigilance is essential for upholding integrity and credibility in the management of examinations. All security precautions should be taken to enhance the security competency in the administration of examinations and assessments.

....