Ghana Infrastructure Investment Fund
Information Systems Policy

As approved by the Board of Directors on 25th July 2024

CONTENTS

1.0 INTRODUCTION 6

3.1 Purpose 7
3.2 Roles and Responsibilities for Information Security 8
3.2.2 Board and Senior Management Oversight 8
3.2.3 IT Security Officer (ISO) 9
3.2.4 Internal Audit Role 10
3.3 Ownership and Responsibility of IT Resources 11

4. NETWORK ACCESS & AUTHENTICATION 11

4.1 OVERVIEW 11

4.2 PURPOSE 11

4.3 SCOPE 12

4.4 ACCOUNT SETUP 12

4.5 ACCOUNT USE 12

4.6 ACCOUNT TERMINATION 13

4.7 SCREEN-SAVER PASSWORDS 13

4.8 MINIMUM CONFIGURATION FOR ACCESS 13

4.9 NON-BUSINESS HOURS 14

4.10 NETWORK ACCESS 14

4.11 UNACCEPTABLE USE 14

4.12 BLOGGING AND SOCIAL NETWORKING 15

5. EMAIL POLICY 16

5.1 EMAIL USE 16

5.2 General Restrictions 16
5.3 Prohibited Material 16
5.4 Disguise of Identity 17
5.5 Altering Indication of Origin 17

5.6 CONFIDENTIALITY 17

5.7 TRANSMISSION OF CONFIDENTIAL MATERIAL 17

5.8 EMAIL ACCOUNTS 18

5.9 MIS-ADDRESSED E-MAIL 18

5.10 UNAUTHORIZED ACCESS 18

5.11 MONITORING & DISCLOSURE OF INFORMATION 19

5.12 Monitoring, Access to and Disclosure of GIIF Information 19

5.13 DISCLAIMER 21

6. INTRANET AND INTERNET SECURITY POLICY 22
6.1 GENERAL INTERNET POLICY 22
6.2 BROWSING POLICY 22
6.3 INTERNET RESPONSIBLE USE POLICY 23
6.4 PROHIBITED USAGE 24
6.5 WEB BROWSING 24
6.6 INTERNET PERSONAL USE 25
6.7 REMOTE DESKTOP ACCESS 25
6.8 CIRCUMVENTION OF SECURITY 25
6.9 NON-GIIF OWNED EQUIPMENT 25
6.10 SOFTWARE INSTALLATION 25
6.11 REPORTING OF SECURITY INCIDENTS 26
7. CONFIDENTIAL DATA 26
7.1 OVERVIEW 26
7.2 STORAGE 26
7.3 USE OF CONFIDENTIAL DATA 27
7.4 DATA STORAGE 27
8. INCIDENCE RESPONSE MANAGEMENT POLICY 28
8.1 PURPOSE 28
8.2 DEFINITION OF INCIDENT AND TYPE OF INCIDENTS 28
8.3 SEVERITY 29
8.4 ELECTRONIC INCIDENTS 29
8.5 INCIDENT CATEGORISATION, PRIORITISATION AND ESCALATION 30
8.5.1 CATEGORISATION 30
9. DATA BACKUP AND RETENTION 32
9.1 OVERVIEW AND POLICY STATEMENT 32
9.2 SCOPE 32
9.3 IDENTIFICATION OF CRITICAL DATA 32
9.4 DATA TO BE BACKED UP 33
9.5 OFF SITE ROTATION 33
9.6 BACKUP STORAGE 33
9.7 BACKUP RETENTION 34

9.8 RESTORATION PROCEDURES & DOCUMENTATION 34
9.9 BACKUP CONTROL, AND REVIEW 34
10. ANTIVIRUS/ANTI-MALWARE POLICY 35
10.1 VIRUS PROTECTION 35
10.2 INFORMATION RESOURCES AND TECHNOLOGY RESPONSIBILITIES 36
10.3 ADVICE AND ASSISTANCE 37
10.4 PROCEDURE FOR DEALING WITH INFECTED COMPUTERS 37
11. SOFTWARE SECURITY POLICY 37
11.1 INTERNAL CONTROLS 38
12. PASSWORD POLICY 38
12.1 OVERVIEW 38
12.2 PURPOSE 39
12.3 SCOPE 39
12.4 POLICY STATEMENT 39
12.5 PASSWORD CONSTRUCTION 39
12.6 CONFIDENTIALITY 40
12.7 CHANGE FREQUENCY 40
12.8 PASSWORD GUIDELINES 41
13. PHYSICAL SECURITY POLICY 42
13.1 OVERVIEW 42
13.2 PURPOSE 42
13.3 SCOPE 42
13.4 CONTROLLED ACCESS AREAS 42
13.5 PHYSICAL DATA SECURITY 43
13.6 FIRE PREVENTION 43
13.7 ENTRY SECURITY 44
13.8 SIGN-IN REQUIREMENTS 44
13.9 VISITOR ACCESS 44
14. VULNERABILITY MANAGEMENT 45
15. REVIEW 48
16. DEFINITIONS 48
17. APPENDIX 54

EMPLOYEE CONFIRMATION AND ACCEPTANCE 54

1.0 INTRODUCTION

This policy explains how corporate information technology resources are to be used and specifies what actions are prohibited.

While this policy aims to be comprehensive, it may not cover every situation. Therefore, users are expected to exercise a duty of care when using company resources. Questions on what constitutes acceptable use should be directed to the user's supervisor. Information and information system resources are essential assets of GHANA INFRASTRUCTURE INVESTMENT FUND (GIIF).

GHANA INFRASTRUCTURE INVESTMENT FUND Users (Directors, Senior Managers, Middle Managers, and staff) are responsible for ensuring that computing and communication facilities are used in an effective, efficient, ethical, and lawful manner.
This Information Security Policy is provided to all members of GIIF to provide proper guidelines on everyone's responsibility to protect the GIIFs information asset. Every individual should understand their obligations relating to the policy statements described herein.

GHANA INFRASTRUCTURE INVESTMENT FUND staff responsible for planning, acquisition, configuration, deployment, and management and auditing of information systems should apply sound risk management practices when selecting security controls. This would include identifying what information is intended to be protected, what are the threats to that information or information system resource and what are the proper cost-effective safeguards that need to be applied to adequately protect the information.

This document records the Information Technology Department's policies with regards to the use of GHANA INFRASTRUCTURE INVESTMENT FUND computing resources – hardware, software, electronic mail, and Internet.
All policies and procedures described herein apply to all employees of the GIIF with or without access to computer systems.

a. Employees will be required to sign a copy of this document to acknowledge acceptance and agreement to the terms and conditions presented in this document.
b. Every component of the GIIF's computer systems, owned, leased, rented, or borrowed by the GIIF, remains the exclusive property of the GIIF, and is provided for use by the employee at the GIIF's expense.
c. The GIIF's computer systems are extremely important and valuable; as such, any abuse thereof will result in disciplinary action in accordance with the GIIF's disciplinary procedures.
d. It is every employee's duty to use the GIIF's computer systems responsibly, professionally, ethically, and lawfully with reference to the GIIFs' Policy
e. The GIIF's computer systems are provided primarily to assist Employees in the performance of their job function for and on behalf of the GIIF. Certain limited personal use is at the absolute discretion of the GIIF, and no Employee may claim such personal use as of right.
f. Designated personnel may, under certain circumstances, access and review all materials that the Employee has created, stored, sent, or received on the GIIF's computer system, whether through the Internet, e-mail or otherwise. In addition, the GIIF may from time-to-time use human or automated means to monitor the use of its computer resources.

1.1 Purpose

Since inappropriate use of corporate information systems exposes GHANA INFRASTRUCTURE INVESTMENT FUND to risk, it is important to specify exactly what is permitted and what is prohibited. The purpose of this policy is to detail the acceptable use of corporate information technology resources for the protection of all parties involved.

This policy provides a set of comprehensive security guidelines to ensure that GHANA INFRASTRUCTURE FUND's information and information system resources are properly

and consistently protected. This Policy outlines all staff responsibilities in supporting the GIIF security program and compliance with this security policy.

The objectives of this policy are to:

i. Provide for uninterrupted IT services to the GIIF staff and clients.
ii. Safeguard the Confidentiality, Integrity, and Availability of the GIIF's data network through appropriate controls.
iii. Protect the computing and communication assets of the GIIF including data, software, and hardware.
iv. Reduce the likelihood that computers within the GIIF are used to attack other organizations, bringing liability and disrepute to the GIIF.
v. Protect GIIF against the loss or misuse of any information.
vi. Define responsibility and accountability to maintain protection of GIIF 's information.
vii. Preserve and support audit and legal compliance.

1.2 Roles and Responsibilities for Information Security

1.2.2 Board and Senior Management Oversight

The Board of Directors of GHANA INFRASTRUCTURE INVESTMENT FUND is responsible for complying with the regulations and laws that affect the GIIF and should achieve this end by developing appropriate policies, procedures, and controls.

The Board of Directors of GIIF shall approve the Information Security Policies and Guidelines manual and procedures after review.

The responsibility and accountability of the Board and senior management is a basic tenet of sound practices and good corporate governance.

The Board of directors and senior management are fully responsible and accountable for managing technology risks, which are becoming increasingly complex, dynamic, and pervasive.

They are also fully responsible for the implementation of effective internal controls and risk

management practices to achieve robustness, reliability, resiliency and recoverability of IT systems and infrastructures.

The Board and senior management should review and appraise the cost-benefit issues regarding investment in controls and security measures for computer systems, networks, data centre, operations, and backup facilities. Factors such as reputation, customer confidence, consequential impact and legal implications should be evaluated, in addition to cost considerations.

It is the responsibility of the management of GIIF to ensure that all staff members are aware of their responsibilities in relation to Information Security policies, procedures, and controls.

