INFORMATION AND COMMUNICATION TECHNOLOGY SECURITY GUIDELINE

Version 1

18 May 2017

Document Version Control

Date	Author	Version
18 May 2017	DPSA	Version 1

Approvals

This Information and Communication Security Guideline are approved by the Head of Department of Public Service and Administration.

Name	Signature	Date

TABLE OF CONTENTS

1. BACKGROUND

Information is the backbone to the achievement of business objectives and government service delivery. Sometimes organisations fail to appreciate the value of information security to proactively protect information against threats and vulnerabilities and the preservation of confidentiality, integrity and availability of information. Hence, there is inadequate institutional information security policies, systems and other means and mechanisms to safeguard their information.

These weaknesses in the information security environment are supported by the repetitive findings of the Auditor General of South Africa (AGSA) on Information and Communication Technology (ICT) security. In their 2013-2014 Report, AGSA identified the lack of or poor implementation or non-compliance to internal ICT security policies to direct the institutions and protect their information and systems as most prominent security risk and weakness. Internal controls were also found to be deficient or not implemented by management.

In an effort geared towards creating and supporting an enabling ICT security environment to address the security risks and weaknesses, the Department of Public Service and Administration (DPSA), in collaboration with key ICT security stakeholders in government, such as the GITO Council (GITOC) and Standing Committee on Information Systems (SCISS) developed this overarching generic ICT Security Guideline (hereafter referred to as the Guideline).

For the purpose of this guideline reference to an ‘‘institution’’ means a national department, a provincial department, and a government component as per Public Service Act No.103 of 1994.

2. INTRODUCTION

A secure ICT environment ensures the confidentiality, integrity and availability of information within the underlying ICT systems and business processes. Achieving ICT security requires an effective management of risk, which encompasses risks from physical, human and technology related threats associated with all forms of use and or processing of information within the institution.

The design and implementation of an institution’s ICT security management system is influenced by the needs and objectives of the institution, its security requirements, the business processes employed, the size and structure of the institution and the effective achievement of legal and regulatory compliance.

Therefore, ICT security management should ascertain that the institution identifies, analyses and addresses its information security risks and protection requirements. Based on this potential risk, the ICT security arrangements should limit security breaches, threats, vulnerabilities and business impacts and if it does occur, to have in place the necessary mitigation arrangements.

To protect the information and mitigate ICT security risks it is necessary for the institution to put in place the necessary ICT Security policy, which will guide the development and implementation of individual policies such as access control.

This Guideline takes cognisance of the International (ISO) Standards on Information Security and other South African prescripts such as the Electronic Communications and Transactions-, Promotion of Access to Information- and Protection of Personal Information Acts, as mentioned in paragraph 6.

3. OBJECTIVE

ICT Security management falls within the ambit of the overarching information security management system of an institution, which includes physical, human and technology security. Due to the interrelationship between the different disciples, ICT Security cannot be approached from an electronic information perspective only. It is therefore necessary to understand the information security landscape of an institution within which ICT security functions.

The objective of this overarching ICT Security Guideline is to make the management of the Institution aware of the different areas that impact on ICT (electronic information) security and what means and mechanisms are required to successfully secure their information.

The means and mechanisms include, but are not limited to, governance, functions, organisation, processes, policies, guidelines, allocation of roles and responsibilities, reporting and monitoring.

Following this overarching Guideline, supporting guidelines intended to provide guidance on specific information security focus areas, such as Access Management, ICT Service Continuity etc. will follow.

4. PURPOSE

This ICT Security guideline is an effort geared towards creating an enabling ICT security environment and to address the security risks and weaknesses.

The purpose of this Guideline is to provide generic guidance to institutions in terms of ICT security management, within the context of the larger information security landscape.

This Guideline is also in support of the requirements as per the DPSA Corporate Governance of ICT Policy Framework.

There is no “one size fits all”, thus this Guideline should be interpreted, taking into account the institution’s context, when developing their individual ICT Security policies and guidelines.

It is not the intent of this Guideline that new positions be created. The existing organisational structure should be utilised to absorb the information security functions.

5. APPOSITENESS

Reference to “institution” in this Guideline means a national department, a provincial department, a municipality or a national or provincial government component as per Public Service Act No.103 of 1994.

The current applicability of this Guideline is national and provincial government as per Public Service Act No.103 of 1994.

6. LEGISLATION AND REGULATIONS

a) Constitution of the Republic of South Africa No. 108 of 1996 as amended

b) Disaster Management Act No. 57 of 2002

c) Electronic Communications and Transactions (ECT) Act No. 36 of 2005

d) General Intelligence Laws Amendment Act No. 11 of 2013

e) Minimum Information Security Standards (MISS) of 1996

f) National Archives Act No. 43 of 1996

g) National Treasury Risk Management Framework

h) Promotion of Access to Information (PAIA) Act No. 2 of 2000

i) Protection of Personal Information (POPI) Act No. 4 of 2013

j) Public Administration Management Act No. 11 of 2014

k) Public Finance Management Act No. 29 of 1999 , as amended

l) Public Service Act No. 103 of 1994 as amended

m) Public Service Regulations of 2001 as amended

n) Regulation Of Interception of Communications and Provisions Of Communication Related Information Act of 2002

o) State Information Technology Agency Amendment Act No. 38 of 2002

p) State Information Technology Agency Act, 1998: General Regulations

q) SMS Handbook

r) Prescripts that are specific to the institution

7. KEY ROLE PLAYERS

The key role players in the public service IT risk space are:

