



Information Security Policy

Effective Date: 3 December 2019

Document Classification:

Confidential

© GEPF 2019

Table Contents

1. Document Versions.....	4
2. Business Areas Impacted by this Policy	4
3. Terms and Definitions	4
4. Introduction.....	10
5. Objective	10
6. Purpose	11
7. Scope of application	11
8. Information Security Policy	11
8.1. Information Labeling and Handling	13
8.2 Information Classification	13
8.3 Disposal of Information	13
8.4 Information Backup	13
8.5 Electronic records management	14
8.6 Duplication of documents.....	14
8.7 Removal of Information.....	14
8.8 Prevention, Detection and investigation of misuse	14
8.9 Legislation.....	14
9. ICT Security.....	15
9.1 User Access Management.....	15
9.3 Physical Network Controls.....	16
9.4 Wireless Network Usage and Access	16
9.5 Network and operational security	16
9.6 E-mail usage	17
9.7 Internet usage.....	17
9.8 Use of cloud storage services	18
9.9 Software usage and asset management.....	18
9.10 Removable media management.....	18
9.12 Malicious activities and codes	20
9.13 Environmental Controls	20
9.14 Physical Access to Data Centers	20
9.15 Backup and disaster recovery	21
9.16 Cabling Security	21

9.17	Equipment Maintenance.....	21
10.	Business Continuity Management.....	22
11.	Human Resource employment and engagement.....	22
12.	Change management.....	22
13.	Non-compliance and corrective action.....	22
14.	Roles and responsibility.....	22
15.	Employees on Suspension.....	23
16.	Policy review	23
17.	Approval	23

1. Document Versions

Version	Revision Date	Prepared by	Business Unit	Status
V1.0	19 January 2012	Gordon Oyomno	Manager: GPAA ICT	Draft
V2.0	3 April 2012	Joelene Moodley	Head: Corporate Services	Draft
V3.0	7 August 2012	Siyanda Dyeshana	Manager: Resources	Draft
V4.0	10 May 2017	Musa Mabesa	Finance Manager	Draft
V5.0	15 October 2019	Paul Masipa	Manager: ICT	Final Draft

2. Business Areas Impacted by this Policy

Name Business Unit/Area	Context and Relevance
All users who act on behalf of the GEPF or are in its employment.	To promote the business continuity of the GEPF information systems and the information they contain.

3. Terms and Definitions

Abbreviations	Descriptions
Availability	Refers to ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to, or use of information or an information system.
Confidentiality	Protecting information from unauthorized access and disclosure.
Device	Any computer or electronic device capable of accessing, storing and communicating data.
Disaster	Any event or occurrence that prevents the normal operation of Electronic Information Resource(s) for a period of time, such that the resulting disruption and/or losses exceed the acceptable limits established consistent with these Guidelines. A disaster may occur as a result of a natural disaster (such as a flood, fire or earthquake), employee error or other accidents, long-term system failures, and criminal or malicious action.
Disaster Recovery Plan (DRP)	A written plan including provisions for implementing and running Electronic Information Resources at an alternate site or provisions for equivalent alternate processing in the event of a disaster.

Abbreviations	Descriptions
Encryption (of data) or Cryptography	The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file/data, you shall have access to a secret key
ICT	Information and Communication Technology
Information Security	Means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction.
Integrity	Safeguarding the accuracy and completeness of information and processing methods.
Intrusion Prevention Systems (IPS)	Is used in computer security. It provides policies and rules for network traffic along with an intrusion detection system for alerting system or network administrators to suspicious traffic, but allows the administrator to provide the action upon being alerted.
GEPF	Government Employees Pensions Fund.
Security	Measures taken to reduce the risk of 1) unauthorized access to or modification of Electronic Information Resources, via either logical, physical or managerial means; and 2) Damage to or loss of Electronic Information Resources through any type of disaster (such as employee error or other accidents, long-term system failures, natural disasters, and criminal or malicious action). Security also encompasses measures taken to reduce the impact of any violation of security or a disaster that occurs despite preventive measures.
Server	A computer or device on a network that manages network resources. For example, a file server is a computer and storage device dedicated to storing files.
System Administrator	An individual responsible for maintaining a multi-user computer system.
Finance and Audit Committee (FAC)	Steering Committee established to monitor implementation of ICT governance within the GEPF.
Access control	Refers to the process of controlling access to systems, networks and information based on business and security requirements.
Access point name or SSID	Access Point Name is a computer protocol that typically allows a user's computer to access the internet using the mobile phone network. Service set identification. This is a unique identifier for a particular wireless local area network
GEPF environment	GEPF's technology resources comprise of computing, networking and software applications that can be accessed by authorized GEPF users.

