

Policy on Security and IT Management

1. Preamble

The purpose of this Security and IT Policy is to ensure the Department of Cooperative Governance and Traditional Affairs assets i.e. information, personnel both movable and immovable assets are secured. Also to ensure safety and secured environment for all clients on the premises.

2. Definitions

Accounting Officer	:	The Head of Department and includes any officer acting in such a post in an institution or Department
COMSEC	:	Communication Security
MISS	:	Minimum Information Security Standard
SACSA	:	South African Communication Security Agency
NIA	:	National Intelligence Agency
NKP	:	National Key Point
Security Vetting	:	The Security Competent Testing conducted to an Individual
Encryption	:	Protection of communication lines for transmitting classified information
Classifications	:	The Grading of Information according to its level of sensitiveness

3. Purpose

The security Manager must draw up business plan to work as a force for the implementation policy within Department.

4. Authorisation /Legal Mandate

4.1 Control of access to public premises and vehicles Act (Act no 53 of 1985)

4.2 Protection of information Act (Act no 82 of 1984)

4.3 Criminal procedure Act (Act no 51 of 1977)

4.4 Fire Arm control (Act no 60 of 2000)

4.5 PFMA (Act no 1 of 1999)

4.6 Promotion of access to information Act (Act no 2 of 2000)

4.7 National Strategic intelligence Act (Act no 39 of 1994)

4.8 Information Communication and transactions Act

4.9 PSIRA Act

4.10 Public Service Act

4.11 National Key point Act (Act no 104 of 1980)

4.12 Trespassing Act (Act no 6 of 1956)

4.13 Constitution of the Republic Act (Act no 108 of 2000)

4.14 National archives Act (Act no 43 of 1996)

4.15 Labour relations Act

4.16 Skills Development Act

4.17 MISS (Minimum Information Security Standard)

5. Policy Framework

5.1 Categorization of information and information classification system

The Department must categorize its information according to the four security discipline levels, that is:

(a) Personnel Security

(b) Document Security

(c) Communication and IT Security

(d) Physical Security

Further more personnel information should be classified into confidential, secret and top secret.

5.2 Personnel Security

5.2.1 Security Screening

All personnel including service providers that are exposed to sensitive information in the Department must be screened by NIA. The officials who are exposed to sensitive information (e.g. Secretaries, Asst. Manager Etc) should all be vetted according to the sensitivity of the information. The Officials may be vetted for confidential, secret or top secret, depending on the information which they are exposed to. It is only in exception cases where immigrants and or a South African Citizen are employed without a Security clearance in a position where he/she will be exposed to sensitive information. The application should be screened immediately after the short listing process, before interviews are conducted. When the applicant is appointed, the vetting process will be fully conducted.

5.2.2 Security Awareness and Training

Management must ensure that security awareness and training takes place in the Department.

5.3 Document Security

The Department must ensure that the security measures are in place to protect information which might be classified either as confidential, secret or top secret.

5.3.1 Communication and IT Security

The Department must ensure that classified information is communicated by using secured communication equipment. SACSA/COMSEC may be consulted in this regard.

Management must ensure that IT Security policy is signed by every employee to secure the IT structure within the Department.

5.4 Physical Security

The Department must ensure that Technical Surveillance Counter Measure is conducted by NIA strategic areas where sensitive information is dealt with.

5.5 IT Security

Management must ensure that IT Security policy is signed by every employee to secure the IT structure within the Department.

5.6 Physical Security

The Department must ensure that physical security measures are implemented. Physical security is dealt with in the MISS document which is available on request.

Business Continuity Planning

The Department must prepare a business continuity plan which will be used in case of any incident, e.g. computer virus, flood etc (it is plan which will assist the Department to continue operating after whatever incident has occurred).

Security Incidents

Breaches reporting process

The Department must ensure that all breaches of security are reported to SAPS and NIA.

Breaches response process

Management and the Security Manager must ensure that all security breaches that have occurred or have been reported are speedily responded to by means of investigation.

Staff Accountability and Acceptable use of Assets

The Management and staff must take ownership of security to ensure accountable and acceptable use of assets. No unauthorized software will be allowed to or used on all computers without approval of the IT /Security Manager

Responsibilities

All sections within the Department must be represented on the Security Committee.

Audience

All the people in business with the Department must comply with the policy, which includes Management, Employees, Contractors and Members of the public.

Implementation

The Head of the Department and Security Manager are charged with the implementation of the policy. Non compliance of this policy must be dealt with as misconduct and its sanctions will be based on a disciplinary code

Communicating the policy

The head of the Department and the Security Manager must communicate the role of the security policy to all stakeholders of the Department by conducting Security Awareness Programmes.

6. Scope of application

The policy will be applicable to all people on business with the Department which will include the following categories:

- Document Security
- Personnel Security
- Physical Security
- ICT Security
- Contract Management
- Toll free line management
- Security Event Management

7. Amendment of the policy

The security Manager with the Security Committee in consultation with other role players of the Department must ensure regular review and update of the policy, based on the factual impact of the legislation and the institution.

8. Monitoring, Evaluating and Report

The Security Manager together with the committee must monitor the implementation of the policy through inspection and audits on quarterly basis.

APPROVED/NOT APPROVED

MR S. NGUBANE

ACTING: HEAD OF DEPARTMENT

DATE_____