



the dpsa

Department:
Public Service and Administration
REPUBLIC OF SOUTH AFRICA

DIRECTIVE ON PUBLIC SERVICE INFORMATION SECURITY

Preface

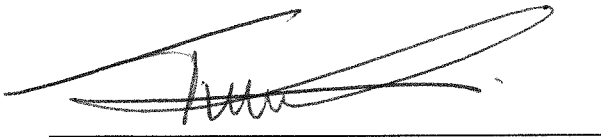
The current digital era has seen the increased importance of data and information, thus giving it the status of being the economy's raw material. It has brought the importance of protecting data and information to ensure its *confidentiality, integrity, and availability*.

The persistent cybersecurity incidents in the Public service reveal the level of vulnerability that the government departments are exposed to with limited ICT security skills to mitigate and combat the cyber-attacks as they emerge.

In line with this, section 3(1)(f) of the Public Service Act, 1994 (Proclamation No. 103 of 1994) provides for the Minister of Public Service and Administration (MINISTER) to establish norms and standards relating to information management in the public service.

Furthermore, regulation 94 of the Public Service Regulations, 2016, specifically provides for the MINISTER to issue information security standards for the public service after consultation with relevant Ministers.

This Directive is issued by the MINISTER in terms of section 41(3) of the Public Service Act to elucidate regulations 94, of the Public Service Regulations.



MR T.W. NXESI, MP

ACTING MINISTER FOR THE PUBLIC SERVICE AND ADMINISTRATION

DATE: 07/06/2022

Table of Contents

- 1. INTRODUCTION..... 4
- 2. PURPOSE..... 4
- 3. AUTHORIZATION..... 4
- 4. SCOPE OF APPLICATION 4
- 5. DEFINITIONS..... 5
- 6. IMPLEMENTATION OF THE DIRECTIVE 8
- 7. NON-COMPLIANCE AND REPORTING..... 8
- 8. DATE OF IMPLEMENTATION 8
- 9. ROLES AND RESPONSIBILITIES..... 8
- 10. MANAGEMENT OF ICT RELATED BUSINESS RISK 8
- 11. SECURITY AWARENESS TRAINING 8
- 12. CLASSIFICATION 9
- 13. INFORMATION SYSTEM ACQUISITION, DEVELOPMENT, AND MAINTENANCE 9
- 14. INTELLECTUAL PROPERTY RIGHTS..... 11
- 15. PHYSICAL SECURITY MANAGEMENT 11
- 16. HR SECURITY 12
- 16.1 HR SECURITY OPERATIONS 12
- 16.2 USER RESPONSIBILITIES..... 12
- 17. COMMUNICATIONS AND OPERATIONS MANAGEMENT 13
- 17.2 SYSTEM OPERATIONS 13
- 17.3 CONTINUOUS VULNERABILITY MANAGEMENT 14
- 17.4 PROTECTION AGAINST MALICIOUS AND MOBILE CODE..... 15
- 17.5 PROHIBITED SOFTWARE 15
- 17.6 NETWORK SECURITY 16
- 17.7 PROTECTION OF INFORMATION SECURITY DEVICES..... 17
- 17.8 BACKUPS..... 17
- 17.9 MEDIA HANDLING 18
- 17.10 DISPOSAL OF MEDIA 18
- 17.11 REMOVAL OF CLASSIFIED DOCUMENTS FROM PREMISES 18
- 18. THIRD_PARTY ACCESS MANAGEMENT..... 19
- 19. ACCOUNTS MANAGEMENT..... 19
- 20. ACCESS CONTROL MANAGEMENT 20
- 21. PASSWORD MANAGEMENT 20
- 22. MOBILE AND REMOTE COMPUTING 21
- 23. USE OF ICT INFORMATION ASSETS 22
- 24. OUTSOURCING REQUIREMENTS 22

25. CYBERSECURITY..... 23

26. CLOUD SECURITY 23

27. ELECTRONIC SIGNATURES 24

28. AUDITING AND MONITORING..... 24

29. ICT SERVICE CONTINUITY AND DISASTER RECOVERY 24

30. ICT SERVICE PROVIDER MANAGEMENT 25

1. INTRODUCTION

The current digital era has seen the increased importance of data and information, thus giving it the status of being the economy's raw material. It has brought the importance of protecting data and information to ensure its *confidentiality, integrity, and availability*.