1.2.3 IT Security Officer (ISO)

The mission of the Information System Security function is to safeguard the GIIFs' information assets by directing and supporting the GIIF in the protection of its information resources from disclosure, Modification, destruction, usage, or transfer, whether intentional or unintentional, through the implementation of appropriate information security policies, standards, procedures, and guidelines. This corporate function reports to the IT Manager or anyone acting in that position. The ISO has primary responsibility for the oversight of the state of information security at the GIIF. Primary responsibilities include:

i. The IT Security Officer should ensure that the Information Security Policies and Guidelines is regularly reviewed and updated (at least annually) to reflect new or amended issues, processes, or systems across GIIF's network.

ii. In addition, he/she is responsible for handling and escalating all breaches of information/IT security related to management, and will, when appropriate, investigate (and possibly report and escalate incidents) within the confines of the appropriate regulatory and legal framework in which the incident occurs.

iii. Periodic reporting on the state of information security to Senior Management.

iv. Oversight and implementation of security audit efforts accomplished through the IT Audit/Security Coordinator(s).

v. Recommend and maintain internal security policies and procedures that provide for the security of information technology facilities, software, equipment, and the integrity of the GIIF 's automated information.

vi. Recommend security system software and develop administration procedures to support implementation of Security features.

vii. Identify vulnerabilities that may cause inappropriate or accidental access, destruction, or disclosure of information, and recommend security controls necessary to eliminate or minimize their potential effects.

viii. Co-ordinate with technical managers on matters related to the planning, development, testing, implementation, or modification of information security policies and procedures that will affect the GIIF network.

ix. Maintain Security and confidentiality over issuance and proper maintenance of authorized user Id's and passwords and to maintain valid and current user lists.

x. Reviewing access rights and logs periodically and suggesting preventive actions as required

1.2.4 Internal Audit Role

An audit of the Information Security controls must be conducted periodically. With respect to Information System Security, the objective of Internal Audit is to report on the adequacy of controls and protection of the GIIF's information assets. Internal Audit will review compliance with these policies.

Responsibilities will Include:

i. Examination of the GIIF's information security policies and procedures to provide an independent and objective appraisal of controls for the protection of information assets to the Management.

ii. Review and evaluation of the effectiveness of controls for automated information systems that are either under development or operational, with particular emphasis on major systems.

iii. Ascertaining the extent of compliance with policies, standards, and procedures by the GIIF and its partners.

1.3 Ownership and Responsibility of IT Resources

i. The IT department will assume full ownership and responsibility of all Information Technology resources.
ii. All computing components on the GIIF internal network must be connected by the IT Department.
iii. The IT department shall maintain a list of restricted applications and databases and their corresponding business owners. Authorization for access to restricted business applications and databases must be granted by the designated business owner. An electronic mail message or completion of access forms, where possible, from the business owner granting authorization for appropriate access shall constitute such authorization.
iv. IP addresses assigned to GIIF devices either automatically or must be assigned by an authorized representative of IT Department.
v. Only the IT Department must move or (re-)install devices on the GIIF's internal network.

4. NETWORK ACCESS & AUTHENTICATION

4.1 OVERVIEW

Consistent standards for network access and authentication are critical to GHANA INFRASTRUCTURE INVESTMENT FUND's information security and are often required by regulations or third-party agreements. Any user accessing GIIF's computer systems can affect the security of all users of the network. An appropriate Network Access and Authentication Policy reduces the risk of a security incident by requiring consistent application of authentication and access standards across the network.

4.2 PURPOSE

The purpose of this policy is to describe what steps need to be taken to ensure that users connecting to the GIIF network are authenticated in an appropriate manner, in compliance with the GIIF

standards, and are given the least amount of access required to perform their job function. This policy specifies what constitutes appropriate use of network accounts and authentication standards.

4.3 SCOPE

The scope of this policy includes all users who have access to the GIIF-owned or provided computers or require access to GIIF network and/or systems. This policy applies not only to employees, but also to guests, contractors, and anyone requiring access to the GIIF network. Public access to GIIF's externally reachable systems, such as its corporate website or public web applications, are specifically excluded from this policy.

4.4 ACCOUNT SETUP

During initial account setup, certain checks must be performed to ensure the integrity of the process. The following policies apply to account setup:

i. Positive ID and coordination with Human Resources is required.
ii. Users will be granted least amount of network access required to perform his or her job function.
iii. Users will be granted access only if he or she signed the Acceptable Use Policy.
iv. Access to the network will be granted in accordance with the Acceptable Use Policy.

4.5 ACCOUNT USE

Network accounts must be implemented in a standard fashion and utilized consistently across the organization. The following policies apply to account use:

Accounts must be created using a standard format (i.e., first-name. Last name, etc.)

i. Accounts must be password protected (refer to the Password Policy for more detailed information).
ii. Accounts must be for individuals only. Account sharing and group accounts are not permitted.
iii. User accounts must not be given administrator or 'root' access unless this is necessary to perform his or her job function.

iv. Guests will have a legitimate need for access to the corporate network to browse the internet through the virtual local area network (VLAN-GIIF-Guest). This password will expire after 24 hours of setup

v. Individuals requiring access to confidential data must have an individual, distinct account. This account may be subject to additional monitoring or auditing at the discretion of the IT Manager or an executive team member, or as required by applicable regulations or third-party agreements.

4.6 ACCOUNT TERMINATION

When managing network and user accounts, it is important to stay in communication with the Human Resources department so that when an employee no longer works at GIIF, that employee's data must be backed up for six months and account deleted. Human Resources must notify the IT Manager in the event of a staffing change, which includes employment termination, employment suspension, or a change of job function (promotion, demotion, relieving duties, etc.)

4.7 SCREEN-SAVER PASSWORDS

Screen-saver passwords offer an easy way to strengthen security by removing the opportunity for a malicious user, curious employee, or intruder to access network resources through an idle computer. For this reason, screen-saver password is required to be activated after 5 minutes of inactivity.

4.8 MINIMUM CONFIGURATION FOR ACCESS

Any system connecting to the network can have a serious impact on the security of the entire network. A vulnerability, virus, or other malware may be inadvertently introduced in the network through this process. For this reason, users must strictly adhere to corporate standards about antivirus software and patch levels on their machines. Users must not be permitted network access if these standards are not met. This policy will be enforced with products that provide network admission control.

4.9 NON-BUSINESS HOURS

While some security can be gained by removing account access capabilities during non-business hours, GIIF does not mandate time-of-day lockouts. This may be either to encourage working remotely, or because GIIF's business requires all-hours access.

4.10 NETWORK ACCESS

The user should take reasonable efforts to avoid accessing network data, files, and information that are not related to his or her job function. Existence of access capabilities does not imply permission to use this access.

4.11 UNACCEPTABLE USE

The following actions shall constitute unacceptable use of the corporate network. This list is not exhaustive but is included to provide a frame of reference for types of activities that are deemed unacceptable. The user may not use the corporate network and/or systems to:

i. Engage in activity that is illegal under local, state, or international law.
ii. Engage in any activities that may cause embarrassment, loss of reputation, or other harm to GIIF.
iii. Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, annoying, insulting, threatening, obscene or otherwise inappropriate messages or media.
iv. Engage in activities that cause an invasion of privacy.
v. Engage in activities that cause disruption to the workplace environment or create a hostile workplace.
vi. Make fraudulent offers for products or services.
vii. Perform any of the following: port scanning, security scanning, network sniffing, keystroke logging, or other IT information gathering techniques when not part of employee's job function.
viii. Install or distribute unlicensed or 'pirated' software.
ix. Reveal personal or network passwords to others, including family, friends, or other members of the household when working from home or remote locations.

4.12 BLOGGING AND SOCIAL NETWORKING

Blogging and social networking by GIIF's employees are subject to the terms of this policy, whether performed from the corporate network or from personal systems. Blogging and social networking is never allowed from the corporate computer network. The user must not identify himself or herself as an employee of GIIF in a blog or on a social networking site. The user assumes all risks associated with blogging and/or social networking.

5. EMAIL POLICY

The Electronic Messaging (E-mail) service is among the standard, centralized information technology services provided to staff by the GIIF to conduct official business. Reasonable limits for access and parameters of use are set and enforced to safeguard the functionality and integrity of the GIIF's E-mail system. The IT Department will ensure a reliable E-mail environment with high availability and sufficient storage to support the GIIF's business needs.

5.1 EMAIL USE

Employees may not make excessive use of the e-mail system to send or receive messages of a personal nature. Personal usage of GIIF email systems is permitted if:

i. Such usage does not negatively impact the corporate computer network,
ii. Such usage does not negatively impact the user's job performance.
iii. All staff ***shall not*** use their personal/private email addresses for official communications

5.2 General Restrictions

The e-mail system may not be use:

i. To initiate or forward any chain-message or other message which asks the recipient to forward such message to multiple other employees unless required for work purposes.
ii. To send commercials or messages of a profane, fear-inducing, or contradictory message to the GIIF's mission and values.
iii. To send messages that have the potential to upset other people.
iv. Dissemination or storage of personal advertisements, solicitations, promotions, destructive programs, political material, or any material that is not business-related.

5.3 Prohibited Material

i. Use of GIIF's e-mail facilities to send, download, and display or store prohibited material is strictly prohibited.
ii. No Employee shall knowingly receive or store e-mail or any form of electronic communication containing prohibited material.

iii. If any Employee is uncertain as to whether any material or statement constitutes prohibited material, such Employee must obtain clarification from an immediate Supervisor or appropriate quarters without delay.

iv. E-mail containing prohibited material, which has been inadvertently received, shall be deleted by the Employee receiving such e-mail, immediately that he or she becomes aware of the content thereof. The incident must be reported to the IT Manager or his / her Delegate without delay.

