Reviewed by: Mr. Zewdu Ayele	**Approved by: Mrs. Meseret Tessema**
Position: Quality Manager	**Position: Director General**
Signature:	**Signature:**

Table of Contents

1. Purpose

1.1. EAS has a policy to safeguard the security of its ICT infrastructure as a priority to prevent organizational work interruption or loss of important Organizational information. EAS recognizes its dependence on Computer systems, secure data storage and reliable electronic communications. EAS also has regulatory obligations, including the need to retain office and other records of Accreditation outputs.

1.2. EAS uses its IT resources to support total quality assurance of accreditation processes which conform to EAS's document control regulations.

1.3. EAS's ICT systems conform to the requirements of National Information Technology Policy.

1.4. Where feasible EAS's policy is to use up-to-date technology, equipment and software in order that it can deliver high quality, innovative products and support customers with Electronic customer service system.

1.5. EAS complies with the requirements of the Data Protection rules

2. Scope

This policy applies to all individuals working at all levels and grades, including all Directors, managers, Process owners, Team leaders, assessors, employees (whether permanent, fixed-term or temporary),consultants, contractors, trainees, second staff, and agency staff, volunteers, or any other person visiting our premises, wherever located (collectively referred to as workers in this policy).

3. Introduction

All EAS employees and users of EAS's computer systems are personally responsible for the protection of information and computing assets, particularly in the areas of confidentiality, integrity and availability.

Compliance with this Policy is mandatory and will help to protect important office assets such as information, records and the supporting ICT infrastructure, and to minimize the prospect of fraud and loss.

4. Duty and Responsibility

IT head is basically responsible for implementation of this policy

4.1. IT Department and Users

4.2. You must ensure that you read, understand and comply with this policy.

4.3. Any employee who violate this policy will face disciplinary action, as rule and regulation of national information policy.

4.4. Any employee who is issued with a password is responsible for the safeguarding of their password.

5. Software Upgrades & Servicing

The Office intends to keep all IT equipment updated to safeguard the effectiveness of its IT systems and security of data. Laptops and PCs require periodic upgrading (at least once per annum) and must be made available for such purpose at a time to be mutually agreed with the ICT Service Department.

6. Abuse of Equipment

The following are prohibited on the Office's computers and computer system:

- Alterations and upgrades to any Office software or documents without authorization.
- Accessing or attempting to access any area of, or data on the computer system and on modification of programme or data without prior authorization from the specified person(s).
- Copying exceptional data or programme for personal use.
- Using privately acquired programme or data on any portable data storage format, for example, CD-ROMs, DVDs, USB memory sticks or internet downloads on Office machines without prior authorization ICT service Department.
- Using Office computer for unlawful activities such as harassment or the dissemination of offensive/obscene material, pornography, threats or insulting statements.

- Installing, copying, distributing or using proprietary software in violation of copyright or any licensing agreement.
- Loading software, including games on to Office machines without prior authorization of ICT service Department.
- Unauthorized use or exposing of information relating to the computer system including prohibition on exposing passwords or access codes.
- Carrying sensitive Office information off site on a laptop without prior authorization or without ensuring a back-up has been made.

7. Internet, E-mail and Social Media

7.1. The Office's computer system contains an e-mail facility, which is intended to promote effective communication on matters relating to office works. All such communications must be sent from the office domain Office's email address, (xyz@EAS-eth.org) to internal or external recipients. Improper use of e-mail or the Internet may result in disciplinary action being taken.

7.2. The office retains the right to monitor any and all aspects of its computer system, including reviewing e-mail sent and received **using office email(**incase some information miss-use happened which could put the office on unwanted risk). This can be done without the permission of employees.

E-mail has become a common and convenient means for private communication. As it is quicker, cheaper and less disruptive than using the telephone, it is acceptable as a method of private and personal communication, provided such use is not excessive and does not improperly interrupt the working day.

7.3. Sending "**flame mail**" - messages which are abusive, offensive, bullying or which could constitute harassment - is prohibited. Because e-mail is quick to compile and dispatch, messages are sometimes sent without appropriate thought being given to the content, leading to misinterpretation and unintentional offence.

