The State of Eritrea
Office of the Auditor General

Formatted: Centered, Indent: Left: 3"

Information Technology Policies

Version 3.0

March 2019

Foreword

This Information Technology Policy is a key document in guiding the members and guest users of the Office of the Auditor General (OAG) in the use of their OAG IT facilities.

The Office of the Auditor General has been supporting the development of requisite technological capacity for its auditors and corporate staff members as part of a wider structural building of the office. As a result, the office has invested enormous amount of money in providing its staff with necessary technological means that will support them in dealing with the day to day business endeavors.

This policy should be used along with other personal and professional ethics, IT environment and both civil and criminal legal requirements. Therefore, it is expected that all OAG staff shall strive to obtain an understanding of this policy and ensure compliance and implementation during the use of OAG IT facilities.

Commented [G1]:

Commented [G2]:

Commented [G3]:

Commented [G4]:

Commented [G5]:

_____

Auditor General
2019

Introduction

OAG information technology resources constitute valuable OAG assets that must be managed accordingly to ensure their integrity, security, and availability for learning, research and ~~the~~ its~~office's~~ business activities. To accomplish ~~accommodate~~ its mission, OAG requires ~~the office~~ to establish basic information security policies and standards and to provide both access and reasonable security at an acceptable level. The OAG Information Technology policies and controls are intended to facilitate and support authorized access to its~~the office's~~ information system.

Commented [G6]:

The purpose of the OAG Information Policy is:

- ~~•~~ To establish office-wide Protocol for Information Security.
- ~~•~~ To help identify and prevent the compromise of information security and the misuse of OAG information technology resources.
- ~~•~~ To protect the reputation of the office and ~~to~~ amplify~~allow~~ its ~~the office its~~ legal and ethical responsibilities with regard to its information technology resources.
- ~~•~~ To enable OAG ~~the office m~~Management to respond to complaints and queries about real or perceived non-compliance with the office's Information Technology Policies.

Formatted: Bulleted + Level: 1 + Aligned at: 0" + Indent at: 0.25"

Responsibility

Authorized users of OAG information technology resources are individually~~personally~~ responsible for complying with all OAG policies and standards relating to information security, regardless of the location of residence, head office or field, and will be held personally accountable for any misuse of these resources.

Communication

This document governs all IT systems administration of OAG. Authorized users of OAG IT facility, be it employees, students or guest users have both the right and an obligation to know the policy of OAG. Management has an obligation to communicate this policy to all authorized users including new recruits of the office. Any person who has been granted the right to use OAG IT facilities~~y~~ will automatically be an authorized user, and thus agrees to abide by this policy document.

Amendments

Proposals for amendments to this document may be submitted to the Information Communication Technology Division~~Systems Audit Division~~ for review. If the review results in the need to amend the Information Technology Policies, the IT personnel and systems administrator will draft the proposed amendment. The proposed amendment will be forwarded to the Information Technology Division. Upon consensus by that division, the proposed amendment will be forwarded to the Auditor General and if approved, will be included in the Information Technology Policies Manual.

Table of Contents

1. Unauthorized Use Policy

1. 1 Purpose.

This policy sets forth the OAG's policy regarding Unauthorized Use of the OAG Information Technology Network.

1.2. Scope.

This policy covers all Unauthorized Use of the OAG Information Technology Network, whether such Unauthorized Use is done by a person who is not an Authorized User, or by an Authorized User who exceeds the limits of that person's authorization whose use exceeds Authorized Use permitted by the OAG, all of whom are referred to in this policy as "Unauthorized Users."

1.3. Policy.

All Unauthorized Users are prohibited from using OAG Information Technology Network for any purpose whatsoever. Authorized Users are prohibited from using the OAG Information Technology Network in any way that exceeds the limits of their individual authorization.

1.4. Enforcement.

Unauthorized Users who are employees of the OAG may be subject to disciplinary action, up to and including termination of employment, statutory, legal or criminal actions. Unauthorized Users who are Students at the OAG may also be subject to disciplinary action, up to and including expulsion from the OAG training programs. Unauthorized Users whatsoever relationship might have with OAG may also be subject to statutory, legal or criminal actions.

