Confidential

Remote Access Policy

Effective Date: _____

Policy Owner: Corporate Services

Document Classification:

Confidential

Confidential

Table of Contents

Document Versions

Version	Revision Date	Prepared / Revised 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	Resources Manager	Draft
V4.0	10 May 2016	Musa Mabesa	Finance Manager	Draft
V5.0	13 December 2018	Paul Masipa	ICT Manager	Draft
V6.0	31August 2020	Paul Masipa	ICT Manager	Draft
V7.0	08/10/2020	Paul Masipa	ICT Manager	Final

Document Reference Library

Document File Name	Context and Relevance
Cybercrimes and Cybersecurity Bill (B6-2017)	The purpose of this bill is to create offences and impose penalties which have a bearing on cybercrime and to criminalise the distribution of data messages which is harmful and to provide for interim protection orders;
Electronic Communication and Transmissions Act (ECT) (25 of 2002)	The ECT prescribes the measures taken to secure information, using secure equipment.
GEPF Information Security Policy	The purpose of this policy is to ensure a secure GEPF IT environment.
ISO / IEC 2700:2005 standard	The ISO 2700:2005 is a set of International standards that concentrates on the establishment of information security through the implementation of a suitable set of controls, including policies, process, procedures, structures and functions.
Minimum Information Security Standards (MISS)	A minimum information security standard policy approved by Cabinet on 04 December 1996.
Protection of Information Act (84 of 1982)	To provide for the protection from disclosure of certain information, and to provide for matters connected therewith
Protection of Personal Information Act, 2013 (Act No. 4 of 2013) (POPIA)	Promotes the protection of personal information by public and private bodies
Regulation of Interception of Communications and Provision of Communication Related Information Act 70 of 2002	Regulates the interception of communications and associated processes such as applications for and authorisation of interception of communications.

Business Areas Impacted By This Policy

Name Business Unit / Area	Context and Relevance
All users who are in GEPF employment or who act on behalf of the GEPF.	To guide users on acceptable methods of remotely connecting to the GEPF network.

Glossary of Terminology

Abbreviation/Terminology	Description
3G, LTE	Technology that is used to facilitate the communication connections. This is the medium used to transfer information between the transmitter and receiver.
Cyber crime	Criminal activities that involve the use of electronic hardware like a computer and or a network targeted at a person(s), an organisation, the GEPF's systems or the nation's security.
End-user device	These include but are not limited to, smartphone, notebook computers, tablet personal computers (PCs). IPads, Portable Digital Assistants and other similar devices.
External or public connections	Any connection initiated outside the GEPF network .e.g. connections made from other organisation, home , hotel , coffee shops , shopping centre network etc.
Firewall	Software or a combination of hardware and software, that implements security policy governing traffic between two or more networks or network segments. Used to protect internal networks, servers, and workstations from unauthorized access.
GEPF	Government Employees Pension Fund
GEPF Networks	Mobile sim cards provided by the GEPF, GEPF WIFI and GEPF Local Area Network
Hacking	Unlawful and intentional access to data, a computer program, a computer data storage medium or a computer system,
Information Security Standards	The condition created by the conscious provision and application of document, personnel, physical, computer and communication security measures to protect sensitive/classified or valuable information
Phishing	The fraudulent attempt of to obtain sensitive information in its various forms including but not limited to cyber fraud, cyber forgery and uttering, and cyber extortion.
Sensitive	Information whose access shall be controlled due to proprietary, ethical, or privacy considerations. This classification applies even though there may not be legislation requiring protection.
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, and other parties with valid GEPF access accounts.

Abbreviation/Terminology	Description
User ID	A unique identification number or name or combination of both that will identify a person from others. A user ID is used as part of the log in process.
VPN	Abbreviation for Virtual Private Network. A VPN is a computer network in which some of the links between systems on an open network are carried by closed (private) connections or virtual circuits. A virtual network forms tunnels through a normal and open network.
Phishing	The fraudulent attempt of to obtain sensitive information in its various forms including but not limited to cyber fraud, cyber forgery and uttering, and cyber extortion.

1. Policy purpose

The purpose of this policy is to outline the security requirements for connecting remotely to the GEPF network. It is intended to secure the access of the networks by those accessing it and promote compliance.

2. Policy Statement

This policy describes the security requirements required for remote connections to the GEPF's network. It covers a wide variety of technologies including cellular phone connections, dial-up and 3G/LTE modem links, tablets value-added networks, and Internet value-added networks. Every individual user or organisation making these and other types of automated remote connections to the GEPF internal computers and networks shall follow the rules as set out in this policy. This policy must be read with applicable (Cybercrime) national legislation at the time. The main goals of the policy are:

- To highlight the GEPF's approach in dealing with remote access to its network.
- To define the GEPF's approved uses for remote access regardless of application/service.
- To define the users' responsibility and accountability in their use of remote access
- To preserve the integrity, confidentiality and privacy of the information within the organisation's network utilising the appropriate controls.
- To preserve and support the audit, legal and security concerns.

The paragraphs below highlight some of the user categories and how they are affected by the policy without taking away the holistic applicability of the policy to all users.

2.1 External connections

All users provided with username and password are authorised to connect to the GEPF network.

Remote users shall employ a GEPF approved VPN prior connecting to the GEPF through any other non-GEPF , public or external networks.

Such remote access may be revoked at any time especially when it is posing a risk to the GEPF and not complying to GEPF policies.

2.2 Remote access control

Remote access shall be controlled through secure controls as indicated in Annexure A.
The GEPF users with remote access privileges shall ensure that their GEPF owned or personal end-user devices, that are remotely connected to GEPF corporate network, are not connected to any other network at the same time, except personal networks that are under the complete control of the user.