Abbreviations	Descriptions
Approved time source	A reliable time source that information technology (IT) systems or devices are able to use as a standardised time source. This is often achieved through the use of a network time protocol.
Audit trail	A record showing who has accessed a computer system and what operations he or she has performed during a given period of time.
Authentication	It is the act of verifying that an entity is what it claims to be; this could be performed on a person, device or an application.
Authentication credentials	The details used in the verification of the claimed identity through an authentication process.
Authorisation	Granting access to an individual to access a system and/or network device.
Availability	Refers to ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to, or use of information or an information system.
Breach	An information security incident resulting in the unauthorised loss, modification, or disclosure of information.
Business and security requirements	Business requirements describe the functional and non-functional attributes of an IT system, service or device from a business perspective. Security requirements are required in order to support the business requirements.
Business application owner	The person who specifies and authorises business applications.
Control	A control is any administrative, management, technical, or legal method that is used to manage risk. Controls are safeguards or countermeasures. Controls include practices, policies, procedures, programs, techniques, technologies, guidelines, and organisational structures. Controls can be deterrent, preventive, protective, detective or corrective.
Cybercrime	Refers to any criminal or other offence that is facilitated by or involves the use of electronic communications or information systems, including any device or the Internet or any one or more of them.
Data	Electronic or non-electronic information including client's personal information
Default account	Any account on an IT system that is already present after the operating system and/or system components have been installed
Denial of service	An attempt to make a computer resource unavailable to its intended users.

Abbreviations	Descriptions
Demilitarised zone (DMZ)	A physical or logical sub-network that contains and exposes organisation's external services to the untrusted network (internet).
Electronic data destruction	The action of secure removal of data from any IT system, service or device. This is performed before any IT asset is disposed of.
External network connections	A connection point where GEPF network is connected to a non-GEPF network.
Third Party / External user	Refers to a user who has access to user systems but not necessarily employed by the GEPF
File sharing	Refers to the activity of putting a file in a common repository for the purpose of sharing the file with other people
Identification	Refers to the process of uniquely naming or assigning an identifier to every individual or system to enable decisions about the levels of access that shall be given.
Information asset	Refers to a definable piece of information in any form (physical or electronic), recorded or stored on any media.
Information owner	The information owner is usually the head of a business unit where the information is captured.
Intrusion detection system (IDS)	A real-time monitoring process or device that analyses IT systems and network activity for unauthorised entry and/or malicious activity
Intrusion protection system (IPS)	A technology equipment/device or software application that monitors a computing network or systems for malicious activity or policy violations
Malicious code	Malicious code is used interchangeably with malicious software. It refers to software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems or any data that is prohibited from being accessed as determined by the GEPF.
Penetration test (pentest)	A method of evaluating computer and network security by simulating an attack on a computer system or network from external and internal threats.
Personal Information	Any information that can uniquely identify a living natural person or existing juristic person, as defined in the POPI Act.
Physical security	Refers to providing environmental safeguards for controlling physical access to equipment and data on the GEPF network in order to protect ICT resources from unauthorised use, in terms of both physical hardware and data perspectives.