2. Guest User Policy

2. 1 Purpose.

The OAG promotes sharing and learning within its community. In doing so, the OAG often grants to OAG guests and visitors the right to use its information technology resources in compliance with the OAG Information Technology Policies. Such authorized persons are Guest Users and are also Authorized Users to the extent of their authorization.

2.2. Scope.

This policy applies only to any Guest Users and does not include OAG staff.

2.3. Policy.

A Guest User is an Authorized User when utilizing the OAG's information technology resources in compliance with the OAG Information Technology Policies and as long as the use remains within the limits of the Guest User's individual authorization. The Guest User may be authorized to use computers in the OAG's computers pool and selected Software. The Guests may also be permitted to selected areas of the OAG's Information Technology Network.

2.4 Enforcement.

Any Authorized User found to be in violation of this policy will be considered an Unauthorized User, and as such are subject to disciplinary action pursuant with the Enforcement section of the Unauthorized Use Policy.

3. OAG Confidentiality Policy

3.1. Purpose.

Confidential information may be developed or obtained by OAG management, employee or stakeholder as a result of that person's relationship with the OAG. The purpose of this policy is to safeguard information from unauthorized users.

3.2. Scope.

Confidential information includes, but not limited to, the following types of information:

- Clients Audit files and documents
- Student and employee information, such as address, telephone number, birth date and other private information.
- Operations manuals, OAG practices, techniques and materials, development plans, and financial information
- Student or applicant lists, grades, personnel and payroll records, records and files of the OAG, and other information concerning the business affairs or operating practices of the OAG.

3.3. Policy.

All Authorized Users who have contact with and access to confidential information must keep such information confidential. Confidential information must never be released, removed from the OAG premises, copied, transmitted, or in any other way used by the Authorized User for any purpose outside the scope of their OAG employment, nor revealed to non-OAG employees, without the express written consent of OAG management.

Information stored on the OAG Information Technology Network is confidential and may not be distributed outside the OAG except in the course of the OAG's business guidelines or as otherwise authorized by management.

Authorized Users may not remove or borrow from the OAG premises any computer equipment, disks, or related technology, product or information unless authorized to do so.

3.4. Enforcement.

Any Authorized User found to be in violation of this policy will be considered an Unauthorized User, and as such are subject to disciplinary action pursuant with the Enforcement section of the Unauthorized Use Policy. In addition, Auditors who violate this policy will be liable with breach of confidentiality principles as stipulated in the professional code of ethics, fundamental principles.

4. Acceptable Use Policy

4.1. Overview.
Unauthorized uses expose the OAG to many risks including legal liability, Virus attacks, and the compromise of Network systems, Services, and information.

The OAG Information Technology Network includes:
Internet/Intranet/ related systems, including but not limited to computer/Networking equipment, Software, Operating Systems, storage media, network accounts providing electronic mail, Instant Messaging, which are the property of the OAG. They are to be used for OAG business purposes and to serve the interests of the OAG, and as well as all Authorized Users. Effective computer Security is a team effort requiring the participation and support of every OAG member, student and Authorized User who deals with information and/or information systems. It is the responsibility of every computer user to know the OAG Information Technology Policies and Procedures, and to comply with the OAG Information Technology Policies and Procedures.

Formatted: Font: Not Italic

4.2. Purpose.
This policy is intended to protect the OAG, as well as the OAG Students and employees from the consequences of illegal or damaging actions by individuals using the OAG Information Technology Network. This policy describes the Authorized Use of the OAG Information Technology Network and protects the OAG and Authorized Users.

4.3. Scope.

This policy applies to all persons who work with OAG-owned, third party-owned, or personally-owned computing device that is connected to the OAG Information Technology Network.

4.4 Policy

4.4.1 Specific Restrictions on Use.

The following categories of use are inappropriate and prohibited:

1. **Use that impedes, interferes with, impairs, or otherwise causes harm to the activities of others**. Users must not deny or interfere with or attempt to deny or interfere with service to other users in any way, including by "resource hogging," misusing mailing lists, propagating "chain letters" or virus hoaxes, "spamming" (spreading email or postings widely and without good purpose), or "bombing" (flooding an individual, group, or system with numerous or large email messages). Knowing or reckless distribution of unwanted mail or other unwanted messages is prohibited. Other behavior that may cause excessive network traffic or computing load is also prohibited.