All hosts that are connected to GEPF networks via remote access technologies shall use up-to-date anti-virus software, this includes personal end-user devices.

2.3 Third-party compliance agreement

All third parties required to remotely access the GEPF internal computers or networks shall sign a compliance and non-disclosure agreement before being issued a user ID. If a certain

third party already has a user ID, a signature shall be obtained before receiving a renewed user ID. A renewal process should take place every four months.

An approved compliance and non-disclosure agreement will indicate that the user understands and agrees to adhere to the GEPF policies and procedures related to computers and networks. The GEPF retains the right to periodically audit third parties or users who have remote access to the GEPF computers and networks to ensure compliance with this and other policies and requirements.

2.4 Third parties connectivity

Before remote access privileges are granted to third parties, they shall agree in writing that all accounts will be named as per the GEPF standards and that there will be no general use or shared accounts:

- For continuing remote access privileges, access shall be re-approved quarterly by the contractor's project manager and the owner of the system being accessed.
- Remote access privileges shall be terminated when there is a contract termination.
- All third party accounts shall be deactivated until GEPF receives a request to activate the account. When the third parties' work is completed, the account shall be removed .

2.5 User access

User IDs and passwords are used to establish individual accountability within the GEPF network. Users are not to divulge or share their passwords and user id for any reason. Any activity performed by a particular User ID will be the full responsibility of the assigned user.

All remote computer equipment and end-user devices used for business interests, whether personal- or company-owned, shall display reasonable physical security measures. End-user devices will have installed appropriate antivirus software deemed necessary by the Corporate Services.

2.6 Wireless internet access - remote access (hotspot users)

Remote users using public hotspots for wireless internet access shall employ a GEPF-approved personal firewall, VPN, and any other security measure deemed necessary by the Corporate Services.
Hotspot and remote users shall disconnect wireless module when not in use to mitigate attacks by hackers or eavesdroppers.

Users shall change their passwords promptly if they suspect that their password has been compromised especially while being used over external remote connections.

Any remote connection that is configured to access GEPF resources shall adhere to the authentication requirements of Corporate Services. Also, all hardware security configurations (personal or company-owned) shall be approved by Corporate Services.

2.7 Modification of remote access

User will make no modifications to the remote access connection without the approval of Corporate Services. This includes, but is not limited to, split tunnelling, dual-homing, non-standard hardware or security configurations, etc.

If a personally- or company-owned end-user device or related equipment used for remote access is damaged, lost, or stolen, the authorised user will be responsible for notifying their line manager and the designated person within Corporate Services immediately. The user shall report the stolen equipment to the South African Police services and obtain a case number.

2.8 Remote access to information

Information systems that contain organisation, personnel and financial data will be available for off-site remote access through a centrally managed VPN that provides encryption and secure authentication. Access may be revoked at any time for reasons including non-compliance with security policies. Remote access privileges for GEPF information will be reviewed upon a user's change of departments.

2.9 Endpoint security

The external end-user devices that are used to administer the GEPF resources or access sensitive information shall be secured. This includes patching (operating systems and applications), possessing updated anti-virus software, operating a firewall and being configured in accordance with all relevant GEPF policies/procedures.

2.10 User responsibilities, awareness & training

The GEPF will ensure that all users of information systems, applications and the networks are provided with the necessary security guidance, applicable Cybercrimes laws and regulations awareness and where appropriate training to enable them to discharge their risk management responsibilities.

Protection of the information within the GEPF's network is the responsibility of all users and ICT personnel. The user is accountable for the appropriate use and dissemination of the information obtained through remote access communications (sessions).

3. Related Policies

- Information Security Policy
- End-user device Policy
- Email and Internet Policy
- Password& user access Policy

4. Non-compliance with this Policy

Non-compliance with this Policy described in it by any user will be dealt with in accordance with Chapter 7 of the Board Charter and GEPF's disciplinary policy.

5. Acceptance of this Policy

As part of the user induction and ongoing compliance, each user shall be required to review a copy of this Policy and to acknowledge in writing that he/she has reviewed the Policy, understands the content and agrees to be bound by it.

6. Policy Review and Evaluation

This Policy will be reviewed every three-years or as and when necessary provided that such a required review will be within 6-months after the new legislation has been implemented.

The Finance and Audit Committee is responsible for implementing, updating and reviewing this Policy.

Any changes to the Policy shall be communicated immediately to all Trustees.

7. Interpretation

In the event of any inconsistency between this Policy and the Rules of the Fund, the Rules shall prevail.

8. Policy Approval

MR STADI MNGOMEZULU
CHAIRPERSON: FINANCE AND AUDIT COMMITTEE
DATE:

Approved / Not Approved

DR RENOSI MOKATE
CHAIRPERSON: BOARD OF TRUSTEES
DATE:

---

9. Annexure A

Configuration

- Devices shall be configured and maintained in accordance with GEPF security standards including up-to-date anti-virus and operating system patch management.
- Remote connections shall be terminated after three (3) repeated unsuccessful attempts to establish a connection.
- Users shall not use permanent or semi-permanent established VPN connections and shall not use pings or other artificial network processes to keep the connection open.
- Passwords may not be stored, in any form, on the local machine.
- All sensitive data stored on the remote machine shall be encrypted using a corporate-approved encryption tool.
- All remote access connections shall include a “time-out” system. In accordance with GEPF’s security policies, remote access sessions will time out after 180 minutes of inactivity and will terminate after unlimited hours of continuous connection. Both timeouts will require the user to reconnect and re-authenticate to re-enter company networks.