DEPARTMENT OF AGRICULTURE

INFORMATION SYSTEM AND INFORMATION TECHNOLOGY SECURITY POLICY AND STANDARDS

1, Introduction.

Information system security entails the creation of a condition to protect computer hardware, software and data against incidental and/or deliberate unauthorised changes, destruction, disposal, removal and/or disclosure.
Information system security is characterised in this policy and standards as the preservation of;
confidentiality: ensuring that information and associated assets are accessible only to those authorised to have access;
integrity: safeguarding the accuracy and completeness of information and processing methods;
availability: ensuring that authorised users have access to information and associated assets whenrequired.

Increasingly, organisations and their information systems and networks are faced with security threats from a wide range of sources, including computer-assisted fraud, sabotage, vandalism, viruses, computer hacking and denial of service attacks. Dependence on information systems and services means organisations are more vulnerable to security threats.

Management shall set a clear policy direction and demonstrate support for, and commitment to, information system security through the issue and maintenance of this information system and information technology security policy and standards. This document shall be read in concurrence with the Minimum Information Security Standards (MISS).

Users of this policy may wish to comment on its contents and are encouraged to copy and return the Policy and Standards comment and change proposal forms via the normal communication channels to the office of the Information Technology.

ANNEXURE 'A'

DEPARTMENT OF AGRICULTURE

DECLARATION BY

Name: _____ **Persal:** _____

IP Address: _____ **Directorate:** _____

I hereby declare that I:

1. Read and understood the contents of the Policy - Procurement, Safekeeping and Maintenance of IT Resources.

2. Agree to comply with the contents mentioned in the above-mentioned policy.

3. Will be subject to disciplinary action in terms of the Disciplinary Code and Procedures of the Public Service for violation of the above-mentioned policy.

4. Allow my employer to investigate and institute charges against me or any violation of this policy.

5. Give my employer permission to intercept my communication, privacy and government property (Hardware/Software) in terms of Regulations of Interception of Communication and Provision of Communication-Related Information Act, 2002 (Act No. 70 of 2002)

_____

SIGNATURE OF USER

DATE: _____

WITNESS:

FULL NAME: _____

DATE: _____

2. Aim

The broad objective is to provide Department of Agriculture with an information system security policy in order to apply an effective and consistent level of security to all information systems that process Department of Agriculture information. Particular objectives are to apply cost-effective protection to security classified information which is processed by department's information systems;

protect sensitive information that is processed by department's information systems; apply a reasonable level of protection to unclassified information so that department's offices can exercise control over that information, particularly in relation to public release;

be able to demonstrate accountability by a structured method of information system security implementation and verification across department's offices; and develop an information system security culture that reflects a consistent approach, based on an understanding of the security issues and a cost-effective way of dealing with them.

3. Scope

The framework, within which the department information system security policy is discussed, is set out under the following headings:
Security management;
Application systems acquisition;
System operation;
Data security;
System access control and password security;
Workstation security;
Communication security;
Personnel security; and
Physical Security.

4. Terms and definitions

The terms and definitions are provided in alphabetical order.

Accountability
Ensuring that the actions of an entity/individual may be traced uniquely to that entity/individual, who may then be held responsible for that action

Audit
Activities to detect and investigate events that might represent a threat to security/independent review and examination of system records and activities in order to test for effectiveness of system controls, to ensure compliance with established policy and operational procedures, and to reification of the identity recommend any indicated changes in controls, policy or procedures

Authentication
Establishing the validity of claimed entity/verification of the identity of an individual or application

Availability
Being accessible and useable upon demand by an authorised entity

Classified data/information
Official department information which has been determined to require protection in the interests of department security according to the MISS definitions

Closed security area
Any area to which general access is prohibited and where authorisation may only be given by the information technology of such an area, for example a LAN room

Code of conduct
Refers to the official department code of conduct

Communication security
Transmission of data from the point of origin to the destination without changing the sequence or content of the data to the detriment of department

Confidentiality
The principle that information is not made available or disclosed to unauthorised individuals, entities or processes

Confidential security classification
The classification allocated to information that can be utilised by aggressors/hostile/opposing/malicious elements to impede the goals/objectives and activities/ functions of an individual and/or institution and of which the unauthorised disclosure could cause damage to the integrity of a person and/or institution or an embarrassment (according to the MISS definition)

Configuration control the management of changes made to a systems hardware, software, firmware and documentation throughout the development and operational life-cycle of the system.

Digital signature
A cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery by the recipient

Discretionary access control
An access control mechanism which restricts access to objects based on the identity of subjects and/or the groups to which they belong. The controls are discretionary in the sense that it allows users that have been assigned certain access privileges to exercise their

discretion in granting other users the same access to system resources, in particular to information

Domain a technology environment with common operational and functional requirements that offers a distinct set of services

Enterprise security ***management I***
The centralised security control and administration of multiple platforms, including distributed as well as mainframe systems, in order to provide for uniform application of security policies

High *security classified information/systems*
Secret or top secret information/systems

Identification and ***authentication***
Functions to establish and verify the validity of the claimed identity of a user

Information *security*
The science and study of methods of protecting information in computer and communication systems against unauthorised disclosure, transfer, modification and destruction whether accidental or intentional

Information *system*
Applications and systems to support the business whilst utilising information technology as an enabler or tool information system domain

An information system that is controlled by a single management authority (for example System Manager) and where all components of the system are subject to a single, system specific security plan

Information *system security*
The protection afforded to information systems in order to preserve the availability, integrity and confidentiality of the systems and the information contained within the systems according to affordable security practices. Such protection is the application of the combination of all security disciplines including information security, communication security, operations security, resource protection, physical security and personnel security

Information system *security policy*
A security policy applicable to all components of information systems in an organisation that address the laws, rules and controls for physical, environmental, personnel, information and information technology security

Information *technology*
Any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display,

switching, interchange, transmission or reception of vocal, pictorial, textual and numerical data or information

In-sourcing
Procurement of skilled resources, managing the contracted personnel as well as their output

Integrity
The inherent quality of protection that maintains the accuracy of entities of an information system and the information in a system and ensures that the entities and information are not altered or destroyed in an unauthorised manner

Key personnel
System personnel whose activities are critical for the effective functioning of the system

Key posts
High risk posts which are filled by persons whose activities may not be interrupted due to the sensitive nature and continuity thereof.

Label
The marking associated with a resource (including data items) which indicates the security attributes of that resource

Local area network
A high bandwidth bidirectional communication infrastructure which enables users to share resources and which operates over a limited geographic area

Local area network security
LAN security entails the protection of the confidentiality, integrity and availability of all information provided or obtained by a LAN, as well as that of the LAN resources

Logical access control
Access control mechanisms that are implemented and enforced by network operating systems, operating systems, application software and communication processes (for example authentication, resource access, audit etc)

Mandatory access control
An access control mechanism which partitions system resources according to the sensitivity of the information contained in the objects (as represented by a label) and the formal authorisation (for example security clearance) of subjects to access information of such sensitivity on a need-to-know basis. Predetermined access rules are implemented within the trusted system hardware and software so that access to a particular partition is not left to the discretion of other users

Department system
Any system processing DoA information, including systems developed by the department as well as systems managed by the DoA

Monitoring
Performance measurement to ensure the confidentiality, availability and integrity of operational systems and information

Need-to-know
A policy that restricts access to classified information to personnel whose duties necessitate such access

Non-rep udiation
A service that provides proof of the integrity and origin of data, both in an unforgettable relationship, which can be verified by any third party at any time in order to protect a recipient against the false denial by an originator that the data has been sent and to protect an originator against the false denial of a recipient that the data has been received (for example electronic signature)

Open security classification
Minimal security protection required

Outsourcing
The practice of procuring services from external specialist sources rather than developing the expertise within the organisation itself, managing only the output as contractually agreed upon

Password
Confidential authentication information composed of a string of characters

Physical access control
Physical control measures to prevent and/or detect unauthorised access to a security area