2. **Use that is inconsistent with OAG's government body status**. The Office is a government body as such, is subject to specific government laws regarding the use of property, and similar matters. As a result, commercial use of IT Systems for non-office purposes is prohibited.

3. **Harassing or offending use**. Display of offensive, sexual, material in the workplace and repeated unwelcome contacts with another is strictly prohibited.

4. **Unethical use of IT systems**: Using OAG IT systems in recording, editing, storing or distributing media files including but not limited to music, movies and pornographic materials is strictly prohibited.

Formatted: Indent: Left: 0"

5. **Use damaging the integrity of OAG or other IT Systems**. This category includes, but is not limited to, the following six activities:

    a) **Attempts to defeat system security**. Users must not defeat or attempt to defeat any IT System's security – for example, by "cracking" or guessing and applying the identification or password of another User, or compromising room locks. (This provision does not prohibit, however, Systems Administrators from using security scan programs within the scope of their Systems Authority.)

    b) **Unauthorized access or use**. The office recognizes the importance of preserving the privacy of Users and data stored in IT systems. Users must honor this principle by neither seeking to obtain unauthorized access to IT Systems, nor permitting or assisting any others in doing the same. For example, a non-OAG organization or individual may not use IT Systems without specific authorization. Privately owned computers may be used, but such computers may not be used to access OAG network without specific authorization. Similarly, Users are prohibited from accessing or attempting to access data on IT Systems that they are not authorized to access.

    Furthermore, Users must not make or attempt to make any deliberate, unauthorized changes to data on an IT System.

    Users must not intercept or attempt to intercept or access data communications not intended for that user, for example, by "unethical" network monitoring.

    c) **Disguised use**. Users must not conceal their identity when using IT Systems, except when the option of anonymous access is explicitly authorized. Users are also prohibited from masked as or impersonating others or otherwise using a false identity.

    d) **Distributing computer viruses**. Users must not knowingly distribute or launch computer viruses, worms, or other rogue programs.

    e) **Modification or removal of data or equipment**. Without specific authorization, Users may not remove or modify any OAG-owned or administered equipment or data from IT Systems.

f) **Use of unauthorized devices.** Without specific authorization, Users must not physically or electronically attach any additional device (such as an external disk, printer, or video system) to IT Systems.

6. **Use in violation of law**. Illegal use of IT Systems that is, use in violation of civil or criminal law is prohibited.

7. **Use in violation of SAI policy**. Use in violation of other SAIs or other regional and international SAI organizations' policies also violate this Authorized Users Policy (AUP). Relevant SAI's policies include, but are not limited to, professional ethical standards and guidelines regarding incidental personal use of IT Systems.

8. **Use in violation of external data network policies**. Users must observe all applicable policies of external data networks when using such networks.

5. Electronic Communications Policy

1. Overview

Electronic communications systems that utilize the OAG Information Technology Network are not an open forum, but rather are owned and operated by the OAG to promote teaching and learning, and to conduct official OAG business. Authorized Users may use these systems only within the scope of OAG Information Technology Policies and Procedures. Electronic communication systems include, but are not limited to, all electronic mail and Instant Messaging systems, web content, and Internet access.

5.1 Personal Account Responsibility.

5.1.1 Purpose.

The purpose of this policy is to establish a standard for creation and protection of strong passwords for Authorized Users of information technology resources on the OAG information Technology Network. This policy will also establish the frequency of change for those passwords.

5.1.2. Scope.

The scope of this policy includes all Authorized Users who are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any OAG premises, accesses the OAG Information Technology Network, or stores any non-public OAG information.

5.1.3. Policy.

Users are responsible for maintaining the security of their own IT Systems accounts and passwords. Any User changes of password must follow published guidelines for passwords. Accounts and passwords are normally assigned to single Users and are not to be shared with any other person without authorization by the applicable Systems Administrator. Users are presumed to be responsible for any activity carried out under their IT Systems accounts.