7.4. **Internet access** is provided on the basis of duties need; however employees may access the Internet for personal use during lunch breaks and out of working hours on the following basis:

- Internet access for personal use during working hours is strictly prohibited.
- You may not use the Office's Internet resources for commercial or personal advertisements or solicitations.
- You may not download software onto the computer network without full and proper authorization
- You may not access, forward or store pornographic or other offensive material.
- You should be aware that access to the Internet may be monitored without your permission; anyone who accesses sites which could be deemed offensive, whether to view, download or upload material, lays himself or herself open to disciplinary action.
- You may not copy or store Office information onto virtual data storage systems without prior authorization, for example, cloud based repositories such as Drop box.

7.5. You are responsible for the **security of your computer** terminal and/or any portable electronic communication device, such as laptop computer, digital cameras or cell phones issued to you by the office.

- You must not allow any terminal or communication device to be used by an unauthorized person.
- You should therefore keep your personal password confidential and change it regularly. When leaving your terminal or device unattended you should Password locks your device or on leaving the office, you should ensure you log off the computer network system to prevent unauthorized users using your terminal in your absence.

7.6. Should you receive an email message, which has been **wrongly delivered** to your email address, you should notify the sender of the message by re-directing the message to that person.

Further, in the event the e-mail message contains confidential information, you must not disclose or use that confidential information.

- Should you receive an e-mail which contravenes this policy, the e-mail should be brought to the attention of your ICT Service.

7.7. EAS recognizes the benefits of taking part in **socialnetworks** and online communities such as **blogs, wikis, social networking websites, podcasts**, forums, message boards, or comments on web-articles, such as **Twitter**, **Face book**, **LinkedIn**, and etc. If you are using social media, the best advice is to approach the online world in the same way as the physical one – use sound judgment and common sense.

- Online comments and posts are public and permanent, even with privacy settings in place. Try to ensure posts are accurate, not misleading or damaging and be careful to not to reveal sensitive or confidential office information. If you are not sure, don't post it.
- Website user feeding EAS's websites with up-to-date information are responsible and expected to fill the prepared form of communication by ICT Directorate in an ethical and responsible manner, and must be signed by Director General of EAS. If this is not completed, the website service will not be delivered.
- Website user(s) or an employee maintaining EAS's websites are responsible & expected to keep information on websites up-to-date with events (Meetings, trainings, awards, and occasions) held at times with great responsibility in the form of news release, upload pictures & videos, and other graphics.

Mentioning EAS in a derogatory way or otherwise damaging its reputation may result in disciplinary action being taken.

8. General Computer User Responsibilities (Principles)

1. Computer users are responsible for adhering to the most current version of this Policy and for meeting published information technology standards, guidelines and other related policies and documents.
2. Computer users are responsible for maintaining personal awareness of EAS policies. Ignorance of policy does not absolve computer users of responsibility for compliance.

3. Where issues have not been specifically addressed by this Policy, all EAS personnel and computer users must use prudent judgment to determine whether actions would be contrary to EAS's business interests.
4. A violation of this Policy may result in disciplinary action being taken against the computer user.
5. All computer users must take responsibility for their actions and must be held personally accountable for the consequences of their actions.
6. Computer users are responsible for any use of their account. A user must not share account details or passwords.
7. Computer users must ensure, to the best of their ability, the confidentiality and integrity of information and systems.
8. Computer users must protect information, systems and infrastructure against damage or unauthorized access.
9. Computer users must not download, install or run security programs or utilities that reveal or exploit weaknesses in the security of a system. For example, EAS users must not run password cracking programs, packet sniffers, or port scanners or any other non-approved programs on EAS IT resources
10. Computer users may access only information that they are authorized to access.
11. Computer users must not use EAS information technology assets, including electronic messaging and Internet systems, for private commercial purposes or monetary gain, or unauthorized advertising or political lobbying.
12. Computer users must not use EAS information technology assets, including electronic messaging and Internet systems, to:

- Knowingly infringe the copyright or other intellectual property rights of EAS or third parties;
- Send or forward items likely to be covered by copyright or other intellectual property rights;
- Download , store, distribute or promote defamatory, fraudulent or harassing material and files;
- Download, store, distribute or access or play games;

- Download or store items such as mp3's or **non-work**-related video files.
- Download, store, distribute, promote or encourage threatening, harassing, insulting, sexist or racist material;
- Download, store, distribute or access pornographic, obscene or suggestive material; or
- Engage in other antisocial behavior.

