DUE CARE AGREEMENT

Agreement in respect of use of end user devices and information

Entered into between

The Government Employees Pension Fund (GEPF)

and

Full name and surname, hereinafter referred to as "the employee":

_____

_____

Employee no.: _____

Full physical address:

_____

_____

_____

_____

The parties choose the above addresses as their *domicilium citandi et executandi*

1. PURPOSE

1.1 The purpose of this agreement is to outline the acceptable standard for end user devices and data at the GEPF. This agreement is intended to protect the employee and the GEPF. Inappropriate end user devices and information may expose the GEPF to various risks, including malicious attacks, compromise of network systems and services.

1.2 In general, acceptable use means respecting the rights of other end user device users, the integrity of the physical facilities and all pertinent licence and contractual agreements to protect the organisation from reputational damage, loss of intellectual property, etc.

1.3 This agreement applies to the use of data, electronic and computing devices, and network resources to conduct GEPF business or interact with internal networks and business systems, whether owned or leased by the GEPF, the trustees , substitute trustees, contractors , agents employee or a third party.

2. DEFINITIONS

2.1 'End user devices' means any electronic, computing and mobile device

2.2 'EUD' means end user device

2.3 'Data' means electronic or non-electronic information, including a client's personal information.

2.4 'Media file' means any audio, video or image file.

3. BASIS OF AGREEMENT

The GEPF undertakes to make available the below EUD(s) with serial number(s) and GEPF barcode number(s) ("the EUD") for the sole use by the employee for the duration of this agreement.

3.1.1 Serial No.:_____ GEPF Barcode:_____

3.1.2 *Serial No.:_____ GEPF Barcode:_____*

3.1.3 *Serial No.:_____ GEPF Barcode:_____*

3.1.4 *Serial No.:_____ GEPF Barcode:_____*

3.2 All employees are responsible for familiarising themselves with the policies of the organisation that apply to appropriate use of the information and communication technologies and resources.

3.3 All employees, contractors and consultants of the GEPF are responsible for exercising due care regarding appropriate use of information, end user devices and network resources in accordance with the GEPF's policies and procedures, standards and legislation.

3.4 The employee must take possession of the EUD as soon as the employee signs this agreement and shall be responsible for the due care of the EUD for the duration of this agreement.

4. EMPLOYEE OBLIGATIONS IN RESPECT END USER DEVICE

4.1 The employee undertakes–

4.1.1 to use the allocated end user device with the utmost due care.

4.1.2 to keep the end user device secured at all times at the employee's workstation by means of the allocated security lock cable attached to an immovable object. Easily movable objects do not qualify for purposes of this agreement.

4.1.3 to ascertain whether his/her specific workstation allows for the suitable locking of his/her end user device, as contemplated in item 4.1.2 above.

4.1.4 in cases where no suitable object is available to which the security lock cable can be secured, to immediately bring this to the attention of the ICT manager, who must then make the necessary arrangements to enable the employee to secure the lock to a suitable immovable object.

4.1.5 to ensure that the end user device is secured at all times and stored in safe location while at home or at the auditee.

4.1.6 to exercise due care when transporting the end user devices(s) to ensure that the necessary security is provided.

4.1.7 to keep the end user device(s) out of sight and to be kept in the locked vehicle boot while in transit.

4.1.8 not to park the vehicle in a poorly lit or remote areas while the end user device is in transit.

4.1.9 to be vigilant and check the vehicle's doors and boot manually after locking, to protect themselves from remote jamming and to keep the end user device out of plain view.

4.1.10 to refrain from eating or drinking next to the end user device to avoid liquid or food spillage that may cause damage to the end user device.

4.1.11 not to use sharp objects on the end user device screen to avoid damage.

4.1.12 not to leave objects on the keyboard before closing the screen of the end user device.

4.1.13 to carry the end user device in the approved bag provided by the employer while in transit.

4.1.14 to exercise good judgement regarding the reasonable personal use of applications, social media, internet/intranet and extranet systems.

4.1.15 to exercise good judgement regarding the reasonable personal use email and communicating activities.

4.1.16 to promptly report the theft, loss or unauthorised disclosure of GEPF information.

4.2 The list of requirements indicated in item 4.1 above is not exhaustive and the employer may from time to time prescribe further due care requirements and/or arrangements based on the specific operational requirements to further safeguard the end user device.

4.3 GEPF-owned information and technology resources may not be used to engage in any activity that is in contravention of GEPF policies and illegal under national or international law.

4.4 The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use:

4.4.1 Disclosing your account password to others or allowing use of your account by others.

4.4.2 Using the GEPF end user device to actively engage in procuring or transmitting material that is in violation of legislation.

4.4.3 Making fraudulent offers of products, items or services originating from any GEPF account or end user device equipment.

4.4.4 Making statements about warranty, expressly or implied, unless it is a part of normal duties.

4.4.5 Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorised to access, unless these activities are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

4.4.6 Approval must be obtained from the chief information officer for any security scanning on the network.

4.4.7 Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

4.4.8 Circumventing user authentication or security of any host, network or account.

4.4.9 Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

4.4.10 Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the internet/intranet/extranet.