a) The **Department of Public Service and Administration** (DPSA), which has a mandate to ensure the effective use of IT in Public Service, facilitate the use of information technology for modernising Public Service and establishing e-government practices within an acceptable information security environment;

b) The **Auditor General of South Africa** (AG) audits Public Service IT risks related to Public Financial Management Act (PFMA) requirements;

c) The **State Security Agency** (SSA) is the leading authority on state security matters, including Public Service IT risks; The SSA is also responsible for the Government Electronic Communications Security Computer Security Incident Response Team (ECS-CSIRT) system where critical security incidents of national security are reported on;

d) The **State IT Agency** (SITA), a Public Service centre of excellence, is mandated to render IT services that meet appropriate security requirements and also to provide a help desk service. The type of incidents reported on SITA helpdesk system (call log system) are hosting services, managed applications, managed desktop and network services; and

e) The **Department of Telecommunications and Postal Services** (DTPS) formulates, coordinates, and provides policy direction on ICT related matters and will be responsible for the activities of the Cyber Security Hub and its derived objectives from the National Cyber Security Policy Framework. DTPS is the primary point of contact for the private sector and industries outside of government in relation to general ICT policy.

8. OVERVIEW

The Heads of Department and leadership of government institutions should take the responsibility to implement and maintain internal controls that address the risks that could prevent the institution from achieving their objectives.

In this regard top management should demonstrate leadership and commitment to physical, human and technology security. ICT Security management should be addressed within the ambit of the larger institutional security of information environment; adherence to relevant security prescripts in government; mandate the relevant institutional policies; ensure that the necessary ICT security controls and processes are in place; that adequate structures and resources are available; relevant security roles, responsibilities and authorities are assigned to individuals; awareness created and regular monitoring, evaluation and improvement of the ICT security management of the institution.

From a best practice perspective, a formal, structured approach to policy development, implementation, management and monitoring is required to achieve the business objectives.

ICT should also be a key component of government institutions and business strategies and core business processing activities. As technology increased the amount of data and information being processed it has significantly impacted the control environment. The management of ICT risk should therefore be elevated within institutions.

A monitoring process to measure compliance and the extent to which processes meet management expectations should be put into place. This will allow management to assess whether the financial and operational results give a true and fair view of the institution’s operations.

ICT audits should be conducted to collect and evaluate evidence to determine whether a computer system has been designed to maintain data integrity, assets are safeguarded, institutional goals are achieved effectively and resources used efficiently.

9. PROPOSED INFORMATION SECURITY GOVERNANCE MODEL

A prerequisite to effectively ensure the security of an institution's electronic information is governance, through a system by which the institution's information security activities are directed and controlled by a governing body, which could be a person or group of people, who are accountable for the performance and conformance of the institution.

The achievement of effective and efficient ICT security management requires a unique and integrated governance model. Without the right people and clearly defined roles and responsibilities, the ICT processes and technology implemented to enable better service delivery will be insufficient to address the existing, as well as future risks with regards to ICT security.

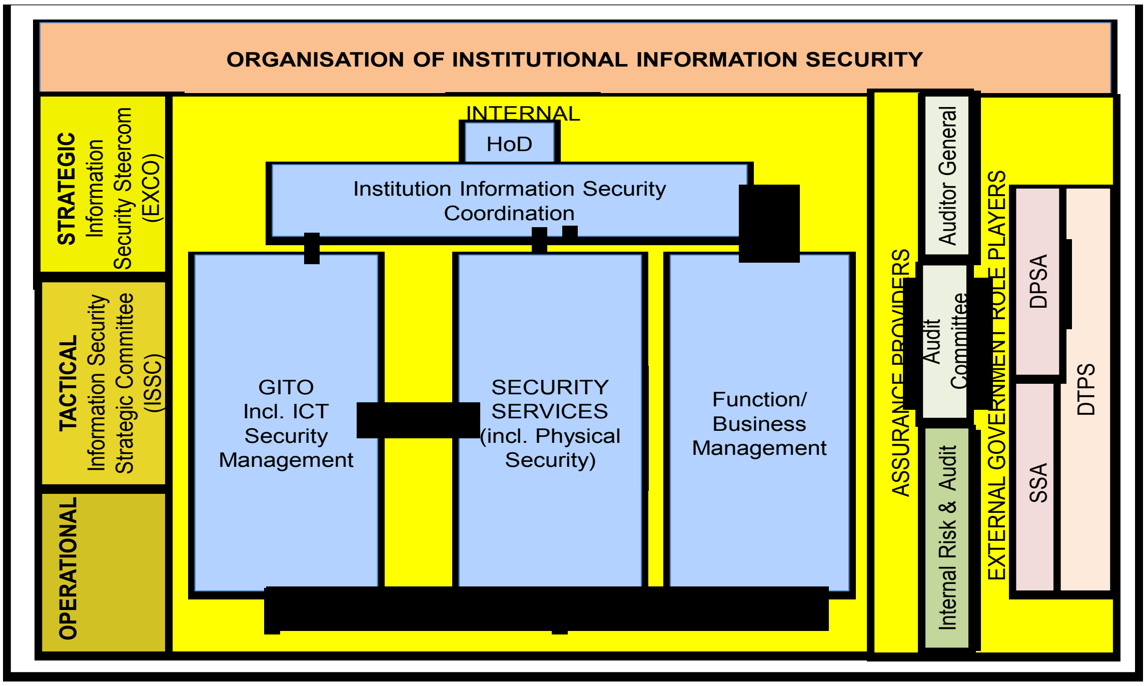
A governance model for ICT security management is shown in Figure 1 below. The scope of this model is limited to the National and Provincial spheres of government, however, the Institutional Organisation of Information Security (IOIS) can also be applied in the local sphere.