5.4 Disguise of Identity

Employees may not disguise their identity while using GIIF's e-mail system.

5.5 Altering Indication of Origin

Employees may not alter the 'From' line or any other indication of the origin of an e-mail message.

All mailboxes will be disabled immediately an employee had left the Institution. Requests to keep the mailbox active for a period must be authorized by the Chief Executive Officer.

5.6 CONFIDENTIALITY

Confidential data must not be:

i. Shared or disclosed in any manner to non-employees of GIIF,

ii. Shall not be posted on the Internet or any publicly accessible systems, and

iii. Shall not be transferred in any insecure manner.

Please note that this is only a brief overview of how to handle confidential information, and that other policies may refer to the proper use of this information in more detail.

All messages distributed via GIIF's email system are GIIF's property.

5.7 TRANSMISSION OF CONFIDENTIAL MATERIAL

Confidential material shall not be sent, transmitted, or otherwise disseminated by Employees to third parties unless the Employee has satisfied himself/herself:

a. That he/she is duly authorized to send, transmit or otherwise disseminate such material.

b. That it is in the ordinary course of the business of the GIIF or in the GIIF's best interests to send, transmit or otherwise disseminate such material; or
c. That such material is already in the public domain
d. The intended recipient is entitled to receive such information or material.
e. Also, ensures that, all confidential information is Encrypted before sending. The IT department will assist staff in this process.

Confidential material that complies with the requirements of the above may be sent via the GIIF's e-mail system in Adobe PDF format.

Personal information concerning any employee, or any third party as may be kept as part of GIIF's records, shall not be disclosed to anyone without the prior authorization from the employee or third party concerned and the relevant Head / Manager of the Department.

5.8 EMAIL ACCOUNTS

All email accounts maintained on GHANA INFRASTRUCTURE INVESTMENT FUND's email systems are the property of the GIIF. Passwords shall not be given to other people.

5.9 MIS-ADDRESSED E-MAIL

Misaddressed e-mail that may have been received and opened inadvertently must be deleted from the system immediately by the employee receiving and opening such e-mail. If its location on the system is uncertain, then the assistance of IT Manager or his / her Delegate should be notified. The employee concerned shall also notify the sender of such e-mail of the circumstances of receipt and of the fact that it has been deleted.

5.10 UNAUTHORIZED ACCESS

Authorized Employees shall not knowingly permit the unauthorized use of GIIF's e-mail system. Any unauthorized use of GIIF's e-mail system must be reported without delay to the appropriate Department's Head or the IT Manager or his / her Delegate.

5.11 MONITORING & DISCLOSURE OF INFORMATION

No employee shall of his/her own accord under any circumstances respond in any way to any discovery notice or demand to disclose any particulars about GIIF e-mail, or to any subpoena to produce any e-mail at any court proceedings, (other than to acknowledge receipt thereof if necessary) without first obtaining the authority and advice of the Corporate Lawyer.

5.12 Monitoring, Access to and Disclosure of GIIF Information

a. Monitoring

The GIIF's computer systems are provided to employees for business and incidentally for personal purposes. To protect its rights and interests, the GIIF reserves the right to procure and install monitoring software to routinely monitor activities involving Internet usage and e-mail usage. GIIF reserves the right to access and read the contents of e-mail messages and track Internet usage in the following circumstances:

i. In far as it is required by law or by legal obligations to third parties to do so,
ii. If it has a legitimate business need or reason to do so,
iii. To protect its interests if it suspects that an employee has committed or is committing a crime that might be aim at or attributable to the GIIF,
iv. If it is of the bona fide opinion that such access or disclosure may be necessary to investigate a breach of the security of the e-mail system or of this policy.

Provided that, subject to the restrictions **set out below**, the GIIF will not seek to obtain access to the contents of any employee's e-mail files without the permission of the employee concerned.

v. Should the IT Manager or his/her Delegate encounter indications of illegal activity or violations of the GIIF policy or security, the IT Manager or his/her Delegate shall investigate further and report any findings to the Head / Manager of the Department concerned and Senior Management.

Employees must ensure that all business-related e-mail messages that should be made available to other employees of the GIIF. The employee consents to access by the GIIF to protect system security or the GIIF's proprietary rights.

b. Internal Disclosure

The contents of legitimate business e-mail may be disclosed within the GIIF without the permission of any employee who was the addressor or addressee of such e-mail. However, any internal disclosure within the GIIF without the consent of the employees concerned shall be limited to those employees who have a reasonable need for access to such e-mail.

c. External Disclosure

i. The Fund may, in its discretion and for any legitimate purpose, disclose to third parties the contents of e-mail messages sent to, or received by, its employees.

ii. The Fund will, however, attempt to accommodate any objections to such disclosure on the grounds, reasonably based, that such disclosure will create personal embarrassment for the employee concerned, unless such disclosure, in the Fund's discretion, is required to serve an important business purpose or satisfy a legal obligation, or that the contents of such message are personal and private in nature.

d. Use of Information for bona fide business purposes

The Fund may use information regarding the number, sender, recipient, and addressees of e-mail messages sent over the GIIF's e-mail system for any bona fide business purpose.

e. Legal Obligation to Disclose

If the Fund is legally obliged to disclose e-mail messages to a third party, GIIF shall give reasonable prior notice to the employee whose e-mail requires to be disclosed, unless:

i. The Fund is legally obliged to allow such disclosure without such reasonable notice or without any notice at all, or

ii. Such disclosure is required by a law enforcement agency and

iii. It is contrary to the interests of justice or law enforcement to notify the employee of such disclosure, or

iv. The Fund has prima facie reason to believe that the law enforcement activity relates to the possibility that GIIF may be the victim of a crime.

f. Any request made to GIIF for access to the contents of e- mail without the consent or knowledge of the sender or recipients shall be considered by the Head /Manager of the department concerned and

i. Such requests must be approved in advance and any access without such approval shall constitute a serious breach of this Policy.

ii. The use or disclosure of information obtained from inspection or monitoring of GIIF's e-mail must be reviewed and approved in advance in writing by the Head/Manager of the Department concerned.

5.13 DISCLAIMER

The following disclaimer will be added to each outgoing email:

GHANA INFRASTRUCTURE INVESTMENT FUND

This e-mail contains confidential information or information belonging to GHANA INFRASTRUCTURE INVESTMENT FUND Company Ltd and is intended solely for the addressees. The opinions therein, explicit, or implied, are solely those of the author and do not necessarily represent those of GHANA INFRASTRUCTURE INVESTMENT FUND as a company. The unauthorized disclosure, use, dissemination or copying (either Whole or partial) of this e-mail, or any information it contains, is prohibited. E-mails are susceptible to alteration and their integrity cannot be guaranteed. GHANA INFRASTRUCTURE INVESTMENT FUND shall not be liable for this e-mail if modified or falsified. If you are not the intended recipient of this e-mail, please delete it immediately from your system and notify the sender of the wrong delivery and the e-mail deletion.

6. INTRANET AND INTERNET SECURITY POLICY

6.1 GENERAL INTERNET POLICY

The Ghana Infrastructure Investment Fund's computer network introduces added resources and new services through Intranet and Internet connectivity. This connectivity not only results in new capabilities, but also in new risks and threats. This document formally defines GIIF's official policy regarding Intranet and Internet security in response to potential risks. All Internet users are expected to be familiar with and to comply with this policy.

i. Unless specifically stated otherwise, all statements and policies will apply to both the Intranet and the Internet.
ii. All users who require access to Internet services must do so by using GHANA INFRASTRUCTURE INVESTMENT FUND approved software and Internet gateways.
iii. Access to Internet services shall be provided by discrete, designated, and secured sources.
iv. Employees must not circumvent the firewalls and filters by using analogue lines, modems, or network tunnelling software to connect to the Internet.
v. At no time should networked workstations with modems be left in an accessible state that could potentially allow unauthorized access.

6.2 BROWSING POLICY

i. Software for browsing the Internet such as Internet explorer or any related browser is provided to employees primarily for business use.
ii. Any personal use must not interfere with normal business activities, must not involve solicitation, must not be associated with any for-profit outside business activity, and must not potentially embarrass GHANA INFRASTRUCTURE INVESTMENT FUND.
iii. No sites known to contain offensive material shall be visited.
iv. GIIF Internet users are prohibited from transmitting or downloading material that is obscene, pornographic, threatening, or racially or sexually harassing.
v. All Internet browsing activity shall be monitored.
vi. Any files downloaded over the Internet shall be scanned for viruses, using approved virus detection software.

6.3 INTERNET RESPONSIBLE USE POLICY

It is GHANA INFRASTRUCTURE INVESTMENT FUND ‘s policy to trust the internal users on its networks. Inherent in this trust is the expectation that every internal user shall act in a responsible manner. To aid an internal user, the following are provided as user-level policy guidelines for responsible use of a firewalled Internet connection.

i. All access to an external network must have as its basis in a related business purpose.

ii. All data coming from the internal networks is the property of GHANA INFRASTRUCTURE INVESTMENT FUND, and GIIF reserves the right to inspect this data and to restrict or prevent its transfer to an external network.

iii. A user may not enter GHANA INFRASTRUCTURE INVESTMENT FUND any obligations on external networks without prior approval.

iv. No confidential material may be sent or posted to an external network unless the sender is explicitly authorized by management to send the material and the material is protected from unauthorized exposure while in transit.

v. All non-confidential material sent or posted to an external network must be professional in nature.

vi. An internal user importing information from an external source must test the imported material (in an isolated context) for hidden viruses and must make a best effort not to activate imported viruses in a manner such that systems on the internal networks are exposed to imported viruses.

vii. An internal user must make a best effort to safeguard all security tokens and passwords used to gain access to the internal networks.

viii. Resource-intensive use of an external connection must be initiated during off hours, not during normal business hours. Responsible use of the Internet connection is not limited to the above guidelines. A complete set of guidelines cannot be devised because it is impossible to plan for every contingency. It is the responsibility of the individual to evaluate his or her unique situation and act in a manner that safeguards both GHANA INFRASTRUCTURE FUND’s resources and the reputation of the GIIF.