Abbreviations	Descriptions
Risk assessment	Refers to a process which determines what information resources exist that require protection and to understand and document potential risks from ICT security failures that may cause loss of information confidentiality, integrity or availability.
Security event	An event on an IT system that may occur as a result of one or more of the following activities: unauthorised access, malicious software outbreak, fraud, theft, and other actions related to the misuse
Sensitive information	Refers to privileged or proprietary information or personal information, which, if compromised through alteration, corruption, loss, misuse or unauthorised disclosure, could cause serious harm to the GEPF, employees as well as third parties.
Classification	The act or process of identifying and grading information in protection categories according to its sensitivity or in compliance with a security requirement and which requires protection from unauthorized disclosure.
Classified information	Sensitive or proprietary information which is produced in or is under the control of the GEPF or which concerns the functions of the GEPF and due to its sensitive nature must be protected against compromise, either accidentally or purposefully.
Compromise	The unauthorized disclosure, exposure or loss of classified, sensitive, personal or proprietary information, whether by design or through negligence.
Confidential	The protection level assigned to information of which the unauthorized disclosure, observation or loss thereof may cause harm to the objectives and functions of the GEPF
Copying/Duplicating/Reproducing	The duplicating of information in either paper based or electronic form through either manual copying or electronic, photographic or digital means.
Document	Any note or writing, whether produced manually or electronically; Any copy, plan, picture, sketch, photographic image or other representation of any place or article, produced Any disc, tape, card, perforated roll, or other device in or on which sound or any signal has been recorded for production; Any rubber stamp displaying information.
Segregation of duties	Refers to separating certain areas of responsibility and duties in an effort to reduce fraud and unintentional mistakes, for example, the person who captures a transaction shall not be the same person approving it.
Trusted network	Refers to a network that is within the GEPF's control and conforms to the GEPF security policies

Abbreviations	Descriptions
Untrusted network	Any network that does not form part of the trusted GEPF network.
Virtual private network (VPN)	Refers to a network that uses a public telecommunication infrastructure, such as the internet, to provide remote offices or individual users with secure access to the GEPF's network. VPNs use encryption and other mechanisms to ensure that only authorised users can access the network and that the data cannot be intercepted.
Trustees	Trustees refers to Trustees as well as Substitute Trustees
User	Anyone with authorised access to the GEPF business information systems, including permanent and temporary employees, Trustees or third-party personnel such as temporaries, contractors, consultants, agents and other parties with valid GEPF access accounts GEPF user.

4. Introduction

The main goal of the information security policy is to enhance data protection by defining procedures, guidelines and practices for configuring and managing information security in the corporate environment. It is imperative that the policy defines the organisation's philosophy and requirements for securing information assets. It is also important that the policy outline how it will apply to corporate user, processes and environments.

Consequences for failed compliance shall also be addressed. A successful information security policy provides several benefits to GEPF. Enforceable policies ensure that vulnerabilities are identified and addressed—protecting business continuity and fortifying the Information Technology infrastructure.

When users throughout the GEPF follow a security policy, ensuring that information is safely shared within the organisation as well as with external entities, partners and vendors, this mitigates corporate risk. Also, the heightened security awareness once the security policy is in place increases the likelihood of individual compliance.

5. Objective

This policy creates a broad baseline of Information Security related requirements and acts as the overarching regulatory document that will ensure that the GEPF complies with all regulatory information structures when adhered to. Following adoption, several aspects referred to in this policy will be addressed in more detail in other, subject related policies.

Furthermore, this policy aims to:

- Ensure the implementation of appropriate protection measures so as to minimise the Risk of theft, fraud, theft, malicious or accidental damage, human error, breach of privacy or confidentiality; misuse of Information resources, sabotage, espionage ;
- Ensure that defined standards, processes and procedures within the ICT are adhered to;
- Outline governance and responsibilities of those involved in ICT Management and operation of the Information systems which will be adequately segregated;
- Establish an Incident Management framework and operational process that will ensure the rapid identification and resolution of Incidents in such a way that the business impact will be minimised and the Risk of similar Incidents occurring will be mitigated if not eliminated;
- Minimise the risk of systems failures and protect the integrity of software and Information;
- Ensure integrity and availability of Information and Information systems through appropriate backup of systems and data;
- Ensure adequate protection of Information being exchanged between GEPF and other outside organisations;
- Ensure security of electronic commerce services and their secure use;

- Ensure the timely detection of unauthorised Information processing activities; and
- Protect the GEPF from damage or liability arising from the use of its ICT facilities provided by its service provider, for purposes contrary to its legislation and policies.