Physical security
Measures used to provide physical protection of resources against deliberate and/or accidental threats

Program library
Where the source codes of programs, utilised by programmers to change/update the programs/system, are kept

Remote access
The access of remote users to corporate IT services through a gateway (for example dial-back facility)

Restricted security area
Areas to which access is restricted and controlled; it need not necessarily be fenced off by a security fence

Security classification
The classification allocated to information that can be utilised by aggressors/hostile/opposing/malicious elements to disrupt the goals/objectives and functions/activities of an institution and/or the state and of which the unauthorised disclosure could disrupt the effective functioning of DoA and/or the state or disrupt the operational co-operation between institutions (according to the MISS definition)

Security domain
Entities subjected to a single security policy with a specific set of security rules and administered by a single authority

Security management
The establishment and enforcement of security policies, the management of security services, mechanisms and objects, and the auditing/monitoring of the security environment

Security mechanisms
The tools and techniques employed to implement security services

Security services
An activity that enhances the security of information systems and information/data transfer

Sensitive information
Any security classified information which requires a specific degree of protection and safeguarding and which should not be made generally available

System integrity
The ability of a system to prevent the circumvention or bypassing of its security mechanisms

Threat
A potential violation of security

Top secret security classification
The classification allocated to information that can be utilised by aggressors/enemies/hostile opposition/malicious elements to neutralise the objectives/goals and functions/activities of NDA and/or the state and of which the unauthorised disclosure could cause exceptionally grave damage to national security (according to the MISS definition)

CONTENTS

15.4 Fire safeguarding
15.5 Movement control
15.5.1 Personnel
15.5.2 Visitors
15.6 Removal control
15.7 Transport control

Annexure A - Policy and standards comment and change proposal form
Annexure B - System registration form
Annexure C - Oath of secrecy
Annexure D - Authorisation for the removal of computers and IS/IT equipment

7, Security management

7.1 *Aim*

To describe the minimum security measures that shall be implemented and applied to ensure that an effective and consistent level of security management is applied to Department of Agriculture computerised systems. Security management entails all the security aspects of information systems, including the management of security services and mechanisms. The aim is to protect systems, data and applications according to its sensitivity and criticality against unauthorised access, and to protect computer hardware, software and data from accidental or deliberate unauthorised changes, destruction, disposal, removal and/or disclosure.

7.2 *Fundamental information system (IS) security management principles*

This policy is based on the results of a risk assessment which indicated that no security classified or critical information is processed by any DoA system and security protection shall thus be afforded accordingly. The following fundamental security principles are applicable:

7.2.1 Management accountability

Management shall be accountable for the implementation of controls that will ensure that the policies described in this document are adhered to.

7.2.2 Individual accountability

Any person who has authorised access to an information system under control of the DoA shall be responsible and accountable to follow recommended procedures and to take all reasonable steps to safeguard the information handled by that system as well as the assets involved. All information systems shall provide a means by which individual users can be held individually accountable for their actions in terms of the DoA code of conduct.

7.2.3 Confidentiality

Users of an DoA information system shall be responsible, as far as reasonably possible, to ensure that no actions are taken which could degrade or compromise the confidentiality levels of the programs, services and information handled by the system.

7.2.4 Integrity

Users of an DoA information system shall be responsible, as far as reasonably possible, to ensure that no actions are taken which could degrade or compromise the required level of accuracy, completeness and reliability of the programs, services and information being handled by the information system or its assets.

7.2.5 Availability

Any user of an DoA information system shall be responsible to ensure that no actions are taken which could degrade or compromise the required level of availability of programs, services and information being provided by the information system to support the stated operational or managerial requirements.

7.2.6 Controlled access

The management of access control shall be the responsibility of the respective DoA offices.A person or any system component shall be granted access to only that information and assets for which appropriate access authorisation(s) and an established need-to-know have been approved. A person or any system component shall be granted access to only those information system resources necessary to perform the assigned task(s) and only when such access will not lead to a breach of this or any other security principle. Controlled access is normally achieved via physical and procedural means.

7.2.7 Least privilege

A person or any system component shall be granted the most restrictive set of privileges needed for the performance of authorised tasks. Least privilege is normally achieved via technical means once access has been granted.

7.2.8 Levels of protection

The protection provided to an DoA information system shall be commensurate with the sensitivity levels of the information and assets involved and shall take into consideration the identified threats to and vulnerabilities of the information system.

7.2.9 Continuity of protection

The minimum security standards, requirements and mechanisms for an information system shall not be degraded except where it may be necessary to temporarily support an immediate operational necessity which clearly outweighs the potential security risks involved.

7.2.10 System stability

All elements and components of the information system shall function in a cohesive, identifiable, predictable and reliable manner so that malfunctions can be detected and reported within a predictable period of time

7.2.11 Survivability

The organisation employing an information system shall be capable of providing for continuity of operations to meet minimum essential levels of services.

7.2.12 Security classification and utilisation of IS resources

All data, information, software and hardware shall be classified In accordance with the classification of the application system it supports. The access, transmission, transport, storage, disposal, publishing, copying, changing and protection of data, information, software and hardware shall only be performed in the prescribed manner and conditions as presented in this policy.

7.3 IS security infrastructure

The management of security can be subdivided in three basic levels -strategic, tactical and operational. The functionaries at the strategic level shall determine the threat, set high level policy and address issues in terms of security services. In the second or tactical level, the focus is on business requirements, the security mechanisms and the appropriate standards. The two higher levels operate at a corporate level. The functionaries at the third or operational security level, shall be responsible to implement these measures.

7.3.1 IS security organisations/junctions

A management framework shall be established to initiate and control the implementation of information system security within DoA offices. The respective DoA offices shall be responsible to develop their own information system security procedures in line with the prescripts of this policy. Security roles and responsibilities shall be allocated.

7.3.1.1 Departmental information technology committee

The departmental IT committee shall ensure clear direction and visible management support for managing security initiatives. The committee is responsible for;

a. the co-ordination and control of information system security services in the DoA;
b. the co-ordination of the insourcing of IS/IT security expertise and outsourcing of security services on advice of the GITO;
c. the providing of guidance to authorities involved in the development of information systems and heads of DoA offices on the implementation of IS/IT security on advice of the GITO;
d. the delegation of responsibilities to provide, review and approve high level IS/IT security policies and standards; and
e. the assessment of priorities with regard to specific information system and information technology security requirements.

7.3.1.2 State Information Technology Agency (SITA)

SIT A is responsible to maintain a comprehensive information system security environment according to approved policy and standards.

7.3.1.3 South African Communication Security Agency (SACSA)

SACSA is according to legislation responsible for the promulgation of policy with regard to telecommunications equipment and telecommunications security in the State.

7.3.2 Security appointments and responsibilities

Responsibilities for the protection of IS related assets and for carrying out specific IS related security processes as required by this policy, shall be clearly defined and allocated to specific officials.

7.3.2.1 Government Information Technology Officer (GITO)

The GITO acts as the controlling authority for the management of DoA information systems and is responsible for

a. the development and maintenance of DoA information system security architecture to be applied in the design, implementation and evolution of all DoA information system infrastructures;
b. the identification of security mechanisms, products and approaches relevant to the implementation of DoA information system security architecture within budgetary constraints;
c. the formulation of a security strategy applicable to all DoA systems;
d. the management of DoA information system security policies and standards for DoA systems;
e. the publication of required DoA information system security implementation guidelines;
f. the evaluation of compliance with information system security policies and standards in conjunction with SITA;
g. ensuring IS/IT security awareness and training for DoA information system users in cooperation with SITA; and
h. virus control on all DoA systems.

7.3.2.2 System Manager

The System Manager is responsible for the secure operation of the respective information systems in accordance with the prescripts of this policy. He/she acts as liaison between the System Owner, the system users and support personnel.

7.3.2.3 Network Administrator

The Network Administrator is accountable for the management and administration of the DoA network (Agrinet) as well as the secure operation of the network. He/she acts as liaison between the System Owner, the system users and support personnel.