In line with this, section 3(1)(f) of the Public Service Act, 1994 (Proclamation No. 103 of 1994) provides for the Minister for the Public Service and Administration (Minister) to establish norms and standards relating to information management in the public service.

Furthermore, regulation 94 of the Public Service Regulations, 2016, specifically provides for the Minister to issue information security standards for the public service after consultation with relevant Ministers.

2. PURPOSE

To provide direction in the public service regarding establishing departmental information security governance, practices, and procedures to protect information and technology assets.

3. AUTHORIZATION

This Directive is issued by the Minister in terms of section 41(3) of the Public Service Act to elucidate regulations 94, of the Public Service Regulations.

4. SCOPE OF APPLICATION

This Directive applies to all national and provincial departments, government components, and employees employed in terms of the Public Service Act. This Directive shall only apply to members of the services, educators, or members of the Intelligence Services only in as far as the provisions of this Directive are not contrary to the laws governing their employment.

5. DEFINITIONS

In this Directive, any word or expression bears the meaning which was assigned in the Public Service Act and the Public Service Regulations, unless the context indicates otherwise-

‘Access Control’ means a fundamental component of data security that dictates who's allowed to access and use company information and resources;

‘Access Control List (ACL)’ means a set of rules used to filter traffic

‘Author’ means any employee, or the person acting on his behalf, who prepares, generates, or initially classifies a document or has it classified;

‘AGSA’ means the Auditor-General of South Africa;

‘BCP’ means business continuity plan;

‘CD-ROM’ means compact disc read-only memory;

‘Certificate Authority’ means a certificate authority uses its private encryption key to sign and issue a digital certificate verifying the identity of the certified holder;

‘Classified Information’ means sensitive information which, in the national interest, is held by, produced in, or under the control of the State or which concerns the State, and which must, because of its sensitive nature, be exempted from disclosure in terms of the Protection of Personal Information Act, 2013;

‘Clearing’ means to clear information at a level of media sanitisation that would protect the confidentiality of information against a robust keyboard attack. Simple deletion of items would not suffice for clearing. Clearing must not allow information to be retrieved by data, disk, or file recovery utilities. It must be resistant to keystroke recovery attempts executed from standard input devices and data scavenging tools;

‘Compromise’ means 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;

‘Computer Security’ means– that condition created in a computer environment by the conscious provision and application of security measures. This includes information concerning the procedure for the procurement and protection of equipment;

‘Dimiliterised Zone (DMZ)’ means a perimeter network that protects and adds an extra layer of security to an organization’s internal local-area network from untrusted traffic

‘DISO’ means Department Information Security Officer;

‘DPSA’ means the Department of Public Service and Administration;

‘Encryption’ means a mathematically derived process involving data coding to achieve confidentiality, anonymity, time-stamping, and other security objectives;

‘Firewall’ network security device for monitoring incoming and outgoing network traffic and allows or denies data packets based on a set of security rules. Its purpose is to establish a barrier between your internal network and incoming traffic from external sources (such as the internet) to block malicious traffic

‘Gateway’ means a computer system used to link different networks;

‘GITO’ means a Government Information Technology Officer;

‘Guideline’ is a general rule, principle, or piece of advice;

‘HR’ means human resources;

‘ICT’ means all aspects of technology that are used to manage and support the efficient gathering, processing, storing, and dissemination of information;

‘Incident’ means an adverse event in an information system and/or network or the threat of the occurrence of such an event;

‘Information Assets’ means computers, communications facilities, networks, data, 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 department and should be protected according to the policies;

‘Information Security’ means the provision of organisational, technical, and social measures to safeguard information assets against unauthorised access, damage, and interference – both malicious and accidental;

‘Information Security Event’ means an identified occurrence of a system, service, or network state indicating a breach of information security policy, failure of safeguards, or a previously unknown situation that may be security-relevant;

‘Information Security Incident’ means a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

‘LAN’ means local area network;

‘MISS’ means the Minimum Information Security Standard which is a national government policy document on information security standards that must be maintained by all departments;

‘Minister’ means the Minister for the Public Service and Administration;

‘System Owner’ means a person or organization having responsibility for the development, procurement, integration, modification, operation, maintenance, and/or final disposition of an information system.