5.2 Email and Communications Activities

5.2.1 Purpose.
The purpose of this policy is to establish a standard for Authorized OAG email account Users on the OAG information Technology Network.

5.2.2. Scope.
The scope of this policy includes all Authorized email Users on any system that resides at any OAG premises, using the OAG Information Technology Network. This policy however does not cover personal email accounts outside OAG's domain (examples are yahoo, Gmail, hotmail, etc).

5.2.3. Policy.
The use of e-mails is limited only for official purposes and not for personal gain.
Authorized User is not permitted to engage in any of the following activity

1. Sending unsolicited Email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (Email SPAM).

2. Any form of harassment via Email, instant messenger, through language, frequency, or size of messages.

4. Solicitation of Email for any other Email address, other than that of the Authorized User's own account, with the intent to harass or to collect replies.

5. Creating or forwarding Chain email, Phishing, or other scams of any type.

6. Use of the OAG's name in any unsolicited Email on behalf of, or to advertise, any service or product without the explicit written permission of the OAG.

7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup SPAM).

5.3 Use of internet

5.3.1 Purpose.
The purpose of this policy is to establish a standard for internet service by Authorized Users on the OAG information Technology Network to protect the security of OAG IT systems from Viruses, malicious programs, traffic overload and to protect the integrity of the office.

5.3.2. Scope.
The scope of this policy includes all Authorized internet Users on any IT system that resides at any OAG premises, using the OAG Information Technology Network.

5.3.3. Policy.
Internet should be used in accordance to OAG business purpose only. However the office also allows staff a reasonable use of internet for their private purpose, as long as users do not surf in malicious websites or put OAG network in compromise.

The following activities are prohibited without exception

- Staff should not download software from internet without prior approval from IT Personnel
- Unless contents are in line with OAG business, users are not allowed to download or share media files like music and movies, using OAG IT systems
- Display of offensive, sexual, material in the workplace and repeated unwelcome contacts with another
- The use of internet in violation of civil or criminal law

5. Enforcement.

Any Authorized User found to be in violation of this policy will be considered an Unauthorized User, and as such are subject to disciplinary action pursuant with the Enforcement section of the Unauthorized Use Policy

6. Physical Security Policy

6.1. Overview.

Physical Security means providing environmental safeguards for, and controlling physical access to, equipment and data on the OAG Information Technology Network in

order to protect information technology resources from unauthorized Use in terms of both physical Hardware and data perspectives.

6.2. Purpose.

The purpose of this policy is to establish standards for granting, monitoring, and terminating physical access to the OAG Information Technology Network and to protect equipment on the OAG Information Technology Network from environmental factors.

6.3. Scope.
This policy applies to the entire OAG Information Technology Network, including but not limited to computer labs, Network Closets, and the Information Technology Services Network Operations Center.

6.4. Policy.
OAG IT facility is strictly restricted from access by unauthorized users, and all IT operations center (network switches, servers etc) is restricted without exception from access besides staff whose job responsibilities require access to that facility.

6.5. Enforcement.

Any Authorized User found to be in violation of this policy will be considered an Unauthorized User, and as such are subject to disciplinary action pursuant with the Enforcement section of the Unauthorized Use Policy.

7. Workstation Configuration Security Policy

7.1. Purpose.

The purpose of this policy is to establish standards for the base configuration of workstations that are owned or operated by the OAG. Effective implementation of this policy will minimize unauthorized access to the OAG Information Technology Network and other Proprietary Information and technology.

7.2. Scope.

This policy applies to all OAG Information Technology Network workstation equipment owned or operated by the OAG, and to workstations registered under any OAG-owned internal Network domain.

7.3. Policy.

Ownership and Responsibilities

All OAG Information Technology Network workstations at the OAG must be the responsibility of an operational group that is responsible for system administration. Approved workstation configuration standards must be established and maintained by the operational group, based on business needs. The operational group must monitor configuration compliance and request special approval for any noted exceptions. The operational group must establish a process for changing the configuration standards, which includes review and approval by appropriate Information system personnel.