13. Computer users must promptly report to the ICT Directorate all breaches of information systems security, whether actual or suspected.
14. Computer users must not change or disable security protection such as virus checking software.
15. Proposals and business cases must consider IT security when IT assets are being developed, enhanced and maintained
16. Computer users must not be granted access to EAS's computer and electronic messaging systems unless and until they have read and agreed to abide by both this Policy and related Policies. Acceptance of these policies is required by EAS's conditions of employment for staff, contractors and consultants. All new computer users accessing the EAS computer and electronic messaging systems must sign an IT security confidentiality agreement as a condition of employment.
17. Employee(s) shall sign an electronic attendance management system to ensure its presence to on hour including shit employees
18. Any absence or presence shall only be confirmed from biometric attendance management system
19. Any Employee can check its **login** results from biometric door lock administrator in case there is complain
20. Concerned Department(s) shall provide official information regarding training or an event o around accreditation for the update of social media /website/news.
21. Reports from CCTV Camera regarding security are acceptable for any disciplinary action or feedback.
22. All **new computer users** accessing the EAS computer and electronic messaging systems

must sign an IT security confidentiality agreement as a condition of employment.

23. Computer user access to information and IT applications will be permitted subject to:

- Approval by the ICT Directorate responsible for the data and the application, and also subject to organizational risk profiles;
- Access being granted to named individuals not to groups or organizations;

9. Disciplinary Actions

1.1. Violation may result in a denial of access to Office IT resources, and those disciplinary actions provided or authorized by the Rules and Regulations of the country (information policy) via ICT Directorate or Human Resource Directorates.

1.2. Computer users (Employees) shall use social media (8.7) for personal purposes at their own time (should not abide office working time).

1.3. All the computer and internet users shall know that the social media (URLs) might be down at working time if its surveyed and found abiding office work. (www.fb.com ……)

1.4. An employee shall give a finger print signature for ensuring its present on its regular working place and a signature which is not registered to the Biometric finger attendance management system is not recognized by the HR Directorate unless confirmed by respective department.

1.5. An employee shall know and use effectively the camera surveillance system of the office for better security of office resources as well as individual resource while in the office.

1.6. An employee who did not get access to Biometric finger print time management system for more than 7 consecutive days might be denied for using the system unless claimed by his/her Directorate with tangible evidence.

Note: Any user who permits an external employee to get access to inter the office compound at off time shall have responsibility.

10. Risks Identified

We have identified that the following are particular risks for our office**:**

- Temporary outage of critical IT systems and networks

- Introduction of malicious computer viruses
- Non-authorized access to our computer systems, data and intellectual property
- Loss or corruption of critical Office data and records
- Failure of electronic communication systems, e.g. email
- Failure of auto mated system and control systems for electronic equipment.

11. Training and Implementation of the Policy

11.1. This policy is added to EAS policy documents and addresses as of EAS policy.

11.2. Management will ensure that all information, instruction, training and leadership necessary to ensure appropriate IT systems and equipment are provided for all employees that need them for their work. Training on IT equipment and software must be part of employee induction for new employees and for employees that are moving to a new work place or role. Training on IT will be provided to employees when systems are changed or updated and at regular intervals to keep employees skills up to date.

12. Monitoring and Review

This policy(if necessary) will be reviewed for continued suitability at least annually by the EAS ICT professional cooperatively with other concerned bodies and presented at the annual Management Review Meeting and any recommendations for changes made to the IT Audit, Document control and other concerned bodies of the office.

IT Audit will be done every three months by ICT Directorate and the changes will be implemented as per the policy.

Every change on EAS's website and social medias will be monitored every month by Deputy Director General.

Revision No.	Date approved	Revision History
1.1	2021-05-11	It is reviewed according to EAS template Purpose and scope added
1.2	2022-05-09	The document is revised due to the name Ethiopian National Accreditation Office (ENAO) change to Ethiopian Accreditation Service (EAS) and new logo developed
1.3	2023-02-07	• Correction done on page 1 that, this document was prepared by Meseret Tessema replaced by Zewdu Ayele (new quality manager). • Former director general was resigned and replaced by Mrs. Meseret Tessema.