6. Purpose

This policy establishes:

- The governance of Information Security within GEPF in order to guide users and serves as a reference for protection of all GEPF information.
- Specify the measures required to protect, prevent, detect and respond Information Assets from all types of threats, whether
 - internal or external, deliberate or accidental;
- It provides assurance to stakeholders that reliance may be placed on GEPF data or information in the information systems and appropriate control measures are implemented to manage the Risk of:
 - Breach of confidentiality
 - Breach of integrity
 - Loss of accessibility
 - Breach of legislation
 - Loss of reputation
- Ensure that appropriate measures are put in place to protect corporate information and information systems, services and equipment of the GEPF based on the security, business and legislative requirements.

7. Scope of application

This policy applies to all users with a GEPF-owned or personally-owned computer or workstation used to connect to the GEPF network.

The provisions of this policy also apply to the members of the Board of Trustees once they have been issued with iPad devices.

8. Information Security Policy

The policy:

- Ensures that information will be protected, commensurate with the risk of its unauthorised disclosure and malicious or inappropriate use, so that:
 - ◆ The confidentiality of information will be assured;

- ◆ The integrity of information, that its accuracy and completeness, will be maintained;
 - ◆ The availability of information and information system will meet business requirements;
 - ◆ Safeguarding of information.
- Ensures that all controls shall be appropriate to the risk identified in the risk assessment exercises.
 - Ensures that all material information security breaches will be reported to the Board and the Board will review this policy annually and/or when significant changes occur, to ensure the suitability, adequacy and effectiveness of the policy. The information security policy shall be approved and enforced by the Board.
 - Shall be published and communicated to users who act on behalf of the GEPF or are in its employment.
 - Shall be revised in accordance with the document management policy and/or when significant changes occur, to ensure the suitability, adequacy and effectiveness of the policy. The information security policy shall be approved and enforced by management.
 - It is the responsibility of users to ensure that they read this policy and that an understanding of the policy.
 - Shall be communicated to users in a form that is relevant, accessible and understandable to the intended reader, e.g. in the context of an “information and cyber security awareness, education and training program”.
 - Information security practices shall
 - ◆ be integrated into essential business activities of the GEPF
 - ◆ deliver value and meet GEPF strategic objectives.
 - All information security roles and responsibilities are clearly defined and documented.
 - GEPF shall enforce a business continuity environment, which will ensure and secure the availability of all its Information Assets.
 - Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the organisations information and information processing assets.
 - Management shall actively support security within the organisation through clear direction, demonstrated commitment, explicit assignment, and acknowledgement of information security responsibilities as defined in the information security roles and responsibilities of this policy.
 - Users required to sign an oath of secrecy or non-disclosure agreement (as the case may be) upon commencing employment or engagement with GEPF and prior to obtaining access to GEPF’s information assets and information processing assets

8.1. Information Labeling and Handling

An appropriate set of procedures is required for information labeling in accordance with the classification scheme adopted by GEPF. These procedures need to cover information assets in physical and electronic formats. Suitably strong encryption measures must be implemented for sensitive information at rest, during transmission and in storage. For each classification, handling procedures shall be defined to cover the following types of information processing activity:

- (a) Copying;
- (b) Storage;
- (c) Transmission by post, fax, and electronic mail;
- (d) Transmission by spoken word, including mobile phone, voicemail, answering Machines; and
- (e) Destruction.

8.2 Information Classification

This policy will ensure that information resources of GEPF are classified, sorted and labeled according to their value, importance, sensitivity, cost and any other concerns in order to guide the implementation of security and prescribe processes of management and use. The assigning of labels such as Public, Private, Sensitive, Internal Only, Confidential and Proprietary etc., will help GEPF users to understand how to use and handle information resources properly. Information will be classified, using the Minimum Information Security Standards (MISS) as a broad baseline guide document.

Corporate Services, together with business unit managers shall determine the category of information according to whether it is of a High, Moderate or Low sensitivity.

When the lifetime of the relevant information has lapsed, the information shall be declassified or disposed of.

8.3 Disposal of Information

GEPF users have a responsibility to apply officially approved security measures when disposing of paper copy information in the course of their work.