7.4 *Threat and risk assessments*

7.4.1 Security analysis

Risks that computer hardware, software, data, buildings, organizations, support services and projects are exposed to shall be identified. A threat and risk assessment shall be executed on every information system and network which handle critical information or have sensitive assets.

7.4.2 Risk measurement

Identified risks shall be quantified and described in terms of the probability of them occurring, in monetary value and the impact on service delivery. The potential consequences of a loss of confidentiality, integrity and/or availability of the information shall also be determined.

7.4.3 Information system security plan

In order to make an evaluation of the specific security threats within the respective DoA offices, security plans shall be compiled and maintained by the head of the specific office. The plan shall address the assets to be protected, the control objectives and controls, and the degree of protection required.

7.4.4 Control measures and procedures.

In order to minimise risks, such measures and/or procedures shall be established to help prevent, detect and correct a potential risk. The expected time when control measures must be implemented and the officials responsible for implementation shall be stated. Control measures and procedures shall be revised regularly.

7.5 *Disaster recovery planning*

7.5.1 Business continuity management

A business continuity strategy and management process shall be implemented to reduce the disruption caused by disasters and security failures to an acceptable level by means of preventative and recovery controls. Contingency plans shall be developed and implemented to ensure that business processes can be restored within the required time-scales. Such plans shall be maintained and practiced to become an integral part of all other management processes.

7.5.2 Disaster recovery plans

Every DoA office shall have a documented and updated disaster recovery plan and emergency procedures for each system that has to be recovered in the event of an emergency, approved by the GITO. Disaster recovery plans shall be tested annually, evaluated and continually updated. The GITO shall be notified timeously of any live disaster recovery exercises. No exercises with regard to mainframe systems and bigger distributed systems shall take place without authorisation of the GITO. Security responsibilities shall be identified and allocated. The conditions for activating the plan shall be clearly stated.

7.5.3 Recovery plan classification

A disaster recovery plan is a blueprint of the weaknesses of an organisation, and it is therefore a document which shall be distributed on a "need-to-know" basis. The recovery plan shall at least be classified confidential.

7.6 Internal monitoring

7 .6.1 Monitoring questionnaire

A monitoring questionnaire shall be compiled in order to conduct planned as well as random internal monitoring. The questionnaire shall address all the security-relevant aspects with regard to the information system configuration and network in accordance with the prescripts of this policy.

7.6.2 Monitoring tools

Monitoring tools shall only be utilised by authorised officials to perform integrity checks on system software and to check for configuration vulnerabilities.

7.7 Auditing

7.7.1 Audit planning and authorisation

There shall be controls to safeguard operational systems and audit tools during system audits. Audit requirements and activities involving checks on operational systems shall be carefully planned and executed to minimise the risk of disruptions to business processes. No external audits shall be executed without the authorisation of the GITO. The scope of the checks shall be agreed, controlled and limited to read-only access to software and data. The system/domain being audited, shall be isolated/compartmented to ensure that the confidentiality, capacity and performance of the other systems/domains are not jeopardised. All access shall be logged to produce an audit trail. An appointed DoA official shall be present during external audits.

7.7.2 Audit tools

Access to audit utilities (e.g. audit/monitoring/sniffing tools), that might be capable of overriding system and application controls, shall be restricted to authorised officials and controlled to prevent any possible misuse or compromise. Monitoring/sniffing tools may only be used with the approval of the GITO. Such tools shall be protected by password/authentication procedures and shall be separated from development and operational systems/application software. It shall not be held in software libraries or user areas, unless given an appropriate level of additional security protection. An audit trail of all the actions executed by audit utilities shall be kept.

*7.8 **Breaches** of security*

Incident response procedures shall be established to cover all types of security incidents including system failures, loss of information, malfunctions, security threats, weaknesses and/or breaches that might have an impact on the security of DoA systems and/or information.

7.8.1 Reporting breaches of security

Users of DoA services shall be made aware of the procedure for reporting security incidents and be required to report any observed or suspect actions/security weaknesses in, or threats to, systems or services. Ail breaches of security shall be investigated and reported as follows:

7.8.1.1 Deliberate breaches of security

As soon as an alleged breach of information system security has been detected and any form of sabotage, or subversion is suspected, the individual who detected it shall report it to the GITO via the appropriate management channels for further investigation. A formal disciplinary process shall be established for dealing with employees who have violated DoA security policies and procedures or have committed a deliberate breach of security.

7.8.1.2 Incidental breaches ofsecuriry

When an alleged breach of information system security has been detected/identified and it is suspected that the breach was incidental due to ignorance, negligence and/or inadequate measures, the matter shall be investigated and reported to the GITO.

7.8.2 Corrective measures.

All security incidents shall be investigated to identify and analyse the cause of the incident. Corrective measures shall be submitted to the GITO for approval and immediate implementation.

*7.9 Security **awareness***

All DoA system users shall undergo an IS security orientation program before being registered on an DoA system. Effective and appropriate information system security awareness shall be provided by the System Manager/Administrator to all system users having access to DoA information systems within his/her area of responsibility.

Security briefings shall clarify security responsibilities with the aim to continually educate users.

*7,10 **Outsourcing***

7.10.1 Business agreement

When the responsibility for DoA information processing is outsourced to SIT A or any another organisation, security controls and procedures shall be addressed in a Business Agreement (BA) between the parties to ensure that the security of DoA information is not compromised.

7.10.2 Security management plan

A security management plan shall be compiled and at least the following aspects shall be addressed:

7.10.2.1 how the legal requirements are to be met, for example data protection legislation;

7.10.2.2 what arrangements will be in place to ensure that all parties involved in the outsourcing, including sub-contractors, are aware of their security responsibilities;

7.10.2.3 how the integrity and confidentiality of DoA's business assets are to be maintained and tested;

7.10.2.4 what physical and logical controls will be used to restrict and limit access to DoA business information to authorised users;

7.30.2.5 how the availability of services is to be maintained in the event of a disaster;

7.10.2.6 what levels of physical security are to be provided for outsourced equipment; and the right of audit.

7.10.3 Service level agreements (SLA)

The SLAs with SITA or any other organisation shall clearly define the level of security that will be contracted for the development, maintenance and operation of a system. The degree and time required for system recover ability shall also be specified.

8. Application systems acquisition

8.1 ***Aim***

To describe the minimum security requirements that shall be adhered to during the acquisition of new DoA application systems to ensure that security is built into the systems.

8.2 ***Business/users requirement*** *specification*

The business/user requirements for new systems or enhancements to existing systems shall specify the specific security objectives of the system as well as the security control requirements, including the need for fall back arrangements.

8.3 System ***design***

8.3.1 Security specifications

The preventive, detection and corrective security control measures and procedures specified in the business/user requirement specification, which protect hardware, programs and data against deliberate or negligent changes, destruction or sabotage, shall be integrated into the system acquisition plan and incorporated into the design specification of the system. Capacity demands shall be noted as well as projections of future capacity requirements to ensure that adequate processing power and storage are available.

8.3.2 Security testing plan

A security testing plan shall be drawn up for the testing of the security features to ensure that the system operates as described in the documentation. The detail regarding what must

be tested and what equipment must be used, shall be spelled out. All security aspects of the system shall be documented and the documentation shall be updated regularly.

8.4 System development

Control measures and procedures for the protection of programs and data, as specified by the specific DoA office, shall be built in, tested and audited to ensure that data and programs cannot be changed (amended/updated) without authorisation, destroyed or subjected to sabotage due to negligence or on purpose. A system manual shall be compiled at the start of the system development phase. All security aspects in respect of the system shall be documented and the documentation shall be updated regularly.

8.5 System testing and evaluation

Before acceptance of a system, an audit of the set security measures shall be done by designated security auditors who were not involved in the development of the system. All emergency maintenance programs (e.g. trapdoors, super zaps, aches etc.) shall be removed before a system is installed. Systems shall be audited for harmful software (e.g. logic bomb) by the designated security auditors before installation and implementation. All security audit actions shall be documented. The testing of the security measures shall be continued during the system life cycle to ensure that the security objectives are met and that controls operate as intended.