7.4. Enforcement.

Any Authorized User found to be in violation of this policy will be considered an Unauthorized User, and as such are subject to disciplinary action pursuant with the Enforcement section of the Unauthorized Use Policy

8. Computer Pool Security Policy

8.1. Purpose.

This policy establishes OAG Information Technology Network Information Security requirements for the OAG Computer pool, to ensure that confidential information and technologies are not compromised, and to ensure that audit Services and other OAG interests are protected from OAG computer pool activities.

8.2. Scope.

This policy applies to all OAG Computer pools, as well as all Authorized Users who use the OAG Computer pool. All existing and future equipment, which falls under the scope of this policy, must be configured in accordance with the following policy.

8.3. Policy.
OAG computer pool is designed for training purpose, thus the pool should not be part of the overall OAG network where the database and other confidential information is stored.

8.4. Enforcement.

Any Authorized User found to be in violation of this policy will be considered an

Unauthorized User, and as such are subject to disciplinary action pursuant with the Enforcement section of the Unauthorized Use Policy.

9. Change Management Policy

9.1. Purpose.

This policy describes a systematic process to document and manage changes to the OAG Information Technology Network in order to permit effective planning by the OAG information Technology Services to serve the OAG user-base.

9.2. Scope.

This policy applies to all Authorized Users that install, maintain, or operate OAG information technology resources, including, but not limited to: computer Hardware, Software, and Networking devices.

9.3. Policy.

Any change to any OAG Information Technology Network information technology resource is subject to this policy, and must be performed in compliance with the OAG's Change Management Procedure.

9.5. Enforcement.

Any Authorized User found to be in violation of this policy will be considered an Unauthorized User, and as such are subject to disciplinary action pursuant with the Enforcement section of the Unauthorized Use Policy.

10. Information Security Audit Policy

10.1. Purpose.

Information Security personnel utilize various methods to perform physical and electronic scans of the OAG's Networks and Firewalls, or on any system connected to the OAG Information Technology Network.

Information Security personnel are authorized to conduct audits to:

• Ensure integrity, confidentiality and availability of information and resources
• Investigate possible Security incidents
•Ensure compliance to OAG Information Technology Policies and Procedures documentation
• Monitor Authorized User or system activity where appropriate

10.2. Scope.

This policy covers all computer and communication devices owned or operated by the OAG. This policy also covers any computer and communications device that are connected to the OAG Information Technology Network, but which may not be owned or operated by the OAG. Information Security personnel will not perform Denial of Service or other disruptive activities.

10.3. Policy.

10.3.1 Authorization to Audit

Formatted: Font: Not Italic

Only Information Security personnel or other specifically authorized parties may audit devices that are owned by the OAG or are connected to the OAG Information Technology Network. Third-party organizations may only perform audits with the explicit written permission of the Information Technology Audit division.

10.3.2 Access

Formatted: Font: Not Italic

Information Security personnel shall be granted access to the following in order to effectively perform audits:

• User level or system level access to any computing or communications device
• Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on the OAG Information Technology Network
• Access to work areas (pool, offices, storage areas, etc.)
• Access to interactively monitor and Log traffic on the OAG Information Technology Network

10.4. Enforcement.

Any Authorized User found to be in violation of this policy will be considered an Unauthorized User, and as such are subject to disciplinary action pursuant with the Enforcement section of the Unauthorized Use Policy.

11. Information assets policy

11.1 Purpose
The purpose of this policy is to clarify the logical management of data and information stored in OAG IT systems.

11.2 Scope
Information in OAG is classified as:

1. Regular Audit Information which includes financial, compliance and performance audits
2. Fraud investigation Audit information
3. Administrative information
4. Other information

This policy governs all information which is part of, or stored in the OAG IT systems.

11.3 Policy:
Regardless of the source, OAG has the right of ownership for any information stored in OAG IT systems. Authorized OAG staff users may not have access to information outside their authorized limit. The degree of information disclosures to third parties will be decided only by top management.

OAG staff shall not use removable devices such as flash disks as storage media for information owned by the OAG.

11.5. Enforcement.

Any Authorized User found to be in violation of this policy will be considered an Unauthorized User, and as such are subject to disciplinary action pursuant with the Enforcement section of the Unauthorized Use Policy.