The IOIS includes members from strategic, tactical and operational levels in order to assist in ensuring that ICT Security is entrenched throughout the institution and receives the required attention to reduce and minimise information and information system security risks.

Each role depicted in the diagram can be fulfilled by a single individual, or in smaller institutions, one individual can fulfill multiple roles if necessary. What remains critical to the successful and effective implementation and functioning of the IOIS is clearly defining roles and responsibilities that are integrated with the role players' employment contract and/or performance scorecard. In addition, clear segregation of duties between policy making, implementation and compliance monitoring within the governance model is vital.

The roles and responsibilities are explained in section 10.

Figure 1: Information Security Governance Model


ORGANISATION OF INSTITUTIONAL INFORMATION SECURITY
STRATEGIC
Information Security Steercom (EXCO)
TACTICAL
Information Security Strategic Committee (ISSC)
OPERATIONAL
INTERNAL
HoD
Institution Information Security Coordination
GITO Incl. ICT Security Management
SECURITY SERVICES (incl. Physical Security)
Function/ Business Management
ASSURANCE PROVIDERS
Auditor General
Audit Committee
Internal Risk & Audit
EXTERNAL GOVERNMENT ROLE PLAYERS
DPSA
SSA
DTPS

10. INSTITUTIONAL ORGANISATION

The institutional arrangements of the management of ICT Security requires a multi-disciplinary approach which could include:

a) Governance and organisational structure, roles and accountabilities;

b) Policies, objectives, and the strategies that are in place to achieve them;

c) Information systems, information flows and decision-making processes (both formal and informal);

d) Standards, guidelines and models adopted by the institution; and

e) Form and extent of contractual relationships.

This section describes the management structure and related functions.

Note: Where possible the proposed information security structures, roles and responsibilities should be absorbed within the existing structures, roles and responsibilities of the Institution.

10.1 Roles and responsibilities

10.1.1 Head of Institution

The Head of the Institution should:

a) Provide strategic leadership and management;

b) Demonstrate commitment to information security management and assign information security roles and responsibilities;

c) Be accountable for the provisioning and maintenance of information within the institution in accordance to the relevant prescripts;

d) Ensure that appropriate capability and capacity are provided;

e) Determine the delegation of authority, accountability and personal responsibility to the Executive Management with regards to the management of physical, human, information and technology security;

f) Ensure that related policies for the institutionalisation of information security management are developed and approved, and implemented by Executive Management;

g) Ensure that information security risks are regularly assessed and managed;

h) Monitor the overall statuses of information ICT initiatives; and

i) Ensure the monitoring and evaluation of the effectiveness of Information Security Management System.

10.1.1.1 Institutional Information Security Coordinating Function

As information security spans different disciplines such as business units (information owners), security services (including physical security) and ICT (electronic information and infrastructure), it is desirable that this coordinating function resides in the Office of the Head of the Institution. The requirements to optimally manage information security risks can sometimes have an impact on ICT performance, which could create conflicts when critical decisions have to be made.

The Head of the Institution may delegate this function.

Note: **If the Institution has an existing Information Security Officer ("DISO"), it is recommended that this function should be executed by such a person/component**.

The Information Security Coordination function should achieve the following:

a) Ensure that information security is considered throughout the institution;

b) Oversee and co-ordinate physical and electronic information security;

c) Monitor the security of ICT systems and co-authorises, monitors and controls specific security improvement projects;

d) Establish, implement and maintain security policies, standards strategies, guidelines and processes;

e) Develop and implement security awareness initiatives;

f) Identify areas of non-compliance to security prescripts;

g) Design, implement, and provide information security compliance monitoring services to business units;

h) Direct and monitor the operational ICT risk management; and

i) Assess the impact of ICT risk on the institution and the efficiency of mitigation measures.

10.1.2 GITO

a) Ensure the confidentiality, integrity and availability of ICT systems within the ICT environment;

b) Manage information security within the institution’s ICT infrastructure landscape;

c) Maintain security of data on the institution’s network;

d) Within the ambit of the ICT function, manage information security within information systems (IS);

e) Server and Network administration;

f) Maintain agreed upon application security:

g) Maintain security of data of IS systems and lifecycle management;

h) Ensure that ICT security arrangements limits security breaches, threats, vulnerabilities and business impacts and if it does occur, to have in place the necessary mitigation arrangements; and

i) Closely collaborate with the head of security services, business management and internal system owners on risks that might impact on electronic information security.

10.1.3 Functional/Business Unit Senior Management

Within the ambit of their functional jurisdiction the Business Owner of information is also responsible for the management of the information life cycle and the protection of electronic information, such as the: classification of information; who should have access to this information; how it should be stored, maintained and disposed of.

Senior management should understand the impact of significant changes within their respective business/functional areas (for example, creation of new projects, changes in structures, etc.) in order to determine the impact of such changes within the larger realms of information security.

The above are specifically in relation to information security and are thus not a totality of the work of a GITO.