8.6 Procurement of computer-related equipment and software

8.6.1 Procurement policy

The acquisition of IS/IT requirements (i.e. computer and computer-related equipment and software) shall be done in accordance with the State procurement policy. Purchasing of computer-related equipment and software shall only take place with the approval of the GITO or delegated authorities.

8.6.2 Security standards

Security standards applicable to the operation and administration of computer and computer-related equipment and software which shall be implemented shall be set by the GITO in conjunction with the relevant DoA offices.

8.6.3 Equipment certification

Computer products (including commercial off-the-shelf (COTS) products) shall not be purchased/installed without the approval of the DITC. A current systems register shall be kept.

8.7 Self-developed software

8.7.1 Security implications

Requests for the writing of own programs for the improvement of local procedures shall be submitted to the DITC for approval and shall contain full particulars of the intended application and security implications.

8.7.2 Copyright

The program, plus source code, shall be registered at the office of the GITO in order to apply quality control to the development process and to facilitate adequate configuration management of the software. The program shall not interfere or be in conflict with the existing laid down systems. All programs developed in this way shall remain the property of the DoA, which holds the copyright.

9. System operation

9.1 Aim

To describe the minimum security requirements that shall be implemented to protect the computer configurations of DoA offices against sabotage and actions endangering security in achieving secure system operation.

9.2 System implementation

All computer hardware and software with regard to new systems shall be implemented in terms of an implementation plan. The implementation plan shall address the activities related to the coordination and implementation of the security measures and specify acceptance criteria to be met before the system is put into operation.

9.3 Documented operating procedures

System operating procedures shall be documented and maintained to ensure the correct and secure operation of information processing facilities. The procedures shall specify the instructions for the detailed execution of each job including processing and handling of information, scheduling requirements, error handling, use of system utilities, output handling and disposal, back-up, equipment maintenance, system restart and recovery.

9.4 Configuration management

9.4.1 Inventory management

An inventory/asset register shall be drawn up and maintained in accordance with the prevailing Government prescripts.

9.4.2 Configuration control

All DoA information systems shall be subject to configuration controls to ensure that configurations are known and only authorised changes are implemented. Configuration management shall ensure that any additions, omissions or changes made to the system are authorised and do not compromise the set security measures. It shall be ensured that a standard for controlling proposed changes to the information system environment is established. All configuration changes shall be recorded and fully documented. Configuration management shall be implemented throughout the life cycle of information systems.

9.5 System amendments

9.5.1 Change control

Procedures for controlling proposed changes to the information system environment shall be established. Strict and prescribed system standards as well as programming standards shall be complied with to ensure that no unauthorised changes to DoA, programs, software or procedures can be made. Before a system amendment can be made, control measures and procedures shall be in place to ensure that data is protected against deliberate or negligent changes, destruction and/or sabotage.

9.5.2 System testing and audit trai1

When changes have been made to a DoA system, the amendment shall be tested and the system documentation shall be updated accordingly. It shall be assured that amendments are done according to change control procedures and do not contain detrimental software. An audit trail of all relevant information about the changes to the system/program shall be kept.

9.6 Information back-up

9.6.1 Back-up of Information on the file servers shall be made on a daily/weekly/monthly basis according to the applicable procedures. Individual users are responsible for their own back-up on microcomputers. Procedures shall be established for the taking of back-up copies of essential business information and software to ensure that it can be recovered following a disaster or media failure. Back-up arrangements for individual systems shall be regularly tested to ensure that they meet the requirements of business continuity plans and that they can be relied upon for emergency use when necessary.

9.6.2 Back-up copies shall be stored off-site and be given an appropriate level of physical and environmental protection consistent with the standards at the main site.

9.6.3 The retention period for back-up copies of essential business information shall be determined and documented. Where possible, outdated technology shall also be retained in order to retrieve archived information.

9.7 System maintenance

The maintenance of hardware and software shall only be done by authorised contractors. All DoA system users shall ensure that computer hardware and software are handled and used according to vendor specifications.

9.8 Documentation control

9.8.1 System supporting documentation

Complete, updated manuals/documentation shall be available to operators, programmers, system analysts, users and auditors as applicable. The System Manager shall authorise the access list for users who may gain access to specific system documentation. Backup copies shall be made of all electronic documentation and be stored in a geographically separate location in a safe.

9.8.2 Classification of documentation

Applicable security classifications shall be allocated to the documentation and be controlled, handled, distributed, stored and disposed of in accordance with the allocated security classification (See terms and definitions). System documentation held on/supplied via a public network shall be appropriately protected.

*9.9 **Disposal** of computer-related articles*

9.9.1 Disposal of hardware

If computer equipment and/or software become obsolete, unserviceable, damaged and/or a newer version of the article exists, only the D: FPA may approve the disposal of the article concerned. It shall be ensured that all data has been removed from any hard disk/storage device by the owner of the equipment before disposal. If a hard disk/storage device containing sensitive information cannot be accessed electronically, it shall be stored in a safe until it can be destroyed in accordance with the prescribed procedures.

9.9.2 Disposal of records and information

Guidelines shall be issued to users on the retention, storage, handling and disposal of records and information. A retention schedule shall be drawn up identifying essential record types and the period of time for which it shall be retained. Appropriate controls shall be implemented to protect essential records from loss, destruction and falsification. The disposal plans for computer documents and records shall be submitted to the DFPA for approval. Disposal of critical items shall be logged, where possible, for future reference and to maintain an audit trail.

9.9.3 Disposal of data

When data which forms part of a transversal system is disposed of, the GITO shall obtain written comments from other users or System Managers in respect of the impact of the disposal on their systems. The request to dispose of data on a transversal system shall be submitted to the Treasury for authorisation. A data disposal system shall be established to ensure that archived data is disposed of in an orderly manner. Disposal shall be performed in compliance with the National Archives of SA Act. Measures shall be in place to ensure that classified information is not compromised in the disposal process.

9.9.4 Disposal of data media

When data media (for example magnetic tapes, microfilms etc) are to be disposed of, the disposal requirements of the computer records on the media shall be noted. Media containing sensitive information shall first be declassified and then be disposed of securely and safely, for example by incineration or shredding.

10 Data security

*10.1 **Aim***

To describe the minimum security control measures and standards applicable to the administration of data from creation to disposal to ensure that electronic data is not changed, destroyed, disposed of or exposed to sabotage deliberately or incidentally.

10.2 Responsibilities and delegation in respect of data security

10.2.1 Liability

All data on databases is the property of the DoA and the responsibility to manage the data and ensure integrity is delegated to the System Manager.

10.2.2 Responsibility

The System Manager is the data possessor and is accordingly responsible for the maintenance of the data. The data integrity responsibilities are delegated to the user level where data is generated.

10.3 Database management system (DBMS)

A database management system(s) which ensures data security shall be established. The system(s) shall make provision for the aspects listed below.

10.3.1 Accounting of data

It shall be ensured that the integrity of existing data can be assessed regularly. The monitoring of data integrity shall be done according to a predetermined year plan. If the data calculation did not meet the accuracy and integrity standard, corrective measures shall be implemented.

10.3.2 Control of input data

Controls to ensure the accuracy and integrity of the input transactions from source documents, to prevent the deliberate input of corrupt data or the incidental loss of correct data, and to ensure that transactions meet the requirements of accountability, integrity and auditability, shall be implemented. A valid signature which certifies an adequate authorisation of the source document with the input data shall be used.

10.3.3 Processing controls

Processing control measures and validation checks shall be implemented to detect and correct errors during the processing phase and to validate the integrity of the data. Errors and problems detected during the processing process shall be logged.

10.3.4 Error handling

Detailed error handling procedures shall be established. An error and correction control log book shall contain all the relevant information regarding errors and corrective actions.