‘Network Access Control (NAC)’ means a solution for restricting unauthorized users and devices from gaining access to a corporate network

‘Third-party code’ means software component is a reusable software component developed to be either freely distributed or sold by an entity other than the original vendor of the development platform

‘Trusted entities’ means ICT service providers rendering a service to a government Department

‘**Virtual LAN**’ means a logical group of nodes that appear to be on the same LAN irrespective of the configuration of the underlying physical network.

6. IMPLEMENTATION OF THE DIRECTIVE

The Head of Department must ensure that -

- a) The department has an Information Security Policy.
- b) The departmental Information Security Policy is aligned with the provisions set out in this Directive.

7. NON-COMPLIANCE AND REPORTING

Failure to comply with this Directive will be dealt with in line with the provisions of section 16A of the Public Service Act, 1994.

8. DATE OF IMPLEMENTATION

This directive becomes effective on the date signed by the MPSA.

9. ROLES AND RESPONSIBILITIES

- a) The Head of Department must delegate an official to fulfill the functions of a Department Information Security Officer (DISO).
- b) The Department Information Security Officer (DISO) must be accountable to the GITO for matters of Information Security.
- c) The departmental ICT Steering Committee (established through the Corporate Governance of ICT Policy Framework- CGICTPF) must function as an information security forum.

10. MANAGEMENT OF ICT RELATED BUSINESS RISK

The Head of Department must ensure that ICT-related business risks are identified during their planning cycle and document such risks on a risk register.

11. SECURITY AWARENESS TRAINING

The Head of Department must ensure that -

-
- a) The DISO develops and implements a continuous information security awareness program to reduce cybersecurity risks from employees in the department.
 - b) The information security awareness program must train employees to recognise & report cyberattacks (phishing, baiting, tailgating, etc) as well as train employees to properly handle (store, transfer, and destroy) sensitive data.
 - c) The information security awareness program must include security awareness or skills training targetted for specific roles including system administrators, web application developers, and the helpdesk administrators
 - d) An appropriate summary of the departmental information security policy is included in the HR policies that all employees sign before starting any work in a department.

12. CLASSIFICATION

The Head of Department must ensure that information is classified according to the uniform sensitivity classification scheme below:

- a) **Public:** this information has been explicitly approved by management for release to the public. Examples include reports, announcements, job openings, press releases, service brochures, and information published on the website.
- b) **Confidential:** this information is private or otherwise sensitive in nature and must be restricted to those with a legitimate business need for access. The unauthorised disclosure of this information could adversely impact the department or third parties. Examples include employee performance evaluations, transaction data, agreements, unpublished memorandums and/or submissions, passwords, internal audit reports, and all client information.
- c) **Secret:** this classification applies to the most sensitive business information which is intended strictly for use within a department and restricted to those with a legitimate business need for access. The unauthorised disclosure of this information could seriously and adversely impact the department or third parties.

13. INFORMATION SYSTEM ACQUISITION, DEVELOPMENT, AND MAINTENANCE

The Head of Department must ensure that -

-
- (a) System development or changes to existing systems follow a formal structured approach whereby information security is considered at all stages of the system development life cycle. These include conception and design, development, quality assurance, and implementation as a production system. All systems or application changes follow a formal change control procedure. All associated or supporting documentation must be appropriately updated in response to the changes made;
 - (b) Any system development, including development through a third party, follows an approved system development methodology outlined in the relevant service level agreements and the methodology must include secure application design standards, secure coding practices, and security of third-party code
 - (c) All aspects of how information security is considered and implemented for all new systems or changes to existing systems are recorded. In addition, system developments and changes to existing systems shall have accompanying up-to-date documentation before going live. This must include appropriate sign-offs by the system owner, the GITO, and the Head of Department;
 - (d) The use of production data for development testing is prohibited unless such use is approved by the data owner. The use of desensitized production data should never jeopardize the security or business-related privacy;
 - (e) Business application systems only go into production after users and information operations staff have received appropriate documentation and training on the relevant application security-related controls and practices;
 - (f) When ICT applications are developed:
 - (i) the application is tested and scanned for vulnerabilities. Exploitable and other high-risk vulnerabilities must be remediated before the application is used (Line Management is responsible for ensuring that appropriate testing takes place); and
 - (ii) the following documentation is available:
 - a. technical program documentation;
 - b. end-user documentation;
 - (g) System requesters by default become system owners.
 - (h) The functionality for checking the validity, accuracy, and completeness of data processed is incorporated into systems that are developed;

-
- (i) Data output from an application is validated to ensure that the processing of stored information is correct and appropriate to the circumstances.