10.1.3.1 Functional / Business Representatives

a) Collate and provide statistical information relating to the adherence of information security requirements;

b) Upon request, attend the Information Security Strategic Committee (ISSC) meetings; and

c) Ensure that information security requirements are rolled out within the relevant business units.

10.2 Structures

10.2.1 Information Security Steering Committee

Due to its strategic nature, this committee, it should be composed of the executive management of the institution. The committee should:

a) Oversee the information security function and its activities;

b) Ensure clear direction and visible management support for security initiatives; and

c) Recommend security policies to the Head of Institution.

This committee does not have to be a separate committee other than the Executive Management Committee of an institution (EXCO).

Due to the strategic direction and impact of this committee, it should be chaired by the Head of the Institution.

10.2.2 Information Security Strategic Committee (ISSC)

A centralised Information Security Coordinating Committee should be established to ensure a clear direction for security initiatives and provide visible management support.

This committee should consist of a group of individuals in the institution who are responsible for information security (both electronic and manual). This committee should assist those charged with the governance of information security as well as those using information systems and technology in carrying out their responsibilities to protect the integrity, availability and confidentiality of public service information assets. The management of Internal Risk should also be a member of this committee.

The chairperson of this committee should be the person to which the institutional information security coordinating function is delegated to.

The objectives of this committee should be, but are not limited to:

a) Formal involvement of functional units in information security initiatives;

b) Provide guidance and direction;

c) Obtain authorisation from the Information Security Steering Committee for information security activities;

d) Reporting; and

e) Monitoring.

10.2.3 Assurance Providers (AGSA, Internal Audit and other)

The role of Assurance Providers, such as internal and external audit, is to:

a) Assess the risk related to the institutional strategy in the context of its mandate. This is to derive the appropriate information system and technology strategy, and operational and control environment's requirements;

b) To assess, either via the use of good practice or the use of the institution's own governance and management frameworks, whether sufficient means, mechanisms and controls exist to amicably address these risks within the risk appetite of the institution;

c) To raise findings (where applicable) in order to support the institution in improving its governance, management and operational practices; and

d) Information security should be included on the activities of the internal Risk and Audit Committees, which should assist the Head of the Institution in carrying out his/her accountabilities and responsibilities in this regard.

11. INFORMATION SECURITY FOCUS AREAS

This Guideline has the objective to provide guidance to strategic management on the overarching information security landscape in order to assist institutions to develop their specific ICT security policies, frameworks and guidelines to secure electronic information.

Due to the interrelationship between the different disciples, ICT security cannot be approached from an electronic information perspective only, but to have a holistic view of the information security ambit within which ICT security functions.

The focus areas that are addressed in these Guidelines are on a more strategic level and are not exhaustive. The focus areas relevant to the specific institution should be further unpacked in more detailed policies and guidelines, e.g. Access Management, ICT Service Continuity, Network Security, etc.

11.1 ICT Risk Management

The protection of the institution’s information is risk based. Achieving secure information requires the management of risk and encompasses risks from physical, human and technology related threats associated with all forms of information within or used by the institution.

To manage risk the institution should have an ICT risk management methodology and process in place for the application of management policies, procedures, practices, communication, consultation, establishing the context, identification of the risk owner(s) who is accountable and has the authority to manage the risk, develop risk criteria, identifying, analysing, evaluating, treating, monitoring and reviewing risk to determine whether the risk and/or its magnitude is acceptable or tolerable.

The institution should ensure that the ICT risks are managed within the institution’s risk management practice in accordance with the risk management prescripts, and that the ICT security function is audited as part of the institution’s audit plan.

Risk assessments of ICT security should identify, quantify, and prioritise risks against criteria for risk acceptance and objectives relevant to the institution. The results should determine the appropriate management action and priorities for managing information security risks and for implementing controls selected to protect against these risks.

To institutionalise appropriate ICT security risk management within the institution the following mechanisms and processes are recommended:

a) Put in place the necessary ICT security risk management system and allocate roles, responsibility and accountability;

b) Develop a comprehensive ICT security risk management methodology;

c) Establish an ICT security risk management program based on business goals and objectives;

d) Establish the risk assessment process;

e) Select proportionate ICT security controls as necessary to reduce the risk to an acceptable level;

f) Develop risk criteria against which the significance of risk is evaluated;

g) Perform comprehensive risk assessments to identify, analyse and evaluate the related risks;

h) Risks should be evaluated by comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable;

i) Risks should be continuously monitored and corrective action taken where necessary;

j) Institutions should develop and maintain ICT risk registers (strategic and operational ICT risk register); and

k) ICT risks should be included in the institution's risk register and be monitored like the rest of the institutional risks.

Risk avoidance is not risk management. The approach taken should be both transparent and justifiable.

Security risks should be regularly reviewed and re-evaluated, and risk management principles embedded as part of day-to-day business. Institutional approaches should be flexible and capable of adapting to fast moving or unpredictable events that require dynamic decision-making.

11.2 Asset Management

Information and information systems constitute valuable government resources. Asset management should define the acceptable use and protection of information, technology and infrastructure related assets.

To maintain protection will require the allocation of roles and responsibilities, develop and maintain related asset management processes and systems, the development and maintenance of asset inventories and to define the acceptable/non acceptable use of assets.