10.3.5 Output controls

Output control measures to verify the accuracy and integrity of processed information, as well as the correct distribution of outputs to the appropriate authorised officials, shall be implemented. The retention period of critical output reports, lists and documents shall be defined and documented by the System Owner. The security classification of outputs shall be indicated.

11. System access control and password security

11.1 Aim

To describe the requirements for system access control and password security in order to implement and maintain an effective level of protection for the IS services and data of DoA offices.

11.2 System access control

11.2.1 Logical access control

11.2.1.1 Access to restricted DoA computer systems shall be controlled by means of an approved computer access control system which identify and verify the identity of each authorised user. Procedures shall be implemented to control the allocation of access rights to systems and services.

11.2.1.2 Access to multi-user information services shall be controlled through a formal user registration process. Unique user IDs shall be allocated so that users can be linked to and made responsible for their actions. The use of group IDs shall only be permitted where they are suitable for the work carried out.

11.2.1.3 A user shall meet the minimum security requirements of the job description before registration as a system user. The level of access granted shall be based on the need-to- know principle and shall not compromise segregation of duties. The User Manager shall compile a user profile for every user, based on what system(s)/data field(s) the user requires access to.

11.2.1.4 A formal record shall be maintained of all users registered to use the service. Access rights shall be reviewed at regular intervals. Access rights and user IDs of users who have changed jobs or left the DoA shall immediately be removed and not be issued to other users.

11.2.2 Mandatory access control

The System Manager shall allocate access rights to a database and the entities in it, to various subjects (users) according to their security profiles. Access to objects (entities) in the database shall be based on the allocated access rights and shall be controlled by the database control system.

11.2.3 Secure logon

Access to DoA IS services shall be via a secure logon process. The users of the system shall be identified uniquely by means of a user identification. After the correct user identification, a password shall be given. The secure logon process shall comply with the following security requirements:

11.2.3.1 System or application identifiers shall not be displayed until the logon process has been successfully completed.

11.2.3.2 Help messages shall not be provided during the logon procedure that would aid an unauthorised user.

11.2.3.3 The logon information shall be validated only on completion of all input data. If any error condition arises, the system shall not indicate which part of the data is correct or incorrect.

11.2.3.4 The number of unsuccessful logon attempts shall be limited to three before action is taken to force a time delay before further logon attempts are allowed, disconnect data link connections and/or disallow future logon completely.

11.2.4 Privilege management.

The System Manager shall allocate only the minimum access privileges to each DoA system user which will enable him/her to perform his/her job effectively. The use of special privileges shall be restricted and controlled through a formal authorisation process and on a need-to-use basis and revised at regular intervals. Special privileges shall be assigned to a different user identity from those used for normal business use. A record of all special privileges allocated shall be maintained.

11.2.5 Cancellation of access

If a user does not use the system(s) for 30 days, access shall be suspended automatically by the system and the user shall be removed from the system after 6 months. If the user no longer needs partial or complete access to the information on the computer system(s), the access authorisation of such a user shall be cancelled or amended immediately. Clearing out procedures shall make provision for a member to be removed from the system(s).

11.2.6 Audit trail

The access control system shall update an audit trail of all authorised as well as unauthorised efforts to gain access to DoA computer systems, and shall be monitored by the System Manager or his/her delegate. This shall include the identification of suspicious access trends, e.g. after hour system accesses etc. Unauthorised access attempts shall be handled as a breach of security and shall be followed up.

11.2.7 Monitoring of remote access

11.2.7.1 Remote access shall be discouraged.

The allocation of remote access rights to authorised systems personnel shall be done in accordance with the DoA Remote Access Policy. The GITO shall keep record of all DoA system users to whom remote access rights have been granted.

11.2.7.2 Control measures and procedures shall ensure that

a. no access is given to any of the production sites. Applications for such access shall be fully motivated and will only be approved in exceptional cases by the DITC;

b. only approved dial-back modems and numbers are used for authentication;

c. the remote access rights are monitored continually in terms of its essentiality, as well as the application of the prescribed security measures;
d, access is limited to only that data which is absolutely essential to the performance of the user's job. If any additional access is required to any system(s) other than the access that was originally approved, the DITC shall authorise such a request;
e. access to the system is only gained through a single point of entry; and
f. re-motivation, re-application, re-assessment and re-authorisation of such requests are done annually as well as in the case of transfers or relocations.

11.2.7.3 Documentation needed for inputs away from DoA premises shall be subjected to all the existing documentation security and removal control measures.

11.2.7.4 In the case of dismissals/suspensions, remote access to all systems shall be terminated immediately.

11.2.8 Third party access control

Access to the IS facilities of DoA offices by non-DoA third parties shall not be provided unless the appropriate measures have been implemented and a contract has been signed defining the terms of the access. Third parties shall be subjected to all the requirements of this policy.

*11.3 Password security **and management***

11.3.1 Password security

System passwords shall be individual and exclusive, allocated with discretion, and it shall not be disclosed without authorisation. Passwords with a minimum length of 6 characters shall be selected. DoA system users shall change passwords on receipt and sign an undertaking to keep personal passwords confidential. Unauthorised disclosure shall be considered a breach of security and an infringement of Sections 3 and 4 of the Protection of Information Act or any other applicable legislation.

11.3.2 Password administration

11.3.2.1 Password administrators shall control the allocation and amendment of passwords. Administrators as well as owners of master and sub-master passwords shall be appointed in writing, and the appropriate segregation of duties shall be applied.

11.3.2.2 Temporary passwords shall be conveyed to users in a secure manner and users shall be forced to change it immediately. Users shall change their passwords at least once every three months. The access control system shall force the user to change the password by refusing access to the system after the specified time.

11.3.2.3 The password database shall be classified at least secret and administered accordingly. Password files shall be stored separately from the main application system data.

11.2.3.4 An audit trail shall indicate which amendments have been made to passwords. The password administrator shall monitor the information regularly and any irregularities shall be reported through the normal service channels to the GITO for further investigation.

12. Workstation security

12.1 Aim

To describe the preventive, detection and corrective control measures that shall be implemented to ensure that DOA workstations are not exposed to sabotage and/or actions endangering security.

12.2 Safeguarding of hardware and peripheral equipment

12.2.1 Physical protection

DoA workstations shall be located in a physically protected environment where access control measures are in place and applied consistently. It shall be ensured that unattended equipment has appropriate security protection. Microcomputers shall only be used for official DoA purposes.

12.2.2 Safeguarding of portable computers

Portable computers (e.g. laptops and notebooks), containing classified data shall not be linked to modems or equipped with fax cards without approval of the DITC. Devices not equipped to protect data (for example Palmtops) shall not be used to receive, store or process critical data. An official anti- virus package shall be installed and updated regularly. Only approved software and utility programs shall be loaded on portable computers. Portable computers shall not be linked to the P ABX system while also connected to the DoA network. Removal control measures shall be complied with.

12.2.3 Safeguarding of stand-alone microcomputers

12.2.3.1 Access to stand-alone microcomputers on which critical data are processed, shall be controlled and limited by means of DoA approved access control software and/or hardware. Active sessions shall be terminated when leaving the workstation or a password protected screen saver shall be installed.

12.2.3.2 The menu system shall be configured to discourage use of the operating system command shell directly.

12.2.3.3 Under no circumstances shall anyone other than authorised maintenance personnel be allowed to change any of the hardware or the complementary metal-oxide semi-conductor (CMOS) settings. Written approval of the GITO shall be obtained before any changes to the CMOS settings are implemented. DoA ownership of new equipment shall, where technical possible, be embedded in the CMOS setting.

12.2.4 Hardware modification and repair of microcomputers

Only authorised contractors shall be approached for the repair or modification of microcomputers. When a computer has been repaired, the hardware shall correspond with the configuration that was initially approved. If a hard disk containing classified information must be removed from an DoA premises, it shall be formatted before being repaired. Storage media (stiffies, CDs, hard discs) shall be removed from equipment before being repaired.