Redundant, re-allocated and re-usable electronic media containing sensitive information shall be cleaned or destroyed.

8.4 Information Backup

Backup copies of essential business information and software shall be taken regularly. Adequate backup facilities shall be provided to ensure that all business information and software can be recovered following a disaster or media failure.

Backup arrangements for individual systems shall be regularly tested to ensure that they meet the requirements of the business continuity plans.

8.5 Electronic records management

Creation of records in accordance with business, legal and regulatory requirements is the responsibility of process owner.

Measures must be put in place to ensure that records are recoverable in the event of a disaster

Records must be disseminated and stored in a manner that will not compromise GEPF's confidentiality of data and information security policies and standards.

Records must be retained in accordance with the retention periods applicable with reference to the appropriate regulations and statues

8.6 Duplication of documents

Duplication information, either manually or through electronic means shall be done according to the stipulations indicated the GEPF's Document Security Policy.

8.7 Removal of Information

GEPF information may only leave GEPF premises and offices after the removal thereof has officially been approved according to the stipulations contained in the GEPF's Document Security Policy and Portable Devices Policy. Information communicated via email or any such technology shall be guided by the provisions of the various policies dealing with GEPF information e.g. email and internet policy.

8.8 Prevention, Detection and investigation of misuse

GEPF retains the right to access all information held on its information and communications facilities, to monitor or intercept any system logs, web pages, e-mail messages, network account or any other data on any computer system owned by or connected to the networks of the GEPF. This will be for the purposes of preventing, detecting or investigating crime or misuse, ascertaining compliance with regulatory standards and GEPF policies, and / or to secure effective system operation. Monitoring of computer facilities usage may take place periodically and users shall have no expectation of privacy.

8.9 Legislation

This policy is subject to the provisions of the following acts and / or regulations associated therewith:

- (a) The Electronic Communications and Transactions Act (Act No. 25 of 2002);
- (b) The Promotion of Access to Information Act (Act No. 2 of 2000);

- (c) The National Archives and Records Service of South Africa Act (Act No. 43 of 1996 as amended);
- (d) The Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 (Act 70 of 2002)
- (e) Protection of Personal Information Act, 2013 (Act No. 4 of 2013) (POPI)
- (f) Protection of Information Act (84 of 1982)
- (g) Minimum Information Security Standards (MISS)

9. ICT Security

9.1 User Access Management

Formal procedures shall be in place to control the allocation of access rights to information systems and services. The procedures shall cover all stages in the lifecycle of user access, from the initial registration of new users to the final deregistration of users who no longer require access to information systems and services. Special attention shall be given, where appropriate, to the need to control the allocation of privileged access rights, which allow users to override system controls. A proper user registration / deregistration process shall be established to control user access and avoid illegal access.

Every Employee must have a unique Employee identification. Access to Information Assets must only be permitted once the Employee has been identified, authorised and authenticated. The level and strength of authentication must be implemented based on the importance of the Information stored on the Information Assets.

Refer to the GEPF Password and user access policy. Users shall enable a keyboard / screen lock that is activated by a period of inactivity (of no longer than 15 minutes), in order to prevent unauthorised access to their systems in the event where they are away from their offices / desks / systems for extended periods of time.

9.2 Logging and monitoring

- ICT system administrators and information owners must ensure that the logging and monitoring requirements of an information system are defined in the relevant procedures and implemented.
- Access to audit log files shall be restricted to authorised individuals to protect the information against tampering.
- Clock-Synchronisation mechanisms shall be put in place and linked to a single reference time source to ensure the accuracy of audit logs.
- The logs shall be reviewed regularly to identify unauthorised or suspicious activities.

9.3 Physical Network Controls

- A range of network controls is necessary to achieve and maintain security in computer networks. Network controllers must implement controls to ensure the security of data in networks, and the protection of connected services from unauthorized access.
- Connections to GEPF networks must be authorised and authenticated.
- User file shares must only be created using authorised file sharing mechanisms.
- Remote access must only be permitted through the use of approved GEPF infrastructure.
- Remote network access must use multifactor authentication where applicable.
- Internet connections originating from GEPF networks must only be made through approved and authorised Internet gateway.
- Connections and communication between GEPF internal and external parties must use trusted network protocols.
- Where authentication is required it must occur before data can be transmitted between trusted and untrusted networks.