The designated owners of assets should be identified. These owners are responsible for protecting information and technology assets. They should identify the assets that need to be protected, to classify the different security levels of the different assets, adequate protection required at each level and define how the protection will be maintained.

11.2.1 Physical assets

Policies and procedures for the acceptable use, return and disposal of physical assets should be defined within the context of the broader asset management system of the institution.

11.2.2 Information assets

Assets used to create, process, store, transmit, delete and destroy information should be defined, their importance documented, and identify and allocate appropriate protection responsibilities.

Information and related infrastructure should be managed throughout the information life cycle.

Not all the information requires the same level of protection as only some information is sensitive or confidential. Information should be classified and labeled by its owners according to the security protection needed, and handled accordingly.

The identified information owner should be held accountable for the security of their information.

Asset inventory and classification should be done on a regular basis in order to monitor and ensure the acceptable use of assets.

11.3 Human Resource Security

Human resource security has the objective to ensure that all employees and external resources are suitably security vetted and contracted in accordance with the information and technology security requirement of the institution and that they understand and execute their security related responsibilities.

In order to limit security risks, cognisance should be taken of the relevant prescripts such as laws, regulations and policies, business requirements, classification of information to be accessed and perceived risks, including that of technology, throughout the entire employment/contracting cycle, from recruitment, appointment up to termination of employment/contract.

The contractual agreement of employment should clearly state their security related role and responsibilities. During employment management should oversee that all security related prescripts and requirements are adhered to.

In absence of a suitable security clearance e.g. whilst the official process is not yet concluded, the employer can expect from the employee/contractor to enter into a declaration of secrecy or non-disclosure agreement.

Management and personnel have different security responsibilities and liabilities that apply prior, during, and at the time of termination of employment. Prior to employment, emphasis is on the awareness of the expected roles and responsibilities, the screening of prospects and the existence of agreements. During employment, policies should establish management responsibilities, education, training and formal processes to handle problematic security situations. Rules should be established to ensure a secure transition when employment/contract is ended or changed.

11.4 Physical and Environmental Security

The objective of physical and environmental security is to prevent unauthorised physical access, damage and or interference to the institution's information and information processing facilities.

The requirements for the protection from environmental and man-made threats to personnel and property in information processing facilities should be identified.

Requirements for the installation, operation, protection and maintenance of computer equipment are identified to preserve the confidentiality, integrity and availability of government information and information systems.

Areas that contain sensitive or critical information and information processing facilities should be protected by appropriate entry controls to ensure only authorised access.

Physical protection against natural disasters, malicious attacks or incidents should be in place. Equipment should be used in a secure manner in order to prevent loss, damage, theft or compromise of assets and interruption to the institution's operations.

Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities. Equipment should be correctly maintained to ensure its continued availability and integrity. Security should be applied to assets used outside the premises of the institution.

Finally there should be appropriate procedures and process in place for the save disposal of assets that contains sensitive data.

11.5 Communications and Operations Management

Communications and operations management security is to protect the information in networks and to ensure correct and secure operations of supporting information processing facilities.

Planning and management of the day-to-day activities is required to ensure the availability and capacity of the resources that provide services. Services can be delivered by external parties, by computer networks and by all services that exchange information. The requirements to control and monitor operations for service delivery should be identified and changes managed as the operations evolve.

Changes to the institution, business processes, information processing facilities and systems that affect information security should be controlled. The integrity of operational systems should be protected and exploitation of technical vulnerabilities should be prevented.

Controls for operations include documented processes, staff duties and formal methods to implement changes to facilities. This includes: methods to protect information, create copies for back-up and to manage the media where those copies are stored. Network protection requirements from threats such as viruses or unauthorised disclosure should also be described.

The installation of software by users should be regulated.

Irrespective if network services are delivered in-house or outsourced, networks should, through service agreements, be managed and controlled to protect the electronic information.

The security of the internal and external exchange of information through all types of communication facilities should be maintained and the information be protected in accordance with the required security level of the information.

11.6 Access Management

Access restrictions protect institutions from security threats such as internal and external intrusions. The restrictions are guided by legislation that protects particular types of information (e.g. personal, sensitive or cabinet confidential) and by business requirements.

The objective of access management is to ensure that access to assets, information and technology is authorised and restricted, based on institution's business and security requirements.

Management should design and put in place user access controls to all applications and systems to prevent and detect unauthorised access to, and the creation or amendment of information stored in the application systems.

To put in place an encompassing access management requires ICT Access Management policies, system, process and procedures and the allocation of accountability, roles and responsibility.

Access Management policies should provide the blueprint for the management of user access, authorisations and control mechanisms for computer networks, information, applications and operating systems.

This policy should be approved by the Head of the Institution.

Areas to be addressed within the Access Management Policy, but not limited to, are:

a) *User access management*: user registration, privilege management, user password management and the review of user access rights;

b) *User responsibilities*: password use and employee, contract or account termination;

c) *Network, operating system and application system access control*: secure logon procedures, user identification and authentication, external connections, segregation in networks and routing control, network connection control, use of system utilities, operating systems access control, application and information access control, and auditing; and

d) *Mobile/remote computing*.

System owners and controllers should, where applicable, provide the GITO with a clear statement of the business requirements for system access, so that the GITO can oversee access to information systems and ICT services and data. Data owners and service providers will also be given the statements of business requirements.

Users access to functions and information should be restricted according to individual user roles and based on a "need to know and need to do basis" as specified by information system owners. The allocation of access should be continuously monitored and corrective action taken where necessary.