12.3 Safeguarding of software

12.3.1 Software and documentation storage

The acquisition of microcomputer software shall be done in accordance with the relevant procurement prescripts. Only authorised software and licenced products shall be installed. Only standard screen savers approved by the DITC or provided by the Microsoft operating system shall be utilised on DoA computers. All computer-related software and documentation shall be stored and safeguarded in accordance with prescribed storage specifications. Access to classified software shall be controlled in terms of the security classification of the software. No configuration changes shall be made to software packages.

12.3.2 Copyright act

The stipulations of the Copyright Act (Act No 98 of 1978, as amended from time to time) shall be complied with at all times. No unauthorised copies shall be made of software for official or personal use. Transgressions shall be dealt with in accordance with the DoA code of conduct.

12.3.3 Software inventory

An inventory shall be kept of all purchased as well as semi-developed software. The licence agreements of proprietary software shall be stored safely.

12.3.4 Anti-virus control

Measures for the prevention, limitation and elimination of malicious software/viruses shall be in place. The use of unknown or unauthorised software is prohibited. Any electronic media of uncertain origin shall be checked for viruses before use. An DoA approved anti-virus package shall be installed on every workstation and be updated regularly to keep track of technological developments in this regard. Procedures and responsibilities shall be established for reporting of software malfunctions and recovering from virus attacks.

*12.4 **Safeguarding** of **information, data** and data **media,***

The MISS classification and criteria system shall be used by the System Owner to define an appropriate set of protection levels to ensure that information assets receive an appropriate level of protection. Where data is in a physical format (printed output, manuals, magnetic tapes/discs etc.) the security classification of the data shall be indicated and it shall be controlled, handled, distributed, stored and disposed of in accordance with the allocated security classification.

12.5 Utilisation of unofficial microcomputers on DoA premises

12.5.1 Written approval shall be obtained from the GITO to use an unofficial microcomputer on an DoA premises.

12.5.2 A register for unofficial microcomputers shall be established by the System Manager containing full personal particulars of the person as well as details of the private microcomputer, for example make, serial number, tapes and software used.

12.5.3 The official anti-virus package shall be loaded on every unofficial microcomputer used for official purposes.

12.5.4 No official or classified data shall be permanently stored on unofficial storage media.

12.5.5 All policies, guidelines and standard operating procedures shall apply to unofficial microcomputers during use on DoA premises.

12.5.6 Before an unofficial microcomputer can remove from a DoA premises, the User Manager shall ensure that no classified information is stored on the hard disc.

12.5.7 Any unauthorised unofficial microcomputers on DoA premises shall be confiscated during monitoring actions.

13. Information system communication security

13.1 Aim

To describe the minimum security measures that- shall be implemented to ensure the confidentiality, integrity, accountability and authentication of data during and after transmission and to prevent the loss, modification or misuse of information exchanged between DoA offices.

13.2 Security of data transmissions

13.2.1 Flow control mechanisms

13.2.2.1 Communication networks shall be equipped with security mechanisms (when required) to ensure the secure flow of information between networks, to limit the unauthorised use of resources accessible through the network and to prevent unauthorised external access.

13.2.2.2 Information flow control mechanisms (such as gateways, routers and firewalls) shall be recommended by SITA and approved by the DITC before installation on a communication network.

13.2.2 Error control

13.2.2.1 Error control in respect of transmission of flow controlled data shall be applied. Applicable error detection measures shall be implemented to trace errors during transmission of data, for example by checking serially controlled totals and/or doing parity checks and testing.

13.2.2.2 Communication hardware shall be checked regularly to ensure proper operation.

13.2.2.3 The prescribed signing-off procedures shall be followed strictly to prevent an intruder from taking over access by canceling the authorised users signing-off message.

13,2.3 Transmissions controls

13.2.3.1 Communication software shall make provision for messages in both directions between the computer system and the terminal, to confirm that the data transmitted has been received.

13.2.3.2 Passwords and dial-back systems shall verify the identity of the communication peer and the origin of the received data.

13.3 Modems/dial-up computer communications

13.3.1 No modems shall be connected to DoA communication networks without authorisation of the DITC. Authorisation shall only be given on receipt of a detailed motivation and only through a single point of entry where access can be controlled and managed.

13.3.2 Only authorised dial-back modems as approved by the DITC which comply with the prescribed security standards shall be installed for inter- and intra-departmental communication by means of a remote access server, to establish the link.

13.4 Voice transmission systems and fax transmissions

13.4.1 Telephone and voice transmission system security

Confidential messages shall not be left on answering machines or voicemail systems. Storage of voice messaging shall comply with the security prescripts in the MISS and any other relevant DoA policies. Physical access to the control room of the PABX telephone system shall be strictly controlled.

13.4.2 Secure fax transmissions

Confidential and higher classified information shall not be sent to unattended fax machines unless the destination machine is in a locked room for which the keys are possessed only by functionaries authorised to receive the information. Confidential and higher classified information shall not be faxed to an electronic fax mailbox. Store and Forward fax systems shall not be used for the transmission of classified documents.

13.5 Internet connections

13.5.1 Execution shall be given to the prescripts of the official DoA Internet Policy.

13.5.2 Access to the Internet shall only be allowed via a secure firewall. Access control during official hours shall be exercised by means of user identification and authentication.

13.5.3 The Internet shall not be used for classified information, communication internal to DoA or as a substitute for the existing communication infrastructure.

13.5.4 Applications for all official Internet connections shall be submitted via the normal communication channels to the DITC for approval.

13.5.5 Only licenced and authorised World Wide Web (www) browsers, shall be used to access the Internet via approved servers. An audit trail of all Internet activities shall be maintained.

13.5.6 The use of the Internet E-mail facilities is not allowed unless approved by the DITC.

13.5.7 The downloading, storage and distribution of unofficial data and software (including free ware for private purposes, Active X or Java/Java script content) by DoA system users are strictly prohibited. Private software downloads shall only be done with the authorisation of the GITO.

13.5.8 An approved anti-virus package shall be installed on every Internet computer.
13.5.9 The use of the Internet shall be in direct support of the DoA's business and personnel shall only use it in line with the DoA Internet Policy. Access shall be revoked immediately when improper use is identified and transgressions shall be dealt with in accordance with the DoA code of conduct.

13.6 ***Intranet*** *connections*
13.6.1 The Intranet shall not be linked to the Internet. It shall not be used as dissemination means for chain letters and/or as an unauthorised distribution platform for illegal software, games, shareware and/or freeware. The Intranet shall only be used for authorised purposes.

13.7 Website security
13,7-1 Directorate Communication shall manage and control the DoA website.
13.7.2 Only information approved by Directorate Communication shall be published on the DoA website.
13.7.3 The availability and integrity of DoA information on the website shall be maintained. To prevent unauthorised alterations or misuse, the following security requirements shall be adhered to:
13.7.3.1 the web server(s) shall be monitored for any suspicious activity.
13.7.3.2 an audit trail/log shall be kept of all security related incidents.
13.7.3.3 he web server(s) shall be taken off-line if an imminent threat to the integrity and/or confidentiality of the website occurs.
13.7.3.4 only web authors, page developers and the web master shall be allowed to administer the web server(s).
13.7.3.5 access to areas that are not for public view (Intranet) shall be restricted to registered DoA system users. The public DoA Website shall be separated from internal DoA databases via a firewall.
13.7.3.6 Home pages of DoA offices shall only be hosted as sub-pages on the official DoA Internet Website.
13.7.3.7 no link between the DoA Website and any other external organisation shall be established unless approved by the DITC.
13.7.3.8 incoming data shall be limited to website visitors feedback.
13.7.3.9 Website data shall be stored on a separate server.