12. IT Purchasing/procuring?, Maintenance and Disposal Policy

12.1 IT purchasing policy (Procuring)??

12.1. 1 Purpose

The purpose of this policy is to have a clear procedure of IT equipment purchasing/procuring?, maintenance or disposal procedure to protect the office from acquiring, or maintaining unwanted and untimely or low quality equipments.

12.1.2. Scope.

This policy covers all purchases related to Information technology which includes but is not limited to hardware, software, storage media and related accessories, which are acquired through OAG budget, be it recurrent or project budget. The MoF "Procurement Procedures and Pproperty Aadministration" guidelines may override this policy.

12.1.3. Policy.

Subject to the MoF "Procurement Procedures and Pproperty Aadministration", the Finance and Administration head has the authority to approve the purchase of any computer hardware, software or related items using the office's budget after IT steering committee has approved the technical details. There is no need approval of the AG?

12.1.5. Enforcement.

Any Authorized User found to be in violation of this policy will be considered an Unauthorized User, and as such are subject to disciplinary action pursuant with the Enforcement section of the Unauthorized Use Policy.

12.2 IT Maintenance
Any IT facility, which may require maintenance, should be referred to OAG IT personnel only. Exposing OAG IT facilities to any external IT experts with-out prior authorization of the systems administrator is strictly prohibited. In certain circumstances where OAG IT personnel do not have the necessary knowledge for certain areas of IT management, the office might contract some of the IT functions.

12.3 IT disposal policy

Any IT facility or part damaged, replaced or whatsoever can only be disposed in accordance to the disposal procedures as specified in the rules and regulations in property management of MoF, after prior approval is gained from the IT administrator or IT steering committee.

13. IT Management Policy

13.1. ICTS ~~Audit~~ Division
13.1.1Purpose:

Formatted: Font: Not Italic

The purpose of this policy is to promote sound and effective IT governance in OAG by establishing proper IT management mechanism in the office.

13.1.2 Scope

OAG IT Audit division is a key component in the IT governance process, since it provide the strategic alignment required to fulfill the Office's goals and objectives. The division has~~is~~ a mechanism to ensure that the IT function is in harmony with the OAG mission and goals as set out in the strategic plan.

13.1.3 Policy

ICT~~T audit~~ division is delegated to review and propose for approval of major acquisitions and major IT projects in OAG. For day to day management of the IT systems and IT audit assignments, the division will use the two units under its administration.

Roles and responsibilities

Some of the basic functions which will be performed by the ICT division typically will include:

- Ensure alignment of IT strategy with the Office's strategy;
- Enhance the understanding and satisfaction with the value of IT investment;
- Promote two way communications between audit and IT.
- Review and propose for approval of major acquisitions;
- Review and propose for approval of major IT projects;
- Review and approval of plans to outsource IT maintenance activities
- Review adequacy and allocation of resources;
- Make decisions with other IT related activities

13.2 ICT HR Management

13.2.1 Purpose

The purpose of this policy is to ensure sufficient IT skills and clear responsibility of IT personnel in the unit.?????

13.2.2 Scope

The scope of this policy is limited within the general "Civil Service Administration" guidelines of the state.????

13.2.3 Policy

IT human resources should have a minimum of three members in each unit or at least one IT professional for every 30 staff members of the OAG, whichever is higher. The Job description of each member should be specified and needs to be properly documented. IT personnel should get sufficient training in their area of expertise to deal with the daily development of technological change.

Formatted: Font: Not Italic

Formatted: Font: Not Italic

Formatted: Font color: Red

14. IT Plans Policy

14.1 Purpose

As IT has a rapid change, proper IT governance needs up to date plans which is flexible to address the rapid technological change in IT systems. The purpose of this Policy is to ensure an Information Technology Infrastructure that promotes the basic missions? of OAG: auditing, training, and administration by safeguarding the office from technological obsolescence that may hinder its basic missions.

Formatted: Font color: Red

14.2 Scope:

IT plans are part of overall strategic and operational plans of OAG. The policy can only address the plans that are designed in the overall strategic plan of the office.