11.7 Information Systems Acquisitions, Development and Maintenance

Security measures should be incorporated into the life cycle of an information system. Security controls should be identified as part of the business requirements during the analysis and specification phase for new information systems or enhancements to existing information systems.

Rules for the development of software and secure systems should be established, documented maintained and applied to any information system implementation efforts.

When operating platforms are developed or changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on the institution's operations or security.

The institution should establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.

Changes to systems should be controlled through formal change control procedures from the design throughout to the maintenance phase.

The institution should ensure that the security of outsourced systems development be protected during the contracting, and be supervised and monitored.

Information security is integrated into the creation, modification, implementation and expansion by ongoing security practices such as the management of vulnerable points and securing system files.

For applications, information security can be applied to the validation of data input and output and by encoding information using electronic keys. Validation should be executed through the provision of objective evidence that the requirements for a specific intended use or application have been fulfilled.

Information involved in application services should be protected from fraudulent activity, contract dispute and unauthorised disclosure and modification.

Information involved in application service transactions should be protected to prevent incomplete transmissions, mis-routing, unauthorised message alteration, unauthorised disclosure and unauthorised message duplication or replay.

11.8 Information Security Incident Management

The institution should limit the probability of information security incidents, which is single or a series of unwanted or unexpected information security events or weaknesses that have a significant likelihood of compromising business operations and threatening information security.

Through information security incident management the institution should put in place the relevant information security incident management policies, allocate responsibilities, put in place processes and procedures to consistently and effectively detect, report, assess, respond to, deal with, and learn from information security incidents and weaknesses, and to collect forensic evidence.

Information security incident management policies identify the mechanisms required to detect and report when information security events occur provide the directives for the consistent management of such events. The information collected about the events can be analysed to identify trends and to direct efforts continually improve and strengthen the information security infrastructure of the institution.

The incident management procedures and processes assist personnel to understand their roles in reporting and mitigating security events.

The criteria to define an information security incident should be developed and reporting on these incidents should be incorporated into the Help Desk system of the institution. To limit the damage, a possible breach of information security should be reported as quickly as possible through the appropriate management channels.

11.9 ICT Service Continuity Management

Government institutions are required to be prepared and to re-establish business or services as swiftly and smoothly as possible.

Information service continuity should be embedded in the institution’s business continuity management systems. Business continuity plans should include the evaluation of security risks in line with the directions set by institution’s Business Continuity Plan.

ICT service continuity controls enable institutions to recover critical business operations and application systems affected by disasters or major system disruptions within reasonable time frames.

The institution should determine its requirements for information security and the continuous availability of information should an adverse event occur. The necessary processes, procedures and controls should be developed, implemented and maintained to ensure the required level of continuity for information and security during such an adverse event.

11.10 Third Party Access Management

Many government institutions grant remote access to numerous third parties such as vendors, service providers and other external parties without requiring any standardisation in terms of tools or solutions.

The third party are all external parties that may access, process, store, communicate, or provide ICT infrastructure components for the institution’s information.

Information security requirements for mitigating risks associated with the third party’s access to the institution’s assets should be agreed with the third party and documented.

External resources should be suitably vetted or Oath of Secrecy signed in accordance to the security requirements of the institution.

By forcing every vendor to use a single, consolidated, institutionally-owned solution to remotely access the network, institutions can greatly improve their ability to monitor and block unwanted activity. It is critical that institutions employ a remote access tool that captures a secure audit trail of every action a vendor executes on the system, and ties that record to the unique credentials of the individual user. In addition, institution should ensure that the audit trail is captured in a secure place within their network, not the vendors. This means that the latter can't delete or modify the record in the event they make a mistake.

11.11 Compliance

For institutions to create a secure environment they should avoid breaches of legal and regulatory or contractual obligations related to any information security requirement. According to legislation records should be protected from loss, destruction, falsification and unauthorised access. Privacy and personal information should also be protected.

Performance (measurable results) evaluation requires the institution to determine and implement suitable security metrics.

Other compliance obligations:

Monitoring for Policy Compliance: Systems should be regularly checked for compliance with security standards, as well as for security vulnerabilities publicised by vendors and computer emergency response alerts;

Monitoring of Individuals: Intensive, direct monitoring of an individual user (actions on the system, content of user files or electronic communications) may only be done by a person to which this responsibility was delegated or firm-appointed agents and in extreme cases where an institution has reason to believe that security threat exists;

Monitoring of software: Regular reviews should be conducted of software and data content of systems supporting critical business processes. The presence of any unapproved files or unauthorised amendments should be formally investigated; and

Network monitoring: Monitoring will be performed at appropriate levels to detect malicious actions and determine the availability of network resources. Special attention should be given to detecting rogue devices (i.e. personal laptops, pocket PC's, wireless access points, etc.) on the LAN (Local Area Network).

11.12 Intellectual Property Rights

Any software developed by government personnel through the use of government or non-government resources but within the scope of employment with government remains the 'intellectual property' of government and may therefore not be copied, sold, leased or removed without the express written consent of government.

All software on government hardware is protected by copyright laws. Commercial software purchased by an institution is authorised for government use only and shall be utilised in accordance with contractual agreements and copyright laws.

Unless specifically authorised within the license agreement, making copies of copyrighted software and related documentation for personal use is illegal and therefore prohibited. Unauthorised software will be removed and the responsible person might be subject to disciplinary action.