14. INTELLECTUAL PROPERTY RIGHTS

The Head of the Department must ensure that -

- a) Any system (software, information, source code, system design documents) developed by and/or on behalf of the department shall remain the intellectual property of the government and may therefore not be copied, sold, leased, or removed without the express of written consent of the relevant executive authority

15. PHYSICAL SECURITY MANAGEMENT

The Head of Department must ensure that -

- a) Physical security measures for all departmental ICT assets (ie. lockable server rooms, switches, cabinets, and/or any other related physical assets that are restricted from public and unauthorised access) are put in place;
- b) There is sufficient protection against environmental threats and hazards such as fire, theft, tampering, water damage, and vandalism;
- c) Multifactor authentication with access logging is implemented in the data centers/server rooms' entrances;
- d) There is adequate security at the entrance of the data center/server rooms and other facilities where ICT infrastructure is housed;
- e) A generator and uninterrupted power supply is available to power critical ICT systems and is tested quarterly and maintained;
- f) Confidentiality agreements and maintenance agreements are in place to ensure the security and confidentiality of the information stored on equipment that is subject to 3rd party and off-site access;
- g) Laptop users have security cables to attach the laptops securely to a desk or similar object, regardless of the location where the laptop is used;
- h) Users who are assigned devices, including portable computers of whatever nature, smartphones, tablets, and peripheral devices that contain government data or have been connected at any time to the government network, do not leave these devices unattended in motor vehicles or public places;

-
- i) FollowMe print must be used to protect the printing of confidential documents. Where FollowMe print cannot be implemented, then users must remove sensitive or restricted documents from printers immediately when printed.
 - j) All users (employees, contractors, and incidental users) are prohibited from making any hardware changes to any shared server or network devices. If there is a business reason for making a hardware change, a change request must be submitted following the department's change management process;
 - k) Non-standard hardware configurations and security configurations (i.e. firewall settings, virtual and physical server settings, router, and switches) are considered for recommendation by the department's GITO;
 - l) Any loss or theft of information assets is treated as a security breach and reported immediately following the departmental loss procedure/protocol. Where necessary and applicable, a mobile device management tool must be implemented to assist with tracking and recovery of government laptops and notebooks.
 - m) Information assets containing government information must be securely stored or retained with the owner while traveling;
 - n) Process, procedures, or technical controls are in place to manage the risks associated with removable media (i.e. data leaks, data loss, data privacy, data sensitivity, malware infection, etc)

16. HR SECURITY

16.1 HR SECURITY OPERATIONS

The Head of Department must ensure that -

- a) The security roles and responsibilities of employees, and third-party users are defined and documented in the Information Security Policy;
- b) Background verification checks or security vetting of contractors, and external party users are carried out under relevant laws, regulations, and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks;

16.2 USER RESPONSIBILITIES

The Head of Department must ensure that -

-
- a) All personnel is responsible for all activities performed with their user identities and special logon identities. As such, user identities and other logon identities may not be used by anyone other than the persons to whom they have been issued and users shall not perform any activity with identities belonging to other users.
 - b) Passwords are never shared or revealed to anyone else and should never be known by anyone other than the authorised user.
 - c) Users submit a request to the help desk to issue a new password if a password is forgotten, and users must prove their identity before the password is issued or reset
 - d) Users report any misuse or unlawful use of user identities and passwords to the help desk,
 - e) The unsuccessful login attempts are logged, and investigations should occur where unsuccessful login attempts are out of the normal range.