14.3 Policy

14.3.1 IT Strategic plan

The OAG is functioningrunning based on the strategic plan of 2019-2023. Once the office agrees on the future direction for IT, the decisions should be formalized and documented in a plan. The future direction should be agreed by the Auditor General. The IT strategy document is in effect the starting point for any investment in IT as it identifies future changes which have to be budgeted for.

14.3.2 IT operational plan

The operational plans must support the strategic plans to ensure that the organization achieves the objectives defined in the strategic plans.

3.1.1 OAG should have a maximum of 1 year operational plan for IT
3.1.2 The IT operational plan should be drafted by the IT division
3.1.3 The IT operational plan should be in line with the IT strategic plan of OAG.
3.1.4 IT strategic plan should be revisitedsed at least bi-annually and should be documented properly

15. Disaster Recovery Policy

15.1 Purpose

The purpose of this policy is to ensure continuous operations of OAG, where there is a disaster that may be a threat to the operations of The Office. Disasters can be terminal

such as fire and earthquake or it can be mild that can temporarily disrupt the day to day operations of The Office.

15.2 Scope:
This policy will address all electronic operations, which includes audit files and programs, finance and administration files, official emails etc.

15.3 Policy

15.3.1 Disaster Recovery Plan: Disaster recovery plans must be documented and reviewed, and should be updated to address for any change that may be introduced in due course.

15.3.2 On-site archives: Information and files should be archived on a weekly basis and backup media should be retained, in a fireproof safe, on-site for operational use.

15.3.3 Off-site archives: Backup media will be periodically updated by IT personnel and on a monthly basis should be stored at a suitable off-site location.

15.3.4 Prioritization of files: information and files produced by each user will be prioritized by OAG management to determine the priority and sensitivity of each file, and the site of archiving.

Appendix A: Defined Terms

1. ***Access Control***: The prevention of Unauthorized Use of a resource, including the prevention of use of a resource in an unauthorized manner.

2 ***Authorized Use***: The use of the OAG Information Technology Network by any person who is authorized to do so by the OAG within the limits of that person's authorization, and as described in and permitted by the OAG Information Technology Policies.

3 ***Authorized User(s)***: Person(s) authorized by the OAG to use the OAG Information Technology Network including but not limited to Departments, staff, Students, and guests, within the limits of such person's authorization.

4 Backup: The process of periodically copying all of the files on a computer's disks onto a magnetic tape or other removable medium.

5 ***Chain Email:*** A term used to describe Emails that encourage you to forward them on to someone else.

6 ***Change Management***: The process of developing a planned approach to change in an organization.

7 ***Denial of Service (DoS***): An attack on a computer system or Network that causes a loss of Service to users, typically the loss of Network connectivity and Services by overloading the computational resources of the victim system.

8 ***Email***: The electronic transmission of information through a mail Protocol such as SMTP.

9. ***Firewall:*** A piece of Hardware or Software which functions in a Networked environment to prevent some communications forbidden by the Network policy. It has the basic task of preventing intrusion from a connected Network device into other Networked devices.

10. ***Forwarded Email***: Email explicitly redirected from one account to another.

11. ***Guest User***: Any visitors to the OAG, not including staff, or Students who are properly authorized to use the OAG Information Technology Network.

12. ***Hardware:*** The physical, touchable, material parts of a computer or other system. The term is used to distinguish these fixed parts of a system from the more changeable Software or data components which it executes, stores, or carries.

13. ***Host:*** Any computing device attached to a computer Network.

14. ***Information Security***: Information Security is the part of Information Technology Services that is responsible for coordinating and overseeing office wide compliance with OAG policies and procedures regarding the confidentiality, integrity, and Security of its information assets.

15. ***Instant Messaging***: An on-line communication Service in which conversations happen in real-time and the "on-line status" between users is conveyed such as if a contact is actively using the computer.

16***. Internet:*** The publicly available worldwide system of interconnected computer Networks.

17. ***Internet Protocol (IP) Address***: A unique number used by machines (usually computers) to refer to each other when sending information through the Internet.

18***. Intranet***: An Intranet is a Network used internally in an organization.

19. ***Log***: A chronological record of system activities to enable the reconstruction and examination of the sequence of events and/or changes in an event (also known as an audit trail).