Software vendor's license agreements and copyright holder's notices shall be strictly adhered to. Whenever bundled systems are being procured, the source is required to provide written evidence of the software licenses.

The agreements for all computer programs licensed from third parties should be periodically reviewed for compliance and additional licensed copies procured as required.

11.13 Information Security Awareness and Training

To limit ICT security risks and create a secure environment for the institution, extensive awareness should be created for both information resources and users of the information through the following actions:

a) Develop packaged security awareness content and material per user level;

b) Develop a workforce development, training, and awareness program plan;

c) Develop a policy and program for information security awareness and training; and

d) Develop awareness and training materials that are appropriate and timely for intended audiences.

The Human Resources component of an institution, in collaboration with the persons responsible for information security within the institution, should be responsible for the facilitation and coordination of initial information security training during the induction of newly appointed employees and thereafter periodic awareness training and annual declarations of personnel understanding of Information Security policies and their security responsibilities.

11.14 Implementation, Monitoring and Evaluation

To establish, monitor, maintain and improve an information secure environment an institution needs to undertake the following steps:

a) Identify information assets and their associated information security requirements;

b) Assess information security risks and threats;

c) Select and implement relevant controls to manage unacceptable risk;

d) Monitor, measure, analyse and evaluate/audit/review the information security controls, processes and information security management system in order to make systematic improvements where appropriate to suitably protect the institution’s information assets; and

e) Continuously improve information security by addressing the findings of audits and reviews (e.g. nonconformities and corrective actions) and to make continual refinements to the information security management system to achieve established objectives.

To ensure the information security management system is effectively protecting the institution’s information assets on an ongoing basis, it is necessary for the aforementioned steps to be continually repeated to identify changes in risks or in the institution’s strategies or business objectives.

It is further recommended that institutions set target Key Performance Areas (KPA) and Key Performance Indicators (KPI) that will be used to measure policy adoption and execution. The result of this assessment will support the institutions in identifying information security priority areas requiring focus and the initiation of information security project/s to advance the maturity of information security.

12. IMPLEMENTATION

The Head of the Institution should determine the necessary functions to safeguard the information of the institution. Once the functions are identified, the roles and responsibilities should be delegated to the related functionaries and necessary consultative and reporting and monitoring structures, systems and processes be implemented.

GLOSSARY OF TERMS AND DEFINITIONS

ACCESS CONTROL

Mechanisms or controls and methods of limiting access to resources to authorised subjects only.

ASSET

Anything that has a value to the institution, whether physical or information.

AUTHENTICATION

To verify the identity of a subject requesting the use of a system and / or access to network resources.

The steps to giving a subject access to an object should be identification, authentication and authorisation.

https://www.out-law.com/page-410

AUTHORISATION

Granting access to an object after the subject has been properly identified and authenticated.

https://www.studyblue.com/notes/note/n/cissp-gl...

AVAILABILITY

Guaranteeing that data is protected from loss and ensuring that it is available to authorise users whenever and wherever required.

http://cdn.cnetcontent.com/31/b5/31b54a59-93ed-...

COMPROMISE

The unauthorised disclosure/exposure or loss of sensitive or classified information, or exposure of sensitive operations, people or places, whether by design or through negligence.

CONFIDENTIALITY

A security principle that works to ensure that information is not disclosed.

DATA

The term “data” refers to all information that can be electronically processed, transmitted and stored. Data may be processed in internal main memories, stored on tapes or disks, and transmitted by networks.

DELEGATE

A delegate is a person who is granted certain powers/authorities or functions in order to represent a higher authority in performing a specific task.

http://kalyan-city.blogspot.com/2010/07/delegat...

This is most often done by paper recycling containing non-confidential information but may also include other media.

http://www.creighton.edu/fileadmin/user/General...

DISPOSAL

Disposal is the act of discarding media with no other sanitation considerations. This is most often done by paper recycling containing non-confidential information but may also include other media.

ENCRYPTION

A mathematically derived process involving data coding to achieve confidentiality, anonymity, time-stamping, and other security objectives.

GUIDELINE

A suggested action or recommendation related to an area of information security policy that is intended to supplement a procedure. Unlike standards, implementation of guidelines may be at a discretion of the reader.

HEAD OF AN INSTITUTION

The person who is serving as the head of an institution, whether defined by law or otherwise, including the official acting in his place.

IDs AND PASSWORDS

IDs, also known as accounts, are character strings that uniquely identify computer users or processes. Passwords authenticate that user or process.

INCIDENT

An adverse event in an information system, and/or network, or the threat of the occurrence of such an event.

https://www.isaca.org

INFORMATION ASSETS

Information assets means computers, communications facilities, networks, data (information) and encryption keys that may be stored, processed, retrieved or transmitted by them. This includes programs, specifications and procedures for their operation, use and maintenance. All such assets are the property of the institution and should be protected according to the policies.

INFORMATION CUSTODIANS

Information users who have responsibility to properly protect institution or government information in keeping with the designated owner's access control, data sensitivity, and data criticality instructions.

INFORMATION OWNERS

Information users who have day-to-day responsibility for the preparation and dissemination of information assets, unless ownership is otherwise designated.

INFORMATION SECURITY

Information security is the provision of organisational, technical and social measures to safeguard information assets against unauthorised access, damage and interference—both malicious and accidental.