17. COMMUNICATIONS AND OPERATIONS MANAGEMENT

17.2 SYSTEM OPERATIONS

The Head of Department must ensure that-

- a) Controls for ICT operations are documented and must include employee duties and formal methods to implement changes to ICT systems;
- b) A formal change control procedure is documented and enforced to govern the application, computer installation, networks, and system development changes;
- c) The relevant system owner approves all business application changes with a financial impact. The GITO must recommend all infrastructure/architectural changes;
- d) ICT systems are accessed and authenticated through the Department's network. The GITO must approve secure emergency remote access/alternative network connection methods;
- e) Emergency changes that bypass some of the elements of the established change control system require the authorisation of all affected business units/ branches and acknowledgment of the risks involved. These actions must be controlled, logged, restored, and kept to a minimum;
- f) Production systems are physically separated from test and development systems. Where this is not feasible, all reasonable efforts must be made, to ensure that

production systems are protected from changes or outages in non-production environments;

- g) The development of new applications or system software is kept separate, both physically and logically, from the production environment. The employee responsible for the development should not normally have access to production systems. For occasional and essential support purposes, the development employee may be granted restricted access for a limited period (e.g., by issuing secure passwords via an emergency access process);
- h) All activities related to changes of systems and performed using supervisory access rights will only be performed once appropriate authorisation is received through the change control process, accompanied by change control documentation. The results of the change will be compared with the change request. This review must be signed-off or electronically verified by the appropriate manager;
- i) The segregation of duties matrix is developed and maintained by all business units in the department. It should contain all user roles and associated access, and any conflicts or roles with excessive access that can result in unauthorised or fraudulent transactions or activities should be reviewed, adjusted where possible, or monitored closely. The segregation of duties matrix should be reviewed by system owners periodically.
- j) Approval and confirmation of the new ICT system satisfy all necessary security requirements before that system is used in a department or government production environment.

17.3 CONTINUOUS VULNERABILITY MANAGEMENT

The Head of Department must ensure that -

- a) The network infrastructure is kept-up-date and is running the latest and stable software versions.
- b) Operating system updates and application updates are performed at least once a month or more regularly through a patch management process.
- c) Bi-annual vulnerability scans and vulnerability remediation are performed through a vulnerability management process.

17.4 PROTECTION AGAINST MALICIOUS AND MOBILE CODE

The Head of Departments must ensure that -

- a) All information devices connected to the government network has up-to-date antivirus and integrity-checking software installed.
- b) Employees do not knowingly distribute viruses or bypass any detection systems in place.
- c) Employees exercise caution when opening any email if the source of the email is unknown to the user.
- d) Employees receiving or downloading data media from any source within, the public service has the responsibility for ensuring that it is checked for viruses before use. Similarly, individuals intending to pass on data media within government or to external parties must ensure that it is first scanned for viruses.
- e) Employees are prevented from disabling or changing the configuration of the antivirus software installed on their personal computers.
- f) Autorun for removable media is disabled to control the installation and execution of malware
- g) Suspected malicious code attacks are reported immediately on identification by following the internal security incident management procedure.
- h) New software, portable media, and information in electronic format from external sources are scanned for malicious program code before being introduced into the department network.

17.5 PROHIBITED SOFTWARE

The Head of Department must ensure that -

- a) The employees are made aware that the use of the following software is prohibited on any computer departmental network unless specifically recommended by the GITO.
 - i Bootleg software: illegal, pirated, or reproduced copies of software or data.
 - ii Powerful system tools: programs that are designed to investigate and/or exploit a department's information security environment (including password

-
- crackers, scanners, network sniffing devices, network packet sniffing devices, and other hacking tools).
 - iii Shareware/freeware: all software available from the Internet, where no licensing requirements are given.
 - iv Personal/non-department software.
 - v Inappropriate content: images and /or text involving race, nudity or sexual themes are not appropriate for the workplace
- b) A list of approved software is developed and maintained to identify and prevent the installation of malicious software.

17.6 NETWORK SECURITY

The Head of Department must ensure that -

- a) Responsibilities for network configuration and operational management are segregated from systems configuration and operational management.
- b) Establish and maintain the secure configuration of ICT assets (i.e. workstations devices, mobile devices, network devices, virtualization platforms, and servers) and software (operating systems and applications).
- c) Secure network architecture is established and maintained through segmentation and segregation. i.e. Virtual LANs, ACL, Firewalls, DMZ, NAC, Least privilege & Need-to-know principles, etc
- d) Information regarding Internal addresses, configurations, related system design for the department, government networks, and computer systems are restricted so that both systems and users outside the internal network cannot access this information without written approval from the Head of Department.
- e) The creation of a remote access facility never compromises the security of a department or government network or any existing department system or data.
- f) The layout of wiring and all network devices is documented.
- g) Firewall rules are reviewed regularly.
- h) Inactivity timeouts are implemented for remote access connections (i.e. idle sessions for applications, unattended workstations, etc) requiring users to re-authenticate following a timeout.