20. ***Malicious Software (malware):*** Any Software developed for the purpose of doing harm to a computer system.

21. ***Mass Emailing***: An Email that is sent to a group of individuals.

22. ***Network:*** A system for communication among two or more computers.

23. ***Network Closet:*** A physically-secured room where production network devices reside.

24. ***Network Drive***: A computer storage medium accessible from a Network connection.

25. ***Network Sniffing:*** The act of watching Internet Protocol packets as they traverse a local Network.

26***. Operating System (OS):*** The system Software responsible for the direct control and management of Hardware and basic system operations, as well as running application Software.

27. ***Program***: See Software.

28. ***Scanning***: Checking for Services presented on Networks, usually as part of a Cracking attempt or computer Security scan.

29. ***Security:*** The term "Security" is used in the sense of minimizing the Vulnerabilities of assets and resources.

30. ***Security Audit***: This function provides monitoring and collection of information about Security-related actions, and subsequent analysis of the information to review Security Policies, controls and procedures.

31. ***Security Policy***: A policy is a document that outlines specific requirements or rules that must be met.

32. ***Security Standard***: A standard is a collection of system-specific or procedural-specific requirements that must be met by everyone.

33. ***Sensitive Information***: Information is considered sensitive if it can be damaging to OAG or its reputation.

34. ***Service***: Work performed (or offered) by a server.

35. ***Software:*** A loadable set of instructions which determines how the computer will operate autonomously or in reaction to user input, when running.

36. ***SPAM:*** Unauthorized or unsolicited electronic mailings.

37. ***Student(s)***: Person(s) enrolled in at least ACCA class of the OAG.

38. ***Surge Protector***: An appliance designed to protect electrical devices from power surges.

39. ***Threat***: A potential violation of Security.

40. ***Traffic Flooding***: To send an excessive amount of traffic to information technology resource, causing a Denial of Service attack.

41. ***Trojan Horse***: Malicious Software that is disguised as legitimate Software.

42. ***Unauthorized Disclosure***: The intentional or unintentional revealing of restricted information to people, both inside and outside the OAG, who are not authorized to know that information.

43. ***Unauthorized Use***: Use of the OAG Network by Unauthorized Users in violation of the law or in violation of the OAG Information Security Policies and Procedures.

44. ***Unauthorized User***s: Use of the OAG Network who are not Authorized Users, or use of the OAG Information Technology Network in violation of the law or in violation of the OAG Information Technology Policies and Procedures.

45. ***Uninterrupted Power Supplies (UPS):*** A device or system that maintains a continuous supply of electric power.

46. ***OAG:*** Office of the Auditor General of Eritrea

47. ***OAG Change Management System***: System that manages the approval process for any modifications to the OAG Information Technology Network, and that stores documentation for each modification.

48. ***OAG Password Management System***: System that stores and manages passwords on the OAG Information Technology Network for all system-level and user-level accounts.

49. ***OAG Security Management System***: System that stores information about the OAG Information Technology Network, including but not limited to contact information, Hardware, and Software (for every part of it).

50. ***OAG Information Technology Policies***: Policies of the OAG that govern the use of the OAG Information Technology Network, as from time to time amended, all as approved by the Steering committee delegates.

51. ***OAG Computer pool*** : Collection of publicly accessible OAG computers that are connected to the OAG Information Technology Network, from which Authorized Users can access the OAG Information Technology Network.

52. ***OAG Data:*** Data that belongs to the OAG that is entered into the OAG Information Technology Network by OAG and other Authorized Users.

53. ***OAG Employees***: Persons employed by the OAG including Audit departments and administration division

.

54. ***User Authentication***: A method by which the user of a system can be verified as a legitimate user independent of the system being used.

55. ***Virus:*** A self-replicating Program that spreads by inserting copies of itself into other Programs or documents.

56. ***Vulnerability***: Any weakness that could be exploited to violate a system or the information it contains.

57. ***Wireless Networks***: Telephone or computer Networks that use radio as their carrier or physical layer.

58. ***Worm:*** A self-replicating Program that is self-contained and does not need to be part of another Program to propagate itself.