INFORMATION SECURITY INCIDENT

An information security incident is indicated by a single or series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

http://www.audit-is.com/terminology/information%20security%20incident-termDefinition.htm

INFORMATION SYSTEM

Systems designed to create, store, manipulate, or disseminate information.

INSTITUTION

Institution means any department of State, body or organisation that is subject to the Public Service Act or any other law or any private undertaking that handles information classifiable by virtue of national interest.

INTEGRITY

A security principle that makes sure that information and systems are not modified maliciously or accidentally.

INFORMATION SECURITY POLICY

The Information Security Policy Statement is sanctioned at the senior management level for application throughout the institution. The document defines principles and responsibilities that constitute information security within the institution and provides the foundation for the day-to-day execution. It deals with the technology part of any information system, and as such deals with hardware, servers, operating systems and software etc.

https://www.sans.org/security-resources/policies

NETWORK

Data communications system that interconnects computer systems and communication enabled devices

NETWORK SECURITY

This refers to security provided for information in transit including transfer protocols, applications, switches and routers.

PERSONAL DIGITAL ASSISTANT (PDA)

PDA's refers to a handheld device that combines computing, telephone, fax, Internet and networking features.

http://www.businessdictionary.com/definition/personal-digital-assistant-PDA.html

Remote access connections include connections to mobile employee laptops, employee dial-in connections from their residence, customer connections and vendor connections.

POLICY

Overall intention and direction as formally expressed by management.

PROCEDURE

A detailed description of the steps necessary to perform specific operations in conformance with applicable standards.

REMOTE ACCESS

Remote access denotes any usage of the institution network that comes from outside the institution’s controlled and protected environment via from outside the institution's controlled and protected environment via either dial-in or VPN. Remote access connections include connections to mobile employee laptops, employee dial-in connections from their residence, customer connections and vendor connections. Remote access also includes all dial-out modem connections established from any machine connected to the institution network. Common to virtually all remote accesses is a reduced or uncertain trust level at the remote end.

RISK

Combination of the probability of an event and its consequence.

SCREEN SAVER

A computer program that automatically blanks and/or locks the screen of a computer monitor or terminal after a certain period of inactivity.

STANDARDS

A metric used to determine the correctness of a thing or process; a set of rules or specifications that, when taken together, define a software or hardware device. A standard is also an acknowledged basis for comparing or measuring something.

THREAT

A potential cause of an unwanted incident, which may result in harm to a system or institution.

SECURITY

That condition free of risk or danger to lives, property and information created by the conscious provision and application of protective security measures.

THIRD PARTY

That person or body that is recognised as being independent of the parties involved, as concerns the issue in question.

USERS

All institution personnel, regardless of their position or job function, who use information assets. Selected customers and external vendors/consultants are also information users. Certain information users will also fall into the categories of information owners, information custodians, IT Product and service providers, and/or information security group.

VIRUS, WORMS AND TROJAN

Malicious software designed to reproduce itself and automatically spread to other computers or networks by attaching to or infecting other software. They can be transmitted via e-mail attachments, by downloading infected programs from the Internet sites, or can be present on a diskette or CD. They can be real or hoax; some can damage a computer as soon as their code is executed; others can lie dormant until circumstances cause their code to be executed by the computer.

VIRTUAL PRIVATE NETWORKS

A secure private network that uses the public telecommunications infrastructure to transmit data. Using encryption, a VPN encrypts all data that pass between two Internet points, maintaining privacy and security.

http://searchnetworking.techtarget.com/definition/virtual-private-network

VULNERABILITY

A weakness of an asset or group of assets that can be exploited by one or more threats to violate security.

WIRELESS NETWORK

A wireless network allows computer systems and communication enabled devices to connect without any physical connection between them.

13. REFERENCES

[1] OECD Guidelines for Security of Information Systems and Networks – Towards a Culture of Security, Paris: OECD, July 2002.

[2] International Organisation for Standardisation: ISO / IEC 27001, 2013. Information Technology – Information Security Management Systems.

[3] International Organisation for Standardisation: ISO / IEC 27002, 2013. Information Technology – Code of Practice for information security controls.

[4] SANS 17799: 2005 Information Technology – Security Techniques – Code of practise for information security management, June 2005 (www.sabs.co.za).

[5] South Africa. Department of Arts and Culture. National Archives and Record Service of South Africa Act No. 43 of 1996.

[6] South Africa. Department of Communication. Electronic Communications and Transactions Act No.25 of 2002.

[7] South Africa. Department of Public Service and Administration. 1994. Public Service Act 103 of 1994, as amended.

[8] South Africa. Department of Public Service and Administration. 2001. Public Service Regulations 2001, as amended. 31 July 2012.

[9] United Kingdom. Information Security Forum – The 2011 Standard of Good Practise for Information Security – June 2011.

[10] South Africa. State Information Technology Act No. 88 of 1998 as amended.

[11] South Africa. State Security Agency. Minimum Information Security Standards (MISS) of 1996.

[12] South Africa. State Security Agency. National Strategic Intelligence Act 39 of 1994 as amended.

[13] South Africa: Provincial Government Western Cape. Enterprise Information Security Policy. 1 November 2013.

[14] South Africa: Provincial Government KwaZulu Natal. ICT Security Policy. 15 November 2012.

[15] South Africa: Provincial Government North West. Information Security Policy.

[16] South Africa: Provincial Government Gauteng. Information Security Policy. July 2014.