-
- i) All computers with wireless LAN devices use an approved department or government virtual private network (VPN) configured to drop all unauthenticated and unencrypted traffic.
 - j) The Wireless LAN service set identifier (SSID) is configured so that it does not contain any identifying information about a department, such as a department name, division title, employee name, or product identifier.
 - k) Government employees or other personnel are prohibited from establishing simultaneous connections to both external networks and government networks.
 - l) All remote access usage and logs are monitored regularly (i.e.failed access attempts, user lockouts, and unusual remote access attempts).
 - m) ICT service provider networks and government networks are segregated into logical and physical segments or network domains based on the value and classification of information or assets that need to be accessed.
 - n) GITO authorises all connections to the Department network.

17.7 PROTECTION OF INFORMATION SECURITY DEVICES

The Head of Department must ensure that -

- a) Secure gateways, firewalls, and other protection devices are used to maintain the level of security when elements of different trust levels are brought together.
- b) Security systems operating within and across public and department networks are protected against internal and external intruders. The systems are to be installed in a physically secured and access-restricted area.
- c) Only trusted entities are allowed full access to the department network. All entry points to the department network must be reviewed and approved by the GITO.

17.8 BACKUPS

The Head of Department must ensure that -

- a) Backups are performed frequently, based on the sensitivity of the data
- b) Regardless of classification, the availability of all data is maintained through periodic backups and recovery mechanisms.
- c) Department backups are covered in the existing contract/arrangement of any service provider and the backups containing sensitive data are encrypted.

-
- d) The department's minimum and maximum retention periods of information are based on contractual, legislative, regulatory, or industry requirements. The information must be retained for as long as necessary, but for no longer than the data owner's requirements.
 - e) All archival backup data stored off-site is reflected in an up-to-date directory that shows the most recent date when the information was modified and the nature of the information.
 - f) All storage devices on which sensitive, valuable or critical information is stored for periods longer than six months must not be subject to rapid degradation. Such media must be tested at least annually to ensure that the information is still recoverable.

17.9 MEDIA HANDLING

The Head of Department must ensure that -

- a) Government information is always stored/saved on Departmental network servers.
- b) Removable computer media is protected against unauthorised access. Any loss or theft of removable computer media must be treated as a security breach and reported immediately.

17.10 DISPOSAL OF MEDIA

The Head of Department must ensure that -

- a) That destruction of storage devices is conducted only by trained and authorised personnel. Safety and special disposition must be identified and addressed before conducting any media destruction.
- b) The disposal of removable media is performed in such a manner that the data is not recoverable.

17.11 REMOVAL OF CLASSIFIED DOCUMENTS FROM PREMISES

The Head of Department must ensure that -

- a) A destruction/disposal certificate is supplied to the author.

-
- b) A business unit retention and disposal plans, and other legal and standard obligations are consulted to ensure the timely disposal of information that is no longer required by the government.
 - c) Retention schedules are developed and implemented.
 - d) Records are available to the entire department or only a designated part of the department, based on the user's access permissions.
 - e) Records are retained for a period as determined by legislation or best practices.

18. THIRD_PARTY ACCESS MANAGEMENT

The Head of Department must ensure that -

- a) ICT human resources from external service providers are suitably vetted, or an oath of secrecy is signed following the institution's security requirements.
- b) External/third-party access to department information assets is only authorised in cases where there is a clearly defined business need. The access facility provided should limit the external/third party to the agreed method of access, the agreed access rights, and the agreed level of functionality.
- c) External ICT consultants, computer security response teams, contractors, or temporary staff who require access to the department network must seek authorization in line with the governance arrangements.
- d) As part of an outsourcing contract procedure, a risk assessment is carried out under the guidance of the DISO to determine the security implications and security control requirements.