9.4 Wireless Network Usage and Access

- The connection of wireless access points, base stations and workstation to the GEPF network must be registered and approved by ICT management. Connection of personal equipment such as notebooks, switches and wireless routers is strictly prohibited.
- A simultaneous connection to the internal network and any wireless network is not allowed.
- Wireless access points shall be configured securely.
- The SSID's assigned to wireless access points should not allow the identification of the organisation i.e. should not include the name GEPF.

9.5 Network and operational security

- A range of network controls is necessary to achieve and maintain security in computer networks. Network controllers shall implement controls to ensure the security of data in networks, and the protection of connected services from unauthorized access.
- Equipment and software shall be maintained and updated in accordance with GEPF's patch management procedure to ensure its continued availability and integrity.
- Periodic vulnerability scans shall be performed on the network.
- Appropriate action shall be taken to ensure that the risks relating to identified vulnerabilities are mitigated in a timely manner.
- A primary firewall is implemented to segregate GEPF's network from the public network (internet) and is used to control both incoming and outgoing electronic communications. The following key characteristics must be considered when working with firewalls:
 - Changes to the firewalls must follow a formal change management process;

- The least privilege principle must be applied to all firewall rules;
- Firewall rules should not allow direct connections with untrusted sites;
- The use of any source, any destination and any port should not be allowed;
- Firewall rules should contain detailed comments explaining the purpose of the rule;
- Network traffic must be controlled in all directions and no bi-directional access should be granted in a single rule;
- The firewall rule base must be reviewed on a periodic basis and the rule base must be approved by management;
- The DMZ should be treated as an external party;
- Anti-Spoofing must be enabled on the firewall;
- A stealth and clean-up rule must be created on the firewall;
- The firewall rule base and configuration must be backed up on a periodic basis to ensure that the firewall can be restored in the event of a disaster;
- Insecure protocols such as file transfer protocol (ftp) and telnet should not be allowed through the firewall;
- Intrusion detection (IDS) and prevention system (IPS) shall be installed to provide real-time monitoring of network activity as well as to proactively prevent unauthorised entry and/or malicious network activity.
- The audit logs and alerts on firewall and IPS/IDS devices shall be reviewed on a periodic basis and all issues identified shall be investigated, recorded and tracked.
- Penetration testing shall be performed at least once a year.
- Only GEPF approved IT security tools, service and hardware may be implemented on the network and information management systems.
- The operational and acceptance requirements of new systems and/or system upgrades must be investigated, documented and tested before implementation into the production network/environment.
- Management shall review compliance to information processing and security policies, standards and procedures within their area of responsibility on a periodic basis.
- Personal firewall on workstation, servers and laptops shall be disabled.

9.6 E-mail usage

E-mail systems shall be used for official and limited personal purpose. Refer to the Email and Internet Policy.

9.7 Internet usage

Internet facilities shall be used for official purposes. Refer to the Email and Internet Policy.

9.8 Use of cloud storage services

- The GEPF has adopted a hybrid or mixed strategy or approach to the use of cloud storage facilities as follows:
 - Under no circumstance shall any of GEPF's classified or confidential and sensitive information be stored within a public cloud storage facility that is outside South African borders (such as iCloud, Dropbox, Google drive etc.) unless approved by management.
 - Only approved service providers whose cloud facilities are located within the South African borders will be used to process and store GEPF information. Such cloud service providers may be requested to undergo information security assessment or audits on a periodic basis to ensure that their facilities satisfy the GEPF's information security requirements.
 - Where there are reasonable grounds to believe that there is a security compromise or that the GEPF information has been accessed or acquired by unauthorised person the service provider must notify the GEPF management immediately.

9.9 Software usage and asset management

- A software inventory must be created, maintained and reviewed by management on a periodic basis.
- Software may only be installed by authorised parties such as by an ICT support representative.
- Software removal and disposal should only be carried out by an authorised individual and in accordance with the End User Licence Agreements (EULA's) or regional legislation.
- Licence keys, original software installation disks and invoices must be stored in a fireproof safe management by ICT.
- Users are prohibited from installing any of the following on GEPF's systems unless approved by management.
- Games and/or entertainment related software such as video codex on any of GEPF's systems.