4.4.11 Providing data about, or lists of, GEPF employees or auditees to parties outside the GEPF.

5. DAMAGE TO THE END USER DEVICE

5.1 In the event that the end user device is damaged for whatever reason, the line manager must conduct a proper investigation to determine the nature and cause of such damage.

5.2 In cases where the end user device is stolen or lost, the employee must report the theft or loss to the South African Police Service (SAPS) within 48 hours and obtain the case number.

5.3 The employee must send the damaged end user device to the ICT business unit to assess the extent of the damage. Upon completion of the assessment, the end user device damage assessment report, with recommendations, will be submitted to the employee's line manager.

6. SOFTWARE

6.1 The employee may not load any unauthorised software or files of whatsoever nature onto the end user device.

6.2 The employee must report any virus infections, malicious codes or any abnormal activities to the ICT service desk.

6.3 The employee may not violate the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the GEPF.

6.4 Unauthorised copying of copyrighted material, including, but not limited to, digitisation and distribution of media or other copyrighted sources, and the installation of any copyrighted software for which GEPF or the end user does not have an active licence shall be strictly prohibited.

6.5 Exporting of software, technical information, encryption software or technology, in violation of international or regional export control laws, is prohibited. The appropriate level of approval must be obtained prior to exporting any material that is in question.

6.6 Introduction of malicious programs or technologies onto the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) is prohibited.

7. INTERNET, INTRANET, SOCIAL MEDIA AND EXTRANET SYSTEMS

7.1 Employees are responsible for exercising good judgement regarding the reasonable personal use of the internet, intranet, social media and extranet systems.

7.2 When using GEPF resources to access and use the internet, users must realise that they represent the GEPF.

7.3 Whenever employees acknowledge an affiliation to the GEPF, they must also clearly indicate that the opinions expressed are their own and not necessarily those of the GEPF.

8. EMAIL AND COMMUNICATION ACTIVITIES

8.1 Employees are responsible for exercising good judgement regarding the reasonable personal use email and communication activities.

8.2 Sending unsolicited email messages, including "junk mail" or other advertising material to individuals who had not specifically requested such material (email spam) is prohibited.

8.3 Any form of harassment via email, telephone or instant messages, whether through language, frequency or size of messages, is prohibited.

8.4 Unauthorised use or forging of email header information is prohibited.

8.5 Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to solicit replies is prohibited.

8.6 Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type is prohibited.

8.7 Use of unsolicited email originating from within GEPF's networks of other internet/intranet/extranet service providers on behalf of the GEPF, or to advertise any service hosted by the GEPF or connected via GEPF's network, is prohibited.

8.8 Posting the same or similar non-business-related messages to large numbers of recipients is prohibited.

8.9 Employees must use caution when opening email attachments or links received from unknown senders which may contain malicious software.

8.10 The employee must lock the end user device screen or log off when the end user device is unattended.

9. DATA

9.1 All data belonging to the GEPF or created by the employee or anyone else for the benefit of the GEPF must be:

9.1.1 backed up and then removed from the end user device when the end user device is returned at the end of this agreement or is due for replacement

9.1.2 The information and documentation remain the property of the GEPF.

9.1.3 The employee is not authorised to take any electronic or physical information from the GEPF.

9.1.4 The employee has a responsibility to promptly report the theft, loss or unauthorised disclosure of GEPF information.

9.1.5 The employee may access, use or share GEPF information only to the extent that it is authorised and necessary to fulfil their assigned duties.

9.1.6 The employee must not store non-official media files on the GEPF Shared storage location.

10. MONITORING

10.1 For security and network maintenance purposes, authorised individuals within the GEPF may monitor equipment, systems and network traffic at any time as per the information security policy.

10.2 The GEPF reserves the right to audit end user devices, resources, networks and systems on a periodic basis to ensure compliance with GEPF policies and this agreement.

11. INCIDENT LOGGING

11.1 Employees must log a call to report any suspicious activities, anomalies or breaches experienced on the end user device devices to the ICT service desk 071 632 2708 michael.komane@gepf.co.za.

12. LIABILITY OF THE EMPLOYEE

12.1 The employee shall be personally liable for the replacement monetary value of damages caused to the end user device in accordance with this agreement if such liability is determined by following a fair procedure and the employee shall be given a chance to state his/her case and show why the liability determination should not be made.

13. THE GEPF's OBLIGATIONS IN RESPECT OF THE END USER DEVICE

13.1 The GEPF is responsible for the servicing and maintenance of the end user device under this agreement.

14. GENERAL

14.1 The employee must use the GEPF resources (end user device, information, software, internet, intranet, extranet and email) for official purposes and limited personal use.

14.2 No variation, amendment or relaxation of any clause(s) contained in this agreement shall be valid unless reduced to writing and agreed to by both parties.

14.3 Subject to any contrary provision in this agreement, all notices in terms of this agreement must be delivered by hand, sent by certified mail, faxed or emailed and must be addressed as stated at the beginning of this agreement, which addresses the parties hereto choose as *domicilium citandi et executandi.*

Signed at _____ on this _____ day of _____

Employee: _____

Signed at _____ on this _____ day of _____ for and on behalf of the GEPF:

In the presence of the undersigned witness:

Witness: _____

Name: _____

Contact no: _____