6.4 PROHIBITED USAGE

Activities that are prohibited include, but are not limited to:

i. Any unauthorized, deliberate action that damages or disrupts computing systems or networks, alters their normal performance, or causes them to malfunction regardless of location or duration.
ii. Wilful or negligent introduction of computer viruses, Trojan horses, or other destructive programs into GIIF systems or networks or into external systems and networks.
iii. Unauthorized decryption or attempt at decryption of any system or user passwords or any other user's encrypted files.
iv. Packet sniffing, packet spoofing, or use of any other means to gain unauthorized access to a computing system or network.

Violations of the *Intranet and Internet Security Policy* shall be documented and can lead to revocation of system privileges and/or disciplinary action up to and including termination of appointment. Additionally, GIIF may at its discretion seek legal remedies for damages incurred because of any violation.

Before access to the GIIF network is approved, the potential Intranet/Internet user is required to read this *Intranet and Internet Security Policy* and sign an acknowledgement (See appendix). The signed acknowledgment form should be turned in and will be kept on file at IT. If there is a question about the correctness of a course of action (with respect to the Internet Gateway), it should be directed to IT Department.

6.5 WEB BROWSING

The Internet is a network of interconnected computers of which GHANA INFRASTRUCTURE INVESTMENT FUND has very little control. The employee should recognize this when using the Internet and understand that it is a public domain and he or she can encounter information, even inadvertently, that he or she may find offensive, sexually explicit, or inappropriate. The user must use the Internet at his or her own risk. GHANA INFRASTRUCTURE INVESTMENT FUND is specifically not responsible for any information that the user views, reads, or downloads from the Internet.

6.6 INTERNET PERSONAL USE

GHANA INFRASTRUCTURE INVESTMENT FUND recognizes that the Internet can be a tool that is useful for both personal and professional purposes. Personal usage of the GIIF computer systems to access the Internet is permitted, and before/after business hours, if such usage follows pertinent guidelines elsewhere in this document and does not have a detrimental effect on GHANA INFRASTRUCTURE INVESTMENT FUND or on the individual's job performance.

6.7 REMOTE DESKTOP ACCESS

Use of remote desktop software (Anydesk) and/or services is allowable if it is provided by GIIF.

6.8 CIRCUMVENTION OF SECURITY

Using GIIF-owned or GIIF-provided computer systems to circumvent any security systems, authentication systems, user-based systems, or escalating privileges is expressly prohibited. Knowingly taking any actions to bypass or circumvent security is expressly prohibited.

6.9 NON-GIIF OWNED EQUIPMENT

The user must obtain written permission from the IT department before installing outside or non-GIIF-provided computer systems on GHANA INFRASTRUCTURE INVESTMENT FUND network. Once this permission is obtained, and dependent on any conditions granted along with such permission, the user can connect a non-GIIF owned system to the network. Reasonable precautions must be taken to ensure viruses, Trojans, worms, malware, spy-ware, and other undesirable security risks are not introduced into GIIF network.

6.10 SOFTWARE INSTALLATION

Installation of non-GIIF supplied programs are prohibited. Numerous security threats can masquerade as malicious software - malware, spy-ware, and Trojans can all be installed inadvertently through games or other programs. Alternatively, software can cause conflicts or have a negative impact on system performance.

6.11 REPORTING OF SECURITY INCIDENTS

If a security incident or breach of any security policies is discovered or suspected, the user must immediately notify his or her supervisor and/or follow any applicable guidelines as detailed in the GIIF Incident Response Policy. Examples of incidents that require notification include:

i. Suspected compromise of log-in credentials (username, password, etc.).
ii. Suspected virus/malware/Trojan infection.
iii. Loss or theft of any device that contains GIIF information.
iv. Any attempt by any person to obtain a user's password over the telephone or by email.
v. Any other suspicious event that may impact GHANA INFRASTRUCTURE INVESTMENT FUND's information system.

Users must treat a suspected security incident as confidential information and report the incident only to his or her supervisor with a copy to the IT Manager. Users must not withhold information relating to a security incident or interfere with an investigation.

7. CONFIDENTIAL DATA

7.1 OVERVIEW

Confidential data is typically the data that holds the most value to an organisation. Often, confidential data is valuable to others as well, and thus can carry greater risk than general company data. For these reasons, it is a good practice to dictate security standards that relate specifically to confidential data.

7.2 STORAGE

Confidential information must be removed from desks, computer screens, and common areas unless it is currently in use. Confidential information should be stored under lock and key (or keycard / keypad), with the key, keycard, or code secured.

7.3 USE OF CONFIDENTIAL DATA

A successful confidential data policy is dependent on the users knowing and adhering to GHANA INFRASTRUCTURE INVESTMENT GIIF's standards involving the treatment of confidential data.

The following applies to how users must interact with confidential data:

i. Users must be advised of any confidential data they have been granted access. Such data must be marked or otherwise designated 'confidential.'
ii. Users must only access confidential data to perform his/her job function.
iii. Users must not seek personal benefit, or assist others in seeking personal benefit, from the use of confidential information.
iv. Users must protect any confidential information to which they have been granted access and not reveal, release, share, email unencrypted, exhibit, display, distribute, or discuss the information unless necessary to do his or her job or the action is approved by his or her supervisor.
v. Users must report any suspected misuse or unauthorized disclosure of confidential information immediately to his or her supervisor.
vi. If confidential information is shared with third parties, such as contractors or vendors, a confidential information or non-disclosure agreement must govern the third parties' use of confidential information.
vii. If confidential information is shared with a third party, GIIF must indicate to the third party how the data should be used, secured, and, destroyed. Refer to GIIF's outsourcing policy for additional guidance.

7.4 DATA STORAGE

The following guidelines apply to storage of the different types of company data:

i. **Personal** - There are no requirements for personal information.
ii. **Public** - There are no requirements for public information.
iii. **Operational** - Operational data must be stored where the backup schedule is appropriate to the importance of the data, at the discretion of the user.

iv. **Critical** - Critical data must be stored on a server that gets the most frequent backups (refer to the Backup Policy for additional information). System- or disk-level redundancy is required.

v. **Confidential** - Confidential information must be removed from desks, computer screens, and common areas unless it is currently in use. Confidential information should be stored under lock and key (or keycard/ keypad), with the key, keycard, or code secured.

8. INCIDENCE RESPONSE MANAGEMENT POLICY

8.1 PURPOSE

This policy is intended to ensure that GHANA INFRASTRUCTURE INVESTMENT FUND is prepared to restore a service operation to normalcy as quickly as possible and minimise the adverse impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained. 'Normal service operation' is defines here as service operation within Service Level Agreement (SLA) limits.

8.2 DEFINITION OF INCIDENT AND TYPE OF INCIDENTS

A security incident is defined as ***"An unplanned interruption to an IT Service or Reduction in the Quality of an IT Service or Failure of any item, Hardware, or Software, used in the support of a system that has not yet affected service is also an incident***".

GHANA INFRASTRUCTURE INVESTMENT FUND's information assets can take one of two forms. For the purposes of this policy a security incident is defined as one of the following:

i. **Electronic**: This type of incident can range from an attacker or user accessing the network for unauthorized/malicious purposes, to a virus outbreak, to a suspected Trojan or malware infection

ii. **Physical**: A physical IT security incident involves the loss or theft of a laptop, mobile device, PDA/Smartphone, portable storage device, or other digital apparatus that may contain company information.

8.3 SEVERITY

Severity is determined by how much the users are restricted from performing their work. There are three grades of severity:

i. Low: Issue prevents the user from performing a portion of their duties.
ii. Medium: Issue prevents the user from performing the critical time sensitive functions
iii. High: Service or major portion of service is unavailable

The severity of an incident will be used in determining the priority for resolution.

Finally, GIIF should review any industry or governmental regulations that dictate how it must respond to a security incident (specifically, loss of customer data), and ensure that its incident response plans adhere to these regulations.

8.4 ELECTRONIC INCIDENTS

Responsibilities may be delegated, but escalation does not remove responsibility from the individual accountable for a specific action.

The IT Department,

i. Owns all reported incidents.
ii. Ensure that all incidents received are recorded or logged in the issue register.
iii. Identify nature of incidents based upon reported symptoms and categorisation rules supplied by the service provider.
iv. Prioritise the incidents based upon impact to the users and SLA guidelines.
v. Responsible for the incident closure
vi. Delegates responsibility by assigning incidents to the appropriate service provider for resolution based upon the categorisation rules.
vii. Performs post-resolution user review to ensure that all work services are functioning properly, and all incident documentation is complete.
viii. Prepare reports showing statistics of incidents resolved/unresolved.

8.5 INCIDENT CATEGORISATION, PRIORITISATION AND ESCALATION

8.5.1 CATEGORISATION

The goals of proper categorisation are:

i. Identify service impacted and appropriate SLA and escalation timelines.
ii. Indicate what support groups need to be involved.
iii. Provide meaningful metrics on system reliability.

For each incident the specific service will be identified. It is critical to establish with the user the specific area of the service being provided. For example, if it's Finance is it GL, Account Payable etc? identifying the service properly establishes the appropriate SLA and relevant Service Level Targets.

In addition, the severity and impact of the incident need to be established. Does the incident cause a work stoppage for the users, or do they have other means of performing the job? An example would be a broken link on the web page is an incident but, if there is another navigation path to the desired page, incident's severity would be LOW because the user can still perform the needed function.