9.10 Removable media management

- All mission critical and confidential information stored on portable storage devices and removable media must be encrypted and/or protected by a strong password.
- It is the responsibility of GEPF employees to ensure that information stored on removable media such as USB devices and external hard-drives is protected against unauthorised access and misuse.
- All information collected on portable storage devices and removable media must be backed up to GEPF's central file server as soon as practically possible.

9.11 Physical and environmental security

- Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) must be used to protect areas that contain information and information processing facilities against unauthorised access.
- The security of the perimeter shall be clearly defined and consistent with the value of the information asset or service under protection.
- Physical barriers shall be extended from floor to ceiling to prevent unauthorised entry and environmental contamination.
- All fire doors on a security perimeter shall be fitted with an alarm and shall have an automated shutting device.
- Access to the GEPF premises and data centre must be granted by an authorised GEPF staff member in line with the GEPF access and physical security policy.
- Physical protection against damage from natural disasters, malicious attack or accidents, such as fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster must be designed and applied in accordance with the GEPF access and physical security policy.
- Environmental conditions shall be monitored for conditions that could adversely affect the operation of information processing facilities.
- All lost or stolen security access cards shall be reported to Facilities management within twelve hours after being lost or stolen. The Information Security Manager must be informed for security purposes.
- Access logs must be maintained and monitored to detect unauthorised entry to the data centre.
- Information security events and breaches shall be reported through appropriate management channels as quickly as possible to the ICT Service Desk.
- Evidence of an information security event, where appropriate, and breaches shall be obtained and secured in accordance with Human Resources and legal policies and procedures.
- Information security events and breaches shall be categorised and prioritised based on an assessment of the risk to GEPF.
- GEPF shall define information security incident and breach response procedures to co-ordinate the response effort and designate roles and responsibilities for breach response.
- Actions undertaken in responding to an information security event or breach shall be recorded, tracked, and reviewed throughout the course of resolution and within a reasonable period thereafter to identify lessons learned and opportunities for improvement.

- Information security event or breach response procedures must be tested on an annual basis to ensure the effectiveness of the plan and ensure that all stakeholders are aware of their role in the breach response effort.
- Where there is a breach of personal information, the GEPF management must be notified and the breach must be addressed in accordance with GEPF's policies.

9.12 Malicious activities and codes

All GEPF systems shall have updated anti-virus software installed at all times. End users shall refrain from introducing malicious activities and codes on GEPF systems through the usage of non-approved devices.

Users shall not circumvent or attempt to circumvent officially approved protective measures.

9.13 Environmental Controls

- All mission critical Information systems must be stored in a physically secure location.
- Access to these areas must be restricted only to authorised persons. These areas must
 - automatically or manually, Jog or notify, access made to those locations.
- The GEPF office, utilised for Information systems must offer adequate protection against
 - threats such as power failures, fire, water damage, and vandalism.
- The server rooms shall have a UPS to support orderly shutdown or continuous running is necessary for equipment supporting business-critical operations.
- The server rooms shall also have the following:
 - Temperature regulating mechanisms
 - Smoke detectors and fire suppression mechanisms
 - Raised floors
 - Generators with adequate fuel
 - Access control and logging facilities

9.14 Physical Access to Data Centers

Servers shall be located in locked rooms where physical access control is implemented. Access control shall only be granted to selected administrators requiring physical access. Contractors and consultants requiring access have to request access permission, and be accompanied by an authorized administrator at all times in the server rooms.

All servers and network equipment shall be housed in locked cabinets of which the keys shall be kept by the Corporate Services.

9.15 Backup and disaster recovery

All key GEPF information and data shall be backed up regularly, i.e. daily. Such information includes emails, network information; spreadsheets used for business purposes and systems that process business information.