13.8 Electronic mail (E-mail)
13.8.1 Execution shall be given to the prescripts of the official DoA E-mail Policy.
13.8.2 Logical access to the DoA internal E-mail system shall be restricted to registered DoA network users.
13.8.3 No E-mail connection that bypass the firewall in any manner shall be established to send and/or receive E-mail via the Internet or any other network. Uncertainties in this regard shall be cleared with the GITO.
13.8.4 The DoA E-mail system shall not be used for unlawful activities, personal purposes, messages that might be offensive or discriminating and/or other uses that violate this or any other DoA policies.
13.8.5 DoA E-mail users shall not employ a false identity when using the E-mail system or use someone else computer to send E-mails.

13.8.6 E-mail services shall not be used for purposes that could reasonably be expected to cause excessive strain on any computing facility or unwarranted interference with other users use of E-mail services.

13.8.7 All E-mail software that is installed and/or upgraded shall be authorised by the DITC.

13.8.8 Access to the DoA E-mail system shall be revoked after misuse of the system/termination of employment. Transgressions shall be dealt with in accordance with the DoA code of conduct.

13.9 Network security ***requirements***

13.9.1 Network controls

13.9.1.1 Network Administrators shall implement controls (as agreed upon with the parties concerned) to ensure the safeguarding and security of information in networks, the protection of the supporting infrastructure and the protection of connected services from unauthorised access.

13.9.1.2 Operational responsibility for networks shall be separated from computer operations where appropriate.

13.9.1.3 The segregation of large networks into separate logical network domains shall be based on the access control policy and access requirements incorporating suitable network routing and/or gateway technology. Routing controls shall be based on positive source and destination address checking mechanisms.

13.9.2 Local area network (LAN) administration

13.9.2.1 The LAN Administrator shall be responsible for configuration management of the LAN. Responsibilities and procedures for the management of the LAN shall be documented.

13.9.2.2 The DoA systems disaster recovery plan shall also provide for the recovery of critical DoA LAN functionality.

13.9.2.3 The utilisation of administrator privileges shall be strictly limited and controlled by the LAN Administrator. Default accounts (for example Guest, Supervisor, Administrator) shall be disabled.

13.9.2.4 ' The connection of unauthorised equipment to the LAN system is prohibited. New workstations being added to the LAN shall be documented, controlled and administered. Any changes in the network shall be approved by the LAN Administrator.

13.9.2.5 The application of LAN monitoring equipment and/or sniffing tools shall be limited strictly to officials authorised by the GITO.

13.9.3 LAN access control

13,9.3.1 Contractors needing access to the DoA LAN shall meet all the security requirements before access is granted. Contractor's access to the DoA LAN shall be managed by the LAN Administrator.

13.9.3.2 Physical access to controlled equipment on the LAN and the central network control office (LAN room) where the file server(s) is located shall be strictly limited and controlled.

13.9.3.3 A centralised and uniform computer access control system shall ensure that every LAN user is identified positively against his/her user profile and authenticated before he/she can link up with a file server. Access control software shall force the user to change his/her password at least every 3 months.

13.9.3.4 Any changes to users responsibilities with conjugated changes to information to which access can be gained shall be controlled and managed.

13.9.3.5 Access to critical information as well as diagnostic ports shall be strictly controlled and limited on a need-to-know basis. Diagnostic ports shall be protected by an appropriate security mechanism to prevent unauthorised access.

13.9.3.6 If, for a predetermined period of time, there has been no keyboard activity on a microcomputer connected to the LAN, the session/connection to the server shall be terminated automatically. A password shall once again be given before activities can be resumed. End terminal connections not in use shall be deactivated.

13.9.3.7 The use of a single password by multiple users to gain access to resources is not allowed.

13.9.3.8 Access by remote users or systems (where approved) via public networks shall be authenticated by a firewall/secure server to provide assurance of the source of the connections or alternatively via approved dial-back modems.

13.9.4 LAN security management

13.9.4.1 DoA LAN users/contractors shall ensure that all security guidelines are complied with. Virus contamination shall be restricted and controlled by means of an official anti-virus package. The manifestation of viruses shall be reported to the LAN Administrator and, in the instance of virus control being outsourced, to that party concerned.

13.9.4.2 Operating software shall be stored safely and access to system files shall be restricted. Operational tasks shall be divided in such a way that no user is responsible for a total process.

13.9.4.3 The security measures on LAN applications shall be monitored continuously. Where security deficiencies are identified, corrective measures shall be implemented. If any form of sabotage or actions endangering security are suspected, the matter shall be reported to the LAN Administrator for further investigation.

14. Personnel security

14.1 Aim

To describe the minimum security measures that shall be implemented to prevent DoA personnel and contractors from committing sabotage, subversion or other actions endangering security, or from being subjected thereto within the information system environment.

14.2 Manpowerplanning

14.2.1 Security clearances

All DoA system users/contractors/consultants with access to critical information are subjected to a security vetting process.

14.2.2 Security post grading

A security grading shall be allocated to all computer-related posts. The security clearance of an incumbent shall at least correspond with the security grading of the post. Authorities at all levels are responsible for ensuring that the security grading of the information being worked with and to which access is gained, does not exceed the security clearance of the DoA information system user/ contractor or exceed the grading of his/her post,

143 Recruitment and security screening

Contractors located on an DoA site for a period of time are equally subjected to the requirements of this policy. Before an information system user/contractor is appointed, the applicant shall meet the minimum security requirements for the post (as indicated in the tender specifications). Access to DoA networks shall automatically be terminated on expiry of a member's/contractor's security clearance and/or if the purpose for access to a network has ceased to exist.

14.4 Application/utilisation

14.4.1 Job description

All DoA information system users/contractors shall have approved job descriptions. IS security roles and responsibilities shall be included in job descriptions where appropriate.

14.4.2 Application

Contractors located at an DoA site are subjected to the same clearing-in and -out procedures like any other DoA member and shall also complete the System Registration Form (see Annexure B). All information system users/contractors shall sign an undertaking of compliance with the security policy and standards (see Annexure C).

14.4.3 Information system security training

Training to effectively and efficiently apply information system security shall be provided. Security consciousness shall continually be promoted among personnel and strengthened through formal training programs, counseling and practice.

14.4.4 Key personnel.

DoA IT key personnel shall be identified and backup IT personnel trained.

14.4.5 Task design

In environments where system users work with critical data, procedures shall be such that an incumbent is not responsible for a complete process (in order to prevent breaches of security, financial manipulation, fraud etc.). Whenever it is difficult to segregate the management or execution of certain duties or areas of responsibility, other controls such as monitoring of activities, audit trails and management supervision shall be considered. There shall be procedures for every job and they shall complement security.

14.5 Resignations

In the case of termination of service, DoA key personnel in a high risk environment shall be dealt with in line with sound labour practices which should include transferal to a lower risk environment. Backup actions shall be in place in this regard and an audit trail shall be instituted on their actions. In the case of disciplinary investigations, DoA personnel shall be dealt with in accordance with the DoA code of conduct. The clearing-out administration for DoA system users/contractors shall provide for the immediate cancellation of access to system(s), removal from the system(s) and submission of all official documentation and equipment.

15. Physical security

75.7 *Aim*

To describe the minimum preventative, detection and corrective security measures which shall be implemented in an DoA computer facility for protection against unauthorised access to information and/or information systems.

15.2 Safeguarding of security areas and buildings

15.2.1 Access control

A security area where computer-related equipment, software and data are accommodated shall be protected in such a way that unauthorised access is prevented. An access control system and procedures shall be implemented with the necessary control measures to prevent unauthorised access to high security areas such as computer rooms where the file servers are located.

15.2.2 Design and location

The DoA shall endeavour to ensure that DoA buildings/installations containing computer-related equipment, personnel and data are designed and/or located in such a way that the effect of natural disasters, radiation and emission is minimised and that optimal safety/security is achieved.

15.3 Safeguarding of equipment and support services

15.3.1 Equipment

IS/IT equipment shall be sited and/or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access. Manufacturers instructions for protecting equipment shall be adhered to. Procedures regarding the safeguarding and protection of information system equipment shall be implemented.