The incident may create a work stoppage for only one person but, the impact is far greater because it is a critical function. An example of this scenario would be the person processing payroll having an issue which prevents the payroll processing. The impact affects many more personnel than just the user.

Below are the targets for response and resolution for incidents based upon priority.

Priority	Target	
	Response	Resolve
3 – Low	90% - 24 hours	90% - 7 days*
2 – Medium	90% - 2 hours	90% - 4 hours
1 – High	95% - 15 minutes	90% - 2 hours

8.6 SECURITY INCIDENT HANDLING AND PROCEDURE

The following establishes an operational incident handling procedure for GIIF information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities, track, document, and report incidents to appropriate department.

If an employee become aware of any policy violation or suspect that your password may have been used by someone else, first, change your password and then, report the violation immediately to the IT helpdesk.

8.6.1 REPORTING PROCEDURE AND COLLECTION OF SECURITY INCIDENT INFORMATION

Below is the procedure for responding to security incidents.

Upon identifying a problem, disconnect the network cable.

Notify the IT helpdesk and the appropriate Chain-of-Command.

Suspected cause for incident (Name, virus, etc.)

Was Antivirus software running at the time of infection?

How and when the problem was first identified?

Has IT staff been notified/are they involved?

Number of workstations infected?

Any other equipment infected?

- Action plan for removal.
- Will infected workstations be re-imaged before reconnection?
- When was the last update of signature files?
- When was the last operating system update?

See Annexure for the form to complete

9. DATA BACKUP AND RETENTION

9.1 OVERVIEW AND POLICY STATEMENT

The purpose of this policy is to maintain data integrity and availability of the University's IT Resources, to prevent data loss within the limits of record retention requirements, and to facilitate the restoration of the IT Resources and business processes.

The GIIF's policy about Data Backup and Retention of corporate Data is as follows:

"All Critical Data being generated, processed, and stored by Ghana Infrastructure Investment GIIF must be always have a Backup. This is to ensure that Data is not lost on the account of hardware/software failure or man-made errors or should there be a physical disaster in the IT Systems".

System Owners must perform system state backups to support the Recovery Point Objective (RPO) and Recovery Time Objective (RTO).

System state backups must be retained for no less than 90 days and no more than one year unless otherwise stated

Annually, System Owner(s) must test restore system state backups.

9.2 SCOPE

This policy applies to all data stored on corporate systems. The policy covers such specifics as the type of data to be backed up, frequency of backups, storage of backups, retention of backups, and restoration procedures.

9.3 IDENTIFICATION OF CRITICAL DATA

GHANA INFRASTRUCTURE INVESTMENT FUND must identify what data is most critical to its organization. This can be done through a formal data classification process or through an informal review of information assets. Regardless of the method, critical data should be identified so that it can be given the highest priority during the backup process.

9.4 DATA TO BE BACKED UP

A backup policy must balance the importance of the data to be backed up with the burden such backups place on the users, network resources, and the backup administrator. Data to be backed up will include:

i. All data determined to be critical to GIIF operation and/or employee job function.
ii. All information stored on the corporate file server(s) and email server(s), as well as these servers operating systems and logs. It is the user's responsibility to ensure any data of importance is moved to the Smart workplace/one drive.
iii. All information stored on network servers, which may include web servers, database servers, domain controllers, firewalls, and remote access servers, etc.
iv. Logs and configuration of network devices such as switches, routers, etc.

9.5 OFF SITE ROTATION

Geographic separation from the backups must be maintained, to some degree, to protect from fire, flood, or other regional or large-scale catastrophes. Off-site storage must be balanced with the time required to recover the data, which must meet GIIF's up-time requirements. Core database backups must be stored in the cloud or Disaster Recovery site daily.

9.6 BACKUP STORAGE

Storage of backups is a serious issue and one that requires careful consideration. Since backups contain critical, and often confidential, company data, precautions must be taken that are commensurate to the type of data being stored. GHANA INFRASTRUCTURE INVESTMENT FUND has set the following guidelines for backup storage. When stored on-site, backup media must be stored in a fireproof container in an access-controlled area. When shipped off-site, a hardened facility (i.e., INVESTMENT commercial backup service) that uses accepted methods of environmental controls, including fire suppression, and security processes must be used to ensure the integrity of the backup media. If a backup service is used, rigorous security procedures must be developed and maintained, which will include, at minimum, credential-verification, and signature of the backup service courier. Online backups are allowable if the service meets the criteria specified herein.

Below is the link to the online storage of SAGE database,

https://teams.microsoft.com/l/channel/19%3ArD2nSFVwdoX5qlpNuOjgD-OJhAhsvOMFktCfOVBdQ9Y1%40thread.tacv2/General?groupId=bb766ee5-54bd-4c9d-aa07-755b808272b1&tenantId=

9.7 BACKUP RETENTION

When determining the time required for backup retention, GHANA INFRASTRUCTURE INVESTMENT FUND must determine what number of stored copies of backup-up data is sufficient to effectively mitigate risk while preserving required data. GIIF has determined that the following will meet all requirements (note that the backup retention policy must conform to any industry, legal and statutory regulations, if applicable e.g., Data Protection Act):

i. Full Backups of non-critical Data must be saved for Twelve months.
ii. Core Business Data system backups must be stored for a period of five years.

9.8 RESTORATION PROCEDURES & DOCUMENTATION

The data restoration procedures must be tested and documented. Documentation should include exactly who is responsible for the restoration, how it is performed, under what circumstances it is to be performed, and how long it should take from request to restoration. It is extremely important that the procedures are clear and concise such that they are not:

i. Misinterpreted by readers other than the backup administrator, and
ii. Confusing during a time of crisis

9.9 BACKUP CONTROL, AND REVIEW

Annually, the back-up policies are reviewed for adequacy and completeness. This review considers the service delivery needs, as determined in conjunction with the business owners, within the institution and whether they have changed sufficiently to require more frequent and stringent back-up requirements.

10. ANTIVIRUS/ANTI-MALWARE POLICY

Computer viruses and malware are pressing concerns in today's threat landscape. If a machine or network is not properly protected, a virus outbreak can have devastating effects on the machine, the network, and the entire institution.

The purpose of this policy is to describe the responsibilities of individuals, departments, and Information Technology (IT) in protecting GHANA INFRASTRUCTURE INVESTMENT FUND computer systems against virus and malware infections.

10.1 VIRUS PROTECTION

Employees are alerted to the fact that viruses can cause substantial harm to GIIF's computer systems. The damage caused is often not limited to hardware or software but can result in significant financial loss to the Fund.

i. The I.T department will ensure that the latest GIIF-approved Antivirus protection software has been installed on all computers and is permanently enabled.
ii. Should any data be received by an Employee via disk; Internet, e-mail or any external source, a comprehensive scan of that data should be performed prior to loading that data onto the GIIF's computer systems.
iii. If a virus is detected, the I.T department should be notified immediately. Installation of non-GIIF approved Virus protection software is prohibited.

Potential sources of viruses include shared media such as flash disks or CD-ROMs, electronic mail (including, but not limited to, files attached to messages), and software or documents copied over networks such as the Internet, and over P2P applications and Web popups.

GIIF provides the following guidelines on the use of antivirus/anti-malware software:

i. All GIIF-provided user workstations must have antivirus/anti-malware (Windows Defender) software installed.
ii. Workstation software must maintain a current 'subscription' to receive patches and virus signature/definition file updates.

iii. Daily Patches, updates, and antivirus signature file updates must be installed in a timely manner, either automatically or manually.

iv. Automatic scanning for virus must be installed on all PCs and servers accessing the Internet and should not be turned off by the user.

v. All software downloaded from non- GIIF sources through the Intranet or Internet must be screened with virus detection software before being invoked.

vi. Always scan files retrieved from a CD or other external source.

vii. Always scan all files downloaded from the Internet.

10.2 INFORMATION RESOURCES AND TECHNOLOGY RESPONSIBILITIES

GHANA INFRASTRUCTURE INVESTMENT FUND maintains licensing for an Antivirus software as its supported client anti-virus application. The Antivirus is automatically installed on personal computers and servers acquired through for use at GIIF. Information Technology department must maintain up-to-date virus definitions for download to individual computers. When a new virus is identified, IT may send out a notice instructing end users to retrieve a new virus definition immediately.

On an ongoing basis, IT staff will take appropriate action to contain virus infections as they occur and to assist in their removal. To prevent the spread of a virus, or to contain damage being caused by a virus, it may be necessary for IT to remove a computer from the network or disable a segment of the network.

Information Technology technical staff will maintain current patch levels and virus protection on all servers under their control. They will scan systems for vulnerabilities on a regular basis and provide product and configuration recommendations to departments regarding system security and virus protection. On an ongoing basis, IT staff will investigate and evaluate security solutions that may benefit the GIIF network and systems.

10.3 ADVICE AND ASSISTANCE

Additionally, Information Technology will provide virus protection assistance in the following ways:

I. The IT Helpdesk and staff will assist individuals with recovery from viruses. This includes advice on containment to stop the spread, help with removing viruses, and advice on how to prevent a recurrence.

II. Timely information regarding virus threats will be sent to users in a variety of ways, including notices via electronic mail and memos and WhatsApp messages.

III. Information Technology will continue to work with staff to increase awareness of the importance of adequate virus protection.

10.4 PROCEDURE FOR DEALING WITH INFECTED COMPUTERS

Virus activity is generally initially suspected when a great deal of traffic is identified by network administration software coming from a particular IP address (in use by a particular individual) on the network. When this occurs, the following steps should be taken:

i. Network access by that computer should be restricted.

ii. IT department is informed immediately, and the incident is logged in the incident/issue register.

iii. A time will be arranged for the infected computer to be scanned and cleaned. If files appear to be damaged or missing, file recovery will be attempted.

iv. The IT staff will ensure that the antivirus is installed and updating daily on the computer.