19. ACCOUNTS MANAGEMENT

The Head of Department must ensure that -

- a) A user account registration process is established and maintained. The process must include the use of formal user registration forms (soft copy, hard copy, or online) to create accounts or grant access to the department network and computer systems. The form(s) must be signed off as an acknowledgment that they understand the conditions of the access granted to them.
- b) Users must use authorised user accounts (unique usernames and passwords) to access government computers, systems, emails, and internet facilities.

20. ACCESS CONTROL MANAGEMENT

The Head of Department must ensure that -

- a) Formal access granting, access review, and access revoking processes are established and maintained. These processes must be founded on role-based access control, the least privilege principle of security, and keeping & maintaining records of granted and revoked privileges or access. The above ensures that users have access only to -
 - i. Their own files and data;
 - ii. Publicly available files;
 - iii. and/or files that they have been authorised to access.
- b) Systems requiring protection against unauthorised access have the allocation of privileges controlled through a formal authorisation process and a record of all privileges allocated must be maintained.
- c) Login privileges or access allocated to users on a need-to-use and event-by-event basis is authorised, i.e., the minimum access required to perform the role.
- d) Department's systems and technical support staff align to a clear separation of functions (such as system administrators vs regular users) to prevent unauthorised access and functions from being performed.
- e) Users' access rights are enforced by automated access control mechanisms (e.g., menus to control access to application functions; and read, write, delete and execute permissions/limitations) to ensure individual accountability.
- f) Privileged accounts must not be used for day-to-day use such as reading emails or accessing the internet.
- g) Privileged access rights, which allow users to override system controls, are regularly reviewed by the GITO and system owners including access rights review of service accounts. It is recommended that these reviews occur more frequently (every three months) than for other access rights.
- h) User access rights are reviewed and re-allocated when an employee moves from one business unit to another within a department.

21. PASSWORD MANAGEMENT

The Head of Department must ensure that -

-
- a) A formal password standard is established and maintained. The password standard must define the length of a password (not less than eight(8) characters), the composition (alphanumeric) and the frequency of change and reuse of passwords.
 - b) Password authentication is used to prevent unauthorized access to transversal government ICT systems and department ICT systems.
 - c) That a procedure for issuing user identities and new or changed passwords is established and implemented with sufficient controls to prevent social engineering attempts from succeeding. A user's identity must be confirmed before resetting a password, providing a temporary password, or issuing a new password.
 - d) Initial passwords issued to new users or when a password is reset are temporary, forcing the user to change the password immediately when he/she logs in to the network with the new password.
 - e) New or changed passwords are communicated to a user securely. The use of electronic mail messages should be avoided when communicating issued passwords.
 - f) Passwords are changed immediately if there is an indication of system or password compromise.
 - g) All stored passwords are encrypted.
 - h) Default system administrator account passwords are changed immediately upon installation, default administrator accounts are renamed where applicable, and the system and guest accounts are disabled
 - i) Multifactor authentication (MFA) is used on critical systems to enhance security measures by providing an additional layer of protection using a combination of authentication factors (OTP, Graphical passwords(CAPTCHAs), Biometrics).

22. MOBILE AND REMOTE COMPUTING

The Head of Department must ensure that -

- a) Line management authorises the issuing of portable computers.
- b) A formal risk analysis process for applications to which remote access is granted to assess risks and identify controls needed to reduce risks to an acceptable level.
- c) A procedure for remote user access authorisation and management is established.

-
- d) A register of all staff members authorised to use remote access facilities is maintained by the DISO.
 - e) The register of authorised remote access users and the access levels provided is reviewed regularly by system owners and the DISO to confirm that there is still a valid business requirement.
 - f) Users are prohibited from altering or disabling any security features that have been enabled on wireless connections.

23. USE OF ICT INFORMATION ASSETS

The Head of Department must ensure that -

- a) The administrator and root-level system accounts are strictly controlled.
- b) Access to administrator and root level accounts is only granted by a DISO and delegation must be kept to an absolute minimum.
- c) Supervisory access rights are allocated on a business need basis and will be limited to the minimum services and functions necessary. Additional security measures must be implemented to ensure that they are used only for the intended purpose.
- d) The processes to control the allocation, revocation, and review of powerful access rights are in place. These processes will include authorisation of all access rights by the appropriate line management and mechanisms to ensure that access rights are adjusted appropriately should the person leave or change the job description.
- e) Critical logical access activities performed using powerful access rights generate audit trails and will be logged. All audit trails and logs must be reviewed monthly by the information owner and/or the GITO and stored for one year.
- f) Power users do not share usernames and they must be given their unique usernames; therefore, no system generic usernames will be used.
- g) A procedure allowing staff to obtain emergency access is in place and the assignment of this access will be reported and reviewed by the DISO. Emergency access must be revoked subsequently.