15.3.2 Support services.

Measures shall be implemented to ensure that hardware, software, personnel and data are not impaired by the ineffective functioning of support equipment (e.g. air conditioning, UPS, cabling infrastructure, etc.) due to exposure to sabotage. Power and telecommunications cabling shall be protected from damage and/or interception. Power cables shall preferably be segregated from communication cables or shielded cabling shall be used to prevent interference and shall be underground, where possible, or subject to adequate alternative protection.

*15.4 **Fire** safeguarding*

Measures shall be implemented to prevent hardware, software, data and buildings from being damaged, overcome or destroyed by fire or smoke and to prevent personnel from being injured. Awareness in respect of fire prevention shall be reaffirmed continuously and evacuation drills shall take place regularly. Fire-fighting equipment shall be tested by the vendor at least twice a year to ensure that it is in working order.

75.5 ***Movement** control 15.5.1 **Personnel***

Movement of DoA personnel, contractors and visitors inside buildings, premises and security areas shall be restricted as such that the need-to-know principle is applied. Identified vulnerable points (data, personnel, equipment and buildings) shall be protected against sabotage and/or internal personnel's actions that could endanger security.

15.5.2 Visitors

Visitors inside a security area building where computer hardware is accommodated and data is processed/stored, shall at all times be accompanied by authorised personnel and carry visible identification.

*15.6 **Removal** control*

In order to prevent computer-related equipment and data (printouts, magnetic tapes/discs etc.) from being removed without authorisation, a removal control system (e.g. register) and procedures shall be established. (See Annexure C for an example of a removal control form.) Records shall be kept for audit purposes with regard to which IS/IT related equipment and data has been removed, by whom and for what reason. Before computers and IS/IT related equipment on which data is stored in a magnetic format can be removed from a security area, the data shall be deleted or otherwise properly protected.

*15.7 **Transport** control*

In order to prevent computer-related articles in transit from being damaged and/or exposed to sabotage, control measures and procedures shall be implemented and executed. Packaging shall be in accordance with the manufacturer's specifications and equipment shall be packed correctly to prevent unauthorised access, tampering, misuse and/or physical damage. Computers and equipment shall not be left unguarded outside a security area.

ANNEXURE A

Policy and standards comment and change proposal form

Detail of proposer: _____

Title:

_____

Name: _____

Address: _____

DoA Office: _____

Phone:

_____

Change request Policy reference: details: _____

Action **Modity/replace/delete/added** only (circle one): _____

Suggested change (Detail proposed change): _____

Reasons (Detail reasons to support proposed change): _____

Date: _____

Signature: _____

ANNEXURE B

System registration form

Whenever an official is employed by or resigns from the Department of Agriculture and is/was assigned to perform functions which allowed access to the DoA computer applications he/she must complete this form and a copy must be sent to the GITO.

Surname and Initials: _____

ID Number: _____

Persal Number: _____

Date of employment; or _____

Date of resignation: _____

District and division: _____

Workstation name and address: _____

User-code assigned to Official: _____

Screen names to which official must have access: _____

Screen names to be cancelled after resignation: _____

Official Signature: _____

Date: _____

Supervisor Signature: _____

Date: _____

Personnel Office Official Verification; _____

Signature: _____

Date: _____

ANNEXURE C

Oath of secrecy

I, (Full names and surname): _____

ID number _____ Job Title _____
hereby subscribe to the contents of this document without being unduly influenced or coerced to do so, and solemnly declare that:

1. I have taken note of the stipulations of the DoA IS/IT security policy and standards and the Protection of Information Act (Act no 84 of 1984) and in particular of the stipulations of article 4 thereof.

2. I understand that I will be guilty of an offence if any information that 1 dispose of on account of my office and work and in respect of which I know or reasonably should know, that the safety or other interests of the Department of Agriculture requires the secrecy thereof, be made known to somebody other than
   a. to whom I may rightfully disclose it; or
   b. to whom it is in the interest of the Department of Agriculture my duty to disclose it; or
   c. to whom I am empowered by the Head of department of the Department of Agriculture to disclose it or by an official empowered to give such sanction.

3. I understand that the above stipulations and prescripts are not only applicable during my tenure or contract period, but also after my services in the Department of Agriculture are terminated.

4. I am fully aware of the serious consequences that may follow any violation or transgression of the above stipulations and prescripts.

Undertaking regarding measures to ensure information system and information technology security at computer workstations

Personal responsibility

5. I hereby undertake
   a. to maintain my security competence and if any change should occur pertaining to my personal circumstances or work environment which may impact negatively on my current security grading, I shall immediately bring that to the attention of my supervisor;
   b. not to misuse any computer or computer terminal or information system of DoA and to perform only authorised functions on the DoA's computers, terminals or any other computerised systems of the State to which I have access to; and

c. to ensure that no unauthorised/illegal software is used on any computer of the DoA under. my authority and control and that no unauthorised copies are made of licenced DoA software for personal use/gain.

Hardware and software

6. I hereby undertake to ensure that

a. computer hardware and software under my control are at all times located and stored according to the MISS document and the DoA IS/IT Security Policy and Standards in order to limit emission as well as electronic eavesdropping and interception;

b. adequate measures are instituted to safeguard computer hardware and software under my control against theft, damage and unauthorised access;

c. any damage, unserviceability or wear and tear to computer hardware and software are immediately reported to the System Manager;

d. computer hardware and software under my control are only used for official purposes and to report any deviation in this regard immediately to the System Manager;and

e. I would not use my own personal computer to load or process DoA information without the written authorisation of the GITO.

Networks

7. I hereby undertake to ensure that

a. no functions will be performed which exceed the security grading of the network carrier; and

b. the network to which I have access to and which is under my control is properly safeguarded and that no computer hardware and software or transmission line security is compromised in any way, and that I shall on the suspicion of any action which possible poses a security risk, make an immediate report to the Network Administrator.

Information/Data

8. I hereby undertake to ensure that

a. all information/data under my control is safeguarded in accordance with security guidelines as set out in the MISS document and the DoA IS/IT Security Policy and Standards;

b. all computerised information/data is classified strictly according to the MISS document and the DoA IS/IT Security Policy and Standards and safeguarded according to its classification;

c. there is compliance with the necessary measures to protect computerised data under my control against unauthorised access, interception and monitoring or any other security compromise (e.g. through computer viruses and manipulation); and

d. all passwords under my control are chosen and protected according to the prescripts of the MISS document and the DoA IS/IT Security Policy and Standards.

Documentation

9. I hereby undertake to ensure that
   a. all classified computerised inputs, of whatever nature, are handled in accordance with the prescripts as set out in the MISS document as well as the DoA IS/IT Security Policy and Standards; and
   b. all source documents, master copies, documentation and information under my control are handled according to the prescripts of the abovementioned documents.

Backup

10. I hereby undertake to ensure that
   a. regular backups are made of all computerised data under my control to prevent a situation where computerised data cannot be returned to its original conditions due to an unforeseen situation; and
   b. all backups of computerised data under my control are properly safeguarded at all times and are readily accessible.

11. If it might become necessary to alter this undertaking, it shall be done in writing.

12. I hereby declare that I understand the contents of this agreement and that I would follow the statutory provisions and guidelines scrupulously.
13. I declare that I have read the undertaking before I signed it.

SIGNATURE: _____

DATE: _____

TIME: _____

PLACE: _____

WITNESSES: _____

ANNEXURE D

I Authorisation for the removal of computers and IS/IT equipment

I, _____ Title _____ hereby request permission to remove computer(s)/hardware/software* from the under mentioned office.

I accept full responsibility for the safeguarding of the equipment against theft and any unusual damage while in my possession.

_____

Reason(s) for the request (Use separate page if necessary)

_____

Description of the equipment to be removed (includina serial number(s) (Use separate page if necessary)

_____

Highest security classification of the data on the equipment to be removed Period for requested permission

From: _____

To: _____

SYSTEM MANAGER: _____

_____

APPROVED/NOT APPROVED*