11. SOFTWARE SECURITY POLICY

Software applications can create risk in several ways, and thus certain aspects of software use must be covered by this policy. This policy provides guidelines for employees to follow to ensure that we are both legal and ethical in the use of our software assets. All software assets are for business use only and should not be used by employees for personal interests.

GHANA INFRASTRUCTURE INVESTMENT FUND provides the following requirements for the use of software applications:

i. GIIF will provide copies of legally acquired software to meet all legitimate needs in a timely fashion and in sufficient quantities for all our computers. The use of software

obtained from any other source could present security and legal threats to GIIF, and such use is strictly prohibited.

ii. Software should be kept reasonably up to date by installing new patches and releases from the vendor.

iii. Vulnerability alerts should be monitored for all software products that GIIF uses. Any patches that fix vulnerabilities or security holes must be installed expediently.

iv. No copies of GIIF software or its documentation can be made without the express written consent of the software publisher and GIIF.

v. The unauthorized duplication of copyrighted software or documentation is a violation of the law and is contrary to established standards of conduct for GIIF employees.

11.1 INTERNAL CONTROLS

GHANA INFRASTRUCTURE INVESTMENT FUND reserves the right to protect its reputation and its investment in computer software by enforcing strong internal controls to prevent the making or use of unauthorized copies of software. These controls may include periodic assessments of software use, announced and unannounced audits of GIIF computers to assure compliance, the removal of any software found on GIIF property for which a valid license or proof of license cannot be determined, and disciplinary actions, including termination, in the event of employee violation of this policy.

12. PASSWORD POLICY

12.1 OVERVIEW

A solid password policy is perhaps the most important security control an organization can employ. Since the responsibility for choosing good passwords falls on the users, a detailed and easy-to-understand policy is essential.

GIIF has no Active Directory in place therefore, this policy section effects on business applications installed and being used by staff.

12.2 PURPOSE

The purpose of this policy is to specify guidelines for use of passwords. Most importantly, this policy will help users understand why strong passwords a necessity is and help them create passwords that are both secure and useable. Lastly, this policy will educate users on the secure use of passwords.

12.3 SCOPE

This policy applies to any person who is provided an account on the GIIF's network or systems, including: employees, guests, contractors, partners, vendors, etc.

12.4 POLICY STATEMENT

i. Security tokens (i.e., Smartcard) must be returned on demand or upon termination of the relationship with GIIF.
ii. All passwords, including initial passwords, must be constructed, and implemented according to the specified guidelines under the password policy.
iii. Stored passwords must be encrypted.
iv. Administrators must not circumvent the Password Policy for the sake of ease of use.
v. Users cannot circumvent password entry with auto logon, application remembering, embedded scripts or hardcoded passwords in client software.
vi. Exceptions may be made for specific applications (like automated backup) with the approval of the IT Manager. For an exception to be approved there must be a procedure to change the passwords.
vii. In the event passwords are found or discovered, the following steps must be taken:
    a. Take control of the passwords and protect them.
    b. Transfer the passwords to an authorized person as directed by the GIIF IT Manager

12.5 PASSWORD CONSTRUCTION

The best security against a password incident is simple: following a sound password construction strategy. The GIIF mandates that users adhere to the following guidelines on password construction:

i. Passwords should be at least 8 characters.

ii. Passwords should be comprised of a mix of letters, numbers, and special characters (punctuation marks and symbols) Passwords should be comprised of a mix of upper- and lower-case characters.
iii. Passwords should not be comprised of, or otherwise utilize, words that can be found in a dictionary.
iv. Passwords should not be comprised of an obvious keyboard sequence (i.e., qwerty)
v. Passwords should not include ‘guessable’ data such as personal information about yourself, your spouse, your pet, your children, birthdays, addresses, phone numbers, locations, etc.
vi. Another way to create an easy-to-remember strong password is to think of a sentence, and then use the first letter of each word as a password. The sentence: 'The quick brown fox jumps over the lazy dog!' easily becomes the password 'Tqbfjotld!'. Of course, users may need to add additional characters and symbols required by the Password Policy, but this technique will help make strong passwords easier for users to remember.

12.6 CONFIDENTIALITY

Passwords should be considered confidential data and treated with the same discretion as any of the GIIF's proprietary information. The following guidelines apply to the confidentiality of GIIF passwords:

i. Users must not disclose their passwords to anyone.
ii. Users must not share their passwords with others (co-workers, supervisors, family, etc.)
iii. Users must not write down their passwords and leave them unsecured.
iv. Users must not check the ‘save password’ box when authenticating to applications. Users must not use the same password for different systems and/or accounts.
v. Users must not send passwords via email.
vi. Users must not re-use same passwords for a period of 1 year.
vii. If the security of a password is in doubt, the password must be changed immediately.

12.7 CHANGE FREQUENCY

To maintain good security, passwords should be periodically changed. This limits the damage an attacker can do as well as helps to frustrate brute force attempts. At a minimum, users must change passwords every 30 days and at most 90 days.

12.8 PASSWORD GUIDELINES

The following is a guideline on 'best practice' in password creation/usage.

i. MINIMUM No. of Characters in password: 8 (Eight)

ii. Composition of a Password: Any character on a standard keyboard. Must contain characters from 3 out of the following 4 groups:
   a. Upper case letters (A, B, C……. Y, Z)
   b. Lower case letters (a, b, c…. y, z)
   c. Number (0,1,2……9)
   d. Non-alphanumeric characters (@! &, *,….etc)

iii. Case Sensitive: YES (Windows Log on)

iv. Maximum number of log-on attempts: 3 (THREE) after which the password will be disabled and can only be enabled by the System Administrator

v. Use of old passwords: You cannot re-use any of the previous 10 passwords used.

vi. Password Validity (Expiry) period: 90 Days. If not changed within sixty days, it expires automatically, and the system will force the user to change the password before he can perform any other action in the system.

vii. Number of Days Password Expiry Warning: 10 (TEN) DAYS. A warning will be given at every sign-on during the last 10 days before a password expires. As each day elapses the system tells you how many days are remaining to expiry.

viii. Maximum No. of active sessions per user id: 1 (ONE). This means a user can only sign on to one workstation at a time i.e., you cannot sign on to more than one workstation simultaneously. This is intentionally meant to reduce incidents of password sharing.

13. PHYSICAL SECURITY POLICY

13.1 OVERVIEW

Information assets are necessarily associated with the physical devices on which they reside. Information is stored on workstations and servers and transmitted on GIIF's physical network infrastructure. To secure GIIF data, thought must be given to the security of GIIF's physical Information Technology (IT) resources to ensure that they are protected from standard risks.

13.2 PURPOSE

The purpose of this policy is to protect GHANA INFRASTRUCTURE INVESTMENT FUND's physical information systems by setting standards for secure operations.

13.3 SCOPE

This policy applies to the physical security of GIIF's information systems, including, but not limited to, all GIIF-owned or GIIF-provided network devices, servers, personal computers, mobile devices, and storage media. Additionally, any person working in or visiting GIIF's office is covered by this policy.

Please note that this policy covers the physical security of GIIF's Information Technology infrastructure and does not cover the security of non-IT items or the important topic of employee security. While there will always be overlaps, care must take to ensure that this policy is consistent with any existing physical security policies.

13.4 CONTROLLED ACCESS AREAS

The following policies apply to GIIF Computer Centres:

i. Server room must be located within the GIIF or vendor Internal Space.
ii. Server room must remain locked even when being attended to.
iii. Visitors to the room must have a valid business purpose and must be escorted by someone authorized for unescorted access. Anyone escorting a visitor to the Server room will be held accountable for their role as a security escort.

iv. Any access by someone not on the access list must be logged and include the identity of the visitor and escort as well as the time in, time out and reason for entry.
v. Access shall be managed by an electronically controlled access system.
vi. In the event of a malfunction of the electronic access system, that system shall be disabled, and access shall be managed by a physical key system until repairs is made to the electronic system.

13.5 PHYSICAL DATA SECURITY

Certain physical precautions must be taken to ensure the integrity of GIIF's data. At a minimum, the following guidelines must be followed:

i. Computer screens must be positioned where information on the screens cannot be seen by outsiders.
ii. Confidential and sensitive information must not be displayed on a computer screen where the screen can be viewed by those not authorized to view the information.
iii. Users must log off or shut down their workstations when leaving for an extended time, or at the end of the workday.
iv. Network cabling must not run through non-secured areas unless the cabling is carrying only public data (i.e., extended wiring for an Internet circuit).
v. Network ports that are not in use must be disabled.

13.6 FIRE PREVENTION

It is GIIF's policy to provide a safe workplace that minimizes the risk of fire. In addition to the danger to employees, even a small fire can be catastrophic to computer systems. Further, due to the electrical components of IT systems, the fire danger in these areas is typically higher than other areas of GIIF's office. The guidelines below are intended to be specific to GIIF's information technology assets and should conform to GIIF's overall fire safety policy.

i. Fire, smoke alarms, and/or suppression systems must be used, and must conform to local fire codes and applicable ordinances.
ii. Electrical outlets must not be overloaded. Users must not chain multiple power strips, extension cords, or surge protectors together.

iii. Extension cords, surge protectors, power strips, and uninterpretable power supplies must be of the three-wire.

iv. Unused electrical equipment should be turned off when not in use for extended periods of time (i.e., during non-business hours) if possible.

v. Periodic inspection of electrical equipment must be performed. Power cords, cabling, and other electrical devices must be checked for excessive wear or cracks. If overly worn equipment is found, the equipment must be replaced or taken out of service immediately depending on the degree of wear.

vi. A smoke alarm monitoring service must be used that will alert a designated GIIF employee if an alarm is tripped during non-business hours.