24. OUTSOURCING REQUIREMENTS

The Head of Department must ensure that -

-
- a) Outsourcing complies with Condition 7 of Chapter 3 of the Protection of Personal Information Act, 2013 (Act No. 4 of 2013).
 - b) All consultants, temporary employees, and contractors must return all department and government property upon termination or expiration of their contract and all associated government network access (including remote access) rights should be simultaneously terminated.
 - c) External parties only use the information assets entrusted to them for the purposes agreed to in their contract.
 - d) The confidentiality and integrity of sensitive information will be protected when accessed through external party connections. A formal risk analysis must be conducted for each external party connection and appropriate controls must be implemented to reduce risks to an acceptable level.
 - e) A regular review of all previously approved external party access is conducted by the GITO. Any changes to the conditions under which the external party access was previously granted will be reviewed by GITO.
 - f) The external party users are restricted to the minimum services and functions necessary for the business process, as determined by the system owner.
 - g) As a condition of gaining access to a department's computer network, every external party computer must be checked by to ensure that the computer's antivirus software is up to date.
 - h) A register of authorised external party access users, as well as the access levels provided, is reviewed regularly (at least quarterly for ongoing contracts and ad hoc when access is set up) by the DISO to confirm that there is still a valid business requirement.

25. CYBERSECURITY

The Head of Department must ensure that -

- a) Penetration testing, vulnerability scans, and threat risk analysis are part of the departmental cybersecurity initiatives.

26. CLOUD SECURITY

The Head of Department must ensure that -

-
- a) Thorough due diligence of the service provider's integrity, legal agreements, physical location, and security must be conducted before deciding on a cloud service provider.

27. ELECTRONIC SIGNATURES

The Head of Department must ensure that -

- b) The use of the electronic signatures solution is approved.
- c) The level of electronic signature selected is appropriate when considering the risks associated with a particular document or approval process.

28. AUDITING AND MONITORING

The Head of Department must ensure that -

- a) Audit log management (collect, alert, logs review, and retain) occurs to detect malicious activities early. This includes the network traffic through both internal and external gateways, e.g., firewalls, email gateways, Intrusion Detections, and routers monitored for unusual activity (for example, abnormal combinations of connections, deliberate probing, or attacks, and unusually substantial amounts of data being transferred cross-border).
- b) Systems to which external parties have access (such as client systems, web servers, and dial-up support facilities) have all transactions and system configuration changes monitored in real-time, with alerts escalated to appropriate personnel where unauthorised transactions occur. Such access must be disconnected when not in use.
- c) Computer clocks are synchronized to ensure the accuracy of audit logs for investigations or as evidence in legal or disciplinary cases. Computers and communication devices that can operate as real-time clocks should be set to an agreed standard.

29. ICT SERVICE CONTINUITY AND DISASTER RECOVERY

The Head of Department must ensure that -

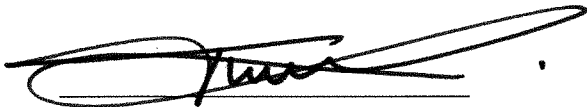
- a) There is an ICT service continuity plan that supports the business continuity of the department.
- b) The continuity plans must include the establishment and maintenance of adequate data recovery processes and data restore testing to prove data recoverability.

30. ICT SERVICE PROVIDER MANAGEMENT

The Head of Department must ensure that -

- a) There is a process to evaluate ICT service providers who have access to sensitive data or hold sensitive data or a have responsibility for ICT infrastructures to ensure the protection of the data and infrastructure.
- b) Security requirements are included in the contracts of the service provider (Data encryption, multifactor authentication)

**APPROVED BY THE MINISTER FOR THE PUBLIC SERVICE AND
ADMINISTRATION**



MR T.W. NXESI, MP

ACTING MINISTER FOR THE PUBLIC SERVICE AND ADMINISTRATION

DATE: 07/06/2022