- It is the responsibility of GEPF personnel to ensure that all corporate information is backed up on a regular basis to limit the risk of information loss and rework.
- GEPF's ICT department or its agents shall perform software, application data backups in line with a business impact analysis.
- A business impact analysis shall be performed periodically or following significant changes to GEPF operations, software, applications, data centres, or other facilities that impact the processing of GEPF's information assets.
- Backup media shall be stored off-site.
- Appropriate collection of backup media and retrieval procedures (including authorisation) shall be in place to protect the movement of 'removable tape backup media' in transit between the primary site, offsite tape vault and disaster recovery site.
- Backups shall be tested on a periodic basis to ensure that back up media is recoverable in the event of a disaster.
- A disaster recovery plan must be established and tested at least annually to provide assurance that business can recover in case of a disaster.
- The same level of security applied to GEPF's primary site and information processing assets shall be applied to disaster recovery sites and equipment hosted at the disaster recovery sites

9.16 Cabling Security

Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.

9.17 Equipment Maintenance

Equipment shall at all times be correctly maintained to ensure continued availability and integrity, compliance with warranty provisions and protection of the GEPF's information assets.

9.18 Intrusion Prevention System

Intrusion Prevention Systems (IPS) shall be deployed to prevent and alert on potential unauthorised access. The IPS shall be configured to monitor the entire network for suspicious traffic through the analysing of all protocol activities to identify threats that generate unusual traffic flows, denial of service attacks, malware, and policy violations. A similar system shall be used to monitor wireless network traffic. The IPS will generate reports on any such incidents

in the network for further investigation by the Information Security team. by the GEPF ICT Steercom. Personal firewall on workstation, servers and laptops shall be disabled.

10. Business Continuity Management

GEPF shall enforce a business continuity environment, which will ensure and secure the availability of all its Information Assets in the event of major failures or disasters according to the Business Continuity Management Policy.

11. Human Resource employment and engagement

- Background verification checks on all candidates for employment shall be carried out in accordance with the relevant Human Resources policies and procedures, laws and regulations.
- No private, contractor and/or 3rd party devices will be connected to the GEPF network unless the connection of devices has been authorised

Change management

requirements of this policy.

New Information systems or changes thereto must be put through an established acceptance criterion prior to their implementation in the production environment.

13. Non-compliance and corrective action

In the event of non-compliance with, or breach of, any aspect of this policy, disciplinary action will be taken against employees in accordance with the GEPF's disciplinary policy, procedures and Board Charter.

Where there is evidence or reasonable suspicion of a criminal offence having been committed, the matter shall be reported to the appropriate law enforcement agency. The GEPF will co-operate with the police and other appropriate external agencies in the investigation of alleged offences.

14. Roles and responsibility

- PEO is accountable and responsible for:
 - Evaluating, directing and monitoring the GEPF's information security risk posture and policy.

- Alignment of the GEPF's information security risk strategy, as incorporated in the information security framework, with the business strategy.
- The Head of Co-operate services is responsible for:
 - Approving the development, implementation and maintenance of processes, procedures, standards and information security management systems in support of this policy.
 - Ensure compliance to the process, policies, standards, procedures and guidelines
- Manager ICT is responsible for:
 - Defining and implementing the GEPF's information security framework, strategy and roll-out program.
 - Monitoring and reporting on compliance to this policy and supporting procedures and standards
 - Recommending corrective actions to Head of Corporate Services where gaps and non-compliance have been identified
- Employees are responsible for:
 - Complying to the process, policies, standards, procedures and guidelines
 - Reporting and logging security events or incidents with the GEPF ICT service desk

15. Employees on Suspension

Suspended employees shall not connect or attempt to connect or make use of any GEPF devices, systems or equipment as indicated in this document.

16. Policy review

The management will review the policy every three years and/or when significant changes occur, to ensure the suitability, adequacy and effectiveness of the policy. The policy shall be approved and enforced by the management.

17. Approval

RECOMMENDED / NOT RECOMMENDED




MR RN MORRIS

ACTING CHAIRPERSON: FINANCE AND AUDIT COMMITTEE

DATE: 2019-12-03

APPROVED / ~~NOT APPROVED~~

A handwritten signature in black ink, appearing to read "Dr. RD Mokate".

DR RD MOKATE

CHAIRPERSON: BOARD OF TRUSTEES

DATE: 2019-12-03