13.7 ENTRY SECURITY

It is GIIF 's policy to provide a safe workplace for employees. Monitoring those who enter and exit the premises is a good security practice in general but is particularly true for minimizing risk to GIIF's systems and data. The guidelines below are intended to be specific to GIIF's information technology assets and should conform to GIIF 's overall security policy.

13.8 SIGN-IN REQUIREMENTS

GHANA INFRASTRUCTURE INVESTMENT FUND must maintain a sign-in log (or similar device) in the lobby or entry area and visitors must be required to sign in upon arrival. At a minimum, the register must include the following information: visitor's name, company name, reason for visit, name of person visiting, sign-in time, and sign-out time.

13.9 VISITOR ACCESS

Visitors should be given only the level of access to GIIF premises that is appropriate to the reason for their visit. After checking in, visitors must be escorted unless they are considered 'trusted' by GIIF. Examples of a trusted visitor may be GIIF's legal counsel, financial advisor, or a courier that frequents the office, and will be decided on a case-by-case basis.

14. VULNERABILITY MANAGEMENT

14.1 Policy objective:

IT resources can be exploited to steal sensitive data, damage systems, or deny access. Vendors, recognizing vulnerabilities in their products, create software patches and other strategies which are distributed to their customers. Unfortunately, as technologies evolve, new vulnerabilities are discovered, which must be mitigated. Some vulnerability can be managed only with add-on security software and other specialized tools. Non-technical vulnerabilities may also exist in the way users control access to sensitive data and computer systems.

"***A vulnerability, in information technology (IT), is a flaw in code or design that creates a potential point of security compromise for an endpoint or network" and***

"Vulnerability management planning is a comprehensive approach to the development of a system of practices and processes designed to identify, analyze and address flaws in hardware or software that could serve as attack vectors".

This policy directs the establishment of vulnerability management practices in order to proactively prevent the exploitation of vulnerabilities and potential loss of Ghana Infrastructure Investment Fund (GIIF) sensitive data. The objectives are to create and document systematic and accountable practices to maintain control programs and applications, and to mitigate other technical and non-technical vulnerabilities. The goals of these effort are to implement stronger protection for GIIF IT resources, ensure compliance with best practices, and reduce the impact of threats to the GIIF and Information Assets.

14.1.2 Intended audience:

All GIIF IT staff has responsibilities covering oversight of server, workstation, network devices, and application security; and tracking and updating of patches and updates for operating systems, network devices, and applications. They have access to sensitive information in electronic system format and must adhere to approved standards and procedures for accessing and managing sensitive data and other IT resources as detailed in the IT Security Policy.

14.2 Policy statement:

14.2.1 Ownership:

GIIF Information Technology infrastructure and systems are owned by the company. Considering that all IT staff members have access to sensitive information of some type, they must follow these procedures to reduce vulnerability risks.

14.2.2 Monitoring:

GIIF has the responsibility to monitor events and provide identification of unauthorized use of systems without notice. Consistent with generally accepted business practices, GIIF logs statistical data from its systems which will be analysed, secured and maintained to assist with troubleshooting and forensic assessments.

14.3 Provisions:

1. **Patch and Update Management**: - GIIF IT staff will install only approved software as listed in the Software Policy. Installed software will be maintained with appropriate patches and updates.
2. **Communications Threat Management**: - GIIF communications systems (e.g. email) will be actively managed for spam, malware and inappropriate content. Suspicious email will be quarantined or blocked.
3. **Internet Browser Threat Management: -** Internet access will have controls implemented to inform users about potentially malicious sites and actively stop access to known malicious sites.
4. **Asset Classification and Inventory**: - GIIF IT staff will maintain an inventory of software and IT equipment, along with an asset classification system.
5. **End-user Device and Server Intrusion Detection and Prevention:** – All end-user devices and servers will have technology deployed to prevent, detect, repair, and manage malicious software and unauthorized intrusions.
6. **Sensitive Data Loss Prevention: -** Sensitive IT resources will have technology deployed to verify the data is protected, accessed, stored, transmitted, and otherwise handled in a secure and authorized manner.

7. **End-user Device and Server Vulnerability Scanning and Threat Mitigation**: - IT Resources used to access, transmit and store sensitive data will be periodically scanned to verify they are free from vulnerabilities and up to date with all software versions and patches.
8. **Network Intrusion Detection and Prevention:** - The GIIF network is actively managed to detect and prevent unauthorized intrusion or access to sensitive data, and the transmission of malicious software or inappropriate content.
9. **File Integrity Management:** - Files containing sensitive data will be managed to ensure only appropriate access and authorized changes are allowed. When necessary, all access to files containing sensitive data will be logged and reviewed when it becomes necessary.
10. **Network Vulnerability Scanning and Threat Mitigation:** - All changes to the network will be approved, recorded, monitored, and verified. The network will be actively managed to detect network vulnerabilities and unauthorized changes or extensions to the network.

14.4 Reporting:

All staff of GIIF must report any flaw or loopholes in business applications, network or operating to the IT department either by phone, mail or verbal.

15. REVIEW

PLEASE NOTE THAT THIS POLICY IS SUBJECT TO REVIEW AND CHANGE BY THE BOARD OF DIRECTORS.

GHANA INFRASTRUCTURE INVESTMENT FUND will from time-to-time review and update this policy; any changes will be communicated to staff by re-issuing the appropriate page or paragraph.

---

16. DEFINITIONS

Account: A combination of username and password that allows access to computer or network resources.

Antivirus Software: An application used to protect a computer from viruses, typically through real time defences and periodic scanning. Antivirus software has evolved to cover other threats, including Trojans, spyware, and other malware.

Authentication: security method used to verify the identity of a user and authorize access to a system or network.

Backup: To copy data to a second location, solely for the purpose of safe keeping of that data.

Backup Media: Any storage devices that are used to maintain data for backup purposes. These are often magnetic tapes, CDs, DVDs, or hard drives.

Backup (Full): A backup that makes a complete copy of the target data.

Backup (Incremental): A backup that only backs up files that have changed in a designated time period, typically since the last backup was run.

Backup Restoration: Also called 'recovery.' The process of restoring the data from its backup-up state to its normal state so that it can be used and accessed in a regular manner.

Biometrics: The process of using a person's unique physical characteristics to prove that person's identity. Commonly used are fingerprints, retinal patterns, and hand geometry.

Blogging: The process of writing or updating a 'blog,' which is an online, user created journal (short for 'web log').

GIIF (The): GHANA INFRASTRUCTURE INVESTMENT FUND

GIIF data: Data in the custody of the GIIF concerning the GIIF, its business and/or its relations (e.g., records, mail etc. about its employees, customers or suppliers).

Certificate: Also called a 'Digital Certificate.' A file that confirms the identity of an entity, such as a company or person. Often used in VPN and encryption management to establish trust of the remote entity.

Datacentre: A location used to house a company's servers or other information technology assets. Typically offers enhanced security, redundancy, and environmental controls.

Demilitarized Zone (DMZ): A perimeter network, typically inside the firewall but external to the private or protected network, where publicly accessible machines are located. A DMZ allows higher-risk machines to be segmented from the internal network while still providing security controls.

Encryption: The process of encoding data with an algorithm so that it is Unintelligible without the key. Used to protect data during transmission or while stored.

Encryption Key: An alphanumeric series of characters that enables data to be encrypted and decrypted.

Employee: Any full-time or part-time employee of the GIIF, contractual staff as well as all contractors, advisors, agents and any third parties who may provide services to the GIIF from time to time.

Firewall: A security system that secures the network by enforcing boundaries between secure and insecure areas. Firewalls are often implemented at the network perimeter as well as in high-security or high-risk areas.

Guest: A visitor to GIIF premises who is not an employee

Harden: Generally, hardening may be treated as all of the steps used to tighten or improve the security on a computer. The process of hardening is that of identifying exactly what a specific machine will be used for and removing or disabling all system components not necessary for that function. It is turning a general-purpose computer into a single or limited purpose computer.

Internet: Is a worldwide 'network of networks' using Transmission Control Protocol/Internet Protocol (TCP/IP) for communication.

Intranet: Is GIIF's internal infrastructure connecting our facilities by using TCP/IP.

Instant Messaging: A text-based computer application that allows two or more Internet-connected users to 'chat' in real time.

Information Resources (IR): any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, handheld computers, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Information Security Officer (ISO): Responsible to General management for administering the information security functions within the GIIF. The ISO is the GIIF's internal and external point of contact for all information security matters.

This function falls under the IT Department.

IDS/IPS: Intrusion Detection / prevention System – A method of inspecting all inbound and outbound network activity that identifies suspicious patterns that may indicate a network or system attack. IPS goes as far as blocking the network or system attack.

Job-related Work: Any activities related to the employee's authorized responsibilities resulting from the contract between the employee and the GIIF (which may include amongst other things the storage and processing of GIIF data).

Keycard: A plastic card that is swiped, or that contains a proximity device, that is used for identification purposes. Often used to grant and/or track physical access.

Keypad: A small keyboard or number entry device that allows a user to input a code for authentication purposes. Often used to grant and/or track physical access.

Mac Address: Short for Media Access Control Address. The unique hardware address of a network interface card (wireless or wired). Used for identification purposes when connecting to a computer network.

Malware: Short for malicious software. Includes all computer viruses, worms, Trojan horses, or other, similar programs that have the potential of damaging files stored on the system, affecting the performance of any application, or degrading the overall performance of Company X's computer network.

Modem: A hardware device that allows a computer to send and receive digital information over a telephone line.

Mobile Data Device: A data storage device that utilizes flash memory to store data. Often called a USB drive, flash drive, or thumb drive.

Mobile Device: A portable device that can be used for certain applications and data storage. Examples are PDAs or Smartphone's.

Password: A sequence of characters that is used to authenticate a user to a file, computer, or network. Also known as a pass phrase or passcode.

Strong Passwords: A strong password is a password that is not easily guessed. It is normally constructed of a sequence of characters, numbers, and special characters, depending on the capabilities of the operating system. Typically, the longer the password the stronger it is. It should never be a name, dictionary word in any language, an acronym, a proper name, a number, or be linked to any personal information about you such as a birth date, social security number, and so on.

PDA: Stands for Personal Digital Assistant. A portable device that stores and organizes personal information, such as contact information, calendar, and notes.

Smartphone A mobile telephone that offers additional applications, such as PDA functions and email.

Peer-to-Peer (P2P) File Sharing: A distributed network of users who share files by directly connecting to the users' computers over the Internet rather than through a central server.

Private data*:* Data in the custody of the employee that does not concern the GIIF, its business and/or its relations (e.g., private address book, private mail).

Remote Desktop Access: Remote control software that allows users to connect to, interact with, and control a computer over the Internet just as if they were sitting in front of that computer.

Remote Access: The act of communicating with a computer or network from an off-site location. Often performed by home-based or traveling users to access documents, email, or other resources at a main site.

Remote Access VPN: A VPN implementation at the individual user level. Used to provide remote and traveling users secure network access.

RTO: Recovery Time Objective

Smart Card: A plastic card containing a computer chip capable of storing information, typically to prove the identity of the user. A card-reader is required to access the information.

Streaming Media: Information, typically audio and/or video, that can be heard or viewed as it is being delivered, which allows the user to start playing a clip before the entire download is complete.

SSID: Stands for Service Set Identifier the name that uniquely identifies a wireless network.

Split Tunnelling: A method of accessing a local network and a public network, such as the Internet, using the same connection.

Site-to-Site VPN: A VPN implemented between two static sites, often different locations of a business.

SFR: Strategy, Finance, and Risk Management

Token: A small hardware device used to access a computer or network.

Tokens are typically in the form of an electronic card or key fob with a regularly changing code on its screen.

Two-Factor Authentication: A means of authenticating a user that utilizes two methods: something the user has, and something the user knows. Examples are smart cards, tokens, or biometrics, in combination with a password.

Trojan: Also called a 'Trojan Horse.' An application that is disguised as something innocuous or legitimate but harbours a malicious payload. Trojans can be used to gain access covertly and remotely to a computer, log keystrokes, or perform other malicious or destructive acts.

Timeout: A technique that drops or closes a connection after a certain period of inactivity.

User: For the purposes of all Information Security Policies, a user is defined as anyone with authorized access to Company X's technology resources including permanent and temporary employees or third-party personnel such as temporaries, contractors, consultants, and other parties with valid Company X access accounts.

Uninterruptible Power Supplies (UPSs): A battery system that automatically provides power to electrical devices during a power outage for a certain period. Typically, also contains power surge protection.

Virus: Also called a 'Computer Virus.' A replicating application that attaches itself to other data, infecting files like how a virus infects cells. Viruses can be spread through email or via network-connected computers and file systems.

Virtual Private Network (VPN): A secure network implemented over an insecure medium, created by using encrypted tunnels for communication between endpoints.

WPA: Stands for Wi-Fi Protected Access. A security protocol for wireless networks that encrypts communications between the computer and the wireless access point. Newer and considered more secure than WEP.

Whole Disk Encryption: A method of encryption that encrypts all data on a particular drive or volume, including swap space and temporary files.

WEP: Stands for Wired Equivalency Privacy. A security protocol for wireless networks that encrypts communications between the computer and the wireless access point. WEP can be cryptographically broken with relative ease.

Wi-Fi: Short for Wireless Fidelity refers to networking protocols that are broadcast wirelessly using the 802.11 family of standards.

Wireless Access Point: A central device that broadcasts a wireless signal and allows for user connections. A wireless access point typically connects to a wired network.

Wireless NIC: A Network Interface Card (NIC) that connects to wireless, rather than wired, networks.

17. APPENDIX

APPENDIX A

EMPLOYEE CONFIRMATION AND ACCEPTANCE

I _____do hereby declare the following:

i. I understand the terms and conditions of GHANA INFRASTRUCTURE INVESTMENT FUND Computer Systems Usage Policy.
ii. I am sufficiently trained in the use of the GHANA INFRASTRUCTURE INVESTMENT FUND's computer systems to comply with the terms and conditions of this Policy.
iii. I am aware that I have no expectation of privacy in accordance with the terms and conditions of this Policy.
iv. I am aware that the terms and conditions of this Policy have the force and effect of GIIF rules, and that disciplinary action may be taken against me for violation of the terms and conditions of this Policy.
v. I am aware that any future amendments to this Policy document will form part of this Policy and will be binding.
vi. I undertake within five working days of signature of this policy to ensure that any software or data resident on my Personal Computer or Server, which is in breach of the terms and conditions of this Policy, is removed.

_____ _____

EMPLOYEE SIGNATURE DATE

APPENDIX B
Laptop Possession Form
SIGN THE PORTION BELOW, PHOTOCOPY THE PAGE AND SEND TO HR DEPARTMENT

LAPTOP POSSESSION DECLARATION
I have read, understood, and agreed to abide by the guidelines and rules set out in this document. I further accept that I will be held solely responsible for any use or misuse of the laptop and therefore accept any disciplinary action that may be taken against me in the case of misuse.

NAME……DATE……..

……

Signed……

…..……..

SUPERVISOR…….DATE…..……

……

Signed……

……..

GIIF Asset Code

…….

Laptop's serial Number…….

APPENDIX C
Application form for Staff e-mail / Internet

AN APPLICATION made this _____ of

_____by_____of the

_____ Department for E-mail and /or Internet Access through the

GHANA INFRASTRUCTURE INVESTMENT(GIIF)

I _____ hereby declare that:

i. I agree to adhere to GHANA INFRASTRUCTURE INVESTMENT FUND's usage policy attached hereto and confirm that I have read and understood the said documents as part and parcel of this Application.

ii. As an employee of GHANA INFRASTRUCTURE INVESTMENT FUND, I recognize and understand that the GHANA INFRASTRUCTURE INVESTMENT FUND's e-mail and Internet systems are to be used for conducting the GHANA INFRASTRUCTURE INVESTMENT FUND's business only.

iii. I am aware that GHANA INFRASTRUCTURE INVESTMENT FUND reserves and may exercise the right to review, audit, intercept, access, and disclose all matters on the GHANA INFRASTRUCTURE INVESTMENT FUND's e-mail and Internet systems at any time, with or without employee notice, and that such access may occur during or after working hours.

iv. I am aware that violations of this policy may subject me to disciplinary action in accordance with my Contract of Employment and GHANA INFRASTRUCTURE INVESTMENT FUND disciplinary code.

v. By signing this document, I agree to abide by E-mail / Internet policy, and to act according to its intention.

_____ _____

EMPLOYEE SIGNATURE DATE

APPENDIX D

Computer Network Access declaration form

Please be informed that, based on your current Job Description/Functions, you have been allocated network system access passwords: Please find below the General and System Specific security guidelines relating to the above passwords. If you have any queries, please get in touch with ICT department.

GENERAL SECURITY GUIDELINES

i. You are requested to change the above password(s) at your first sign-on. A standard feature of most of the above systems is that the system will force you to change the password after the first successful log-on.

ii. The above passwords give you access to confidential GIIF/customer data. Therefore, you must use it with due care. Avoid simple passwords that are easy to guess.

iii. Keep your password secret. Sharing of passwords (i.e., using another person's password) is strictly prohibited and anybody found carrying out this practice is liable for disciplinary action. Therefore, do NOT share your passwords with anybody else, even your staff colleague. Regarding passwords, you must mistrust anybody else other than yourself.

iv. You are solely responsible for the use or misuse of the above password(s). Therefore, if you give your password to someone else, every action logged under your password is presumed to have been performed by you and not that other person.

v. If in doubt consult IT. Only officially licensed software is to be loaded / used on the GIIF PC's and servers. Loading of unlicensed software is prohibited by the GIIF and is a criminal offence for which disciplinary action could be dismissal and possible criminal charges in a court of law.

vi. The GIIF's PC"s is to be used purely for GIIF business. Using GIIF systems/resources for personal work is strictly not allowed and perpetrators of this kind of action are liable for disciplinary action.

vii. Log off or lock your workstation whenever you leave your workplace.

viii. Shut down your PC after work.

APPENDIX E

GIIF SECURITY INCIDENT RESPONSE FORM

REPORTING FORM

DATE OF REPORT: DATE OF INCIDENT:

REPORTING PERSON:

LOCATION(S) OF INCIDENT:

SYSTEM(S) AFFECTED:

METHOD OF DETECTION:

NATURE OF INCIDENT:

INCIDENT DESCRIPTION:

ACTIONS TAKEN/RESOLUTION:

PERSONS NOTIFIED:

SIGN THE PORTION BELOW, PHOTOCOPY THE PAGE AND SEND TO IT DEPARTMENTS

COMPUTER SYSTEM ACCESS DECLARATION

I have read, understood, and agreed to abide by the guidelines and rules set out in this document. I further accept that I will be held solely responsible for any use or misuse of the above passwords(s) and therefore accept any disciplinary action that may be taken against me in the case of misuse.

_____ _____

EMPLOYEE SIGNATURE DATE

POLICY CONTROL

Authority to approve	Board
Authority to recommend to Board	Risk and Compliance Committee
Policy owner	IT Manager
Prepared By	IT Manager
Current version	2.0
Created date	July 2022
Approval date	25th July 2024
Due for review	30th June 2026

Version Control

Version	Revision Date	Author	Description
1.0	July 2022	IT Manager	Information Systems Policy
2.0	July, 2024	IT Manager	Information Systems Policy

……..

Manager, Information Technology (Policy Owner)