Table of Contents

Forward by the Director General

Information technology has become ubiquitous and vital to the success of almost every enterprise. Significant changes have occurred in the generation, storage and usage of information with a profound impact on work, social interaction, education and governance. For most organisations, information, and the tools used to manipulate it, have become important assets, the effective use of which are essential to organizational success. However, this reliance on information technology also means that data and systems must be protected from threats that may result in financial loss or reputational damage.

As the lead agency in the implementation of the ECOWAS Monetary Cooperation Programme, WAMA is committed to the highest standards of rigor in its contributions to the technical, policy, statistical, institutional and legal work required for creating the conditions for achieving economic and monetary union in ECOWAS. In this regard, the Agency has a responsibility to ensure that its systems and information are used effectively for the benefit of the Agency, meet highest standards of integrity and availability and minimise the risk of financial loss or reputational damage.

This Information Technology Policies and Procedures manual outlines the policies and procedures for defining the processes, accountabilities, roles and responsibilities necessary to deliver reliable and sustainable IT services to the Agency. I expect that all members of staff shall familiarise themselves with it and comply with its provisions.

Momodou Bamba Saho
Director General

Section 1. Introduction

The West African Monetary Agency (WAMA) Information Technology (IT) Policy and Procedures Manual details the policies and procedures for defining the processes, accountabilities, roles and responsibilities necessary to deliver reliable and sustainable IT services to the Agency.

The Agency will keep all IT policies current and relevant. Therefore, from time to time, it will be necessary to update and amend some sections of these policies and procedures, or add new policies and procedures.

These policies and procedures shall apply to all employees of the Agency.

Section 2. Hardware Acquisition Policy

2.1 Purpose of the Policy: This policy provides guidelines for the acquisition of hardware for the Agency to ensure fit for purpose, value for money and where appropriate, compatibility with other hardware used by the Agency. The purpose of this policy is to minimize the differences in the hardware used by the Agency.

2.2 Purchase of Hardware: The purchase of all desktops, servers, portable computers, computer peripherals and mobile devices must adhere to this policy. The server systems, desktop computer systems, portable computer systems and computer peripherals purchased must run the Windows operating system and integrate with existing hardware and software. Any change from the above requirements must be authorized by the Head of IT Unit. Professional staff members will be given a choice of a desktop or a laptop machine. All purchases of hardware must be consistent with the requirements of the Financial Rules and Regulations.

The IT Unit will request quotes from vendors, manage the equipment purchase and install and support the new hardware. Computer hardware that is not acquired officially by the Agency shall not be supported. Due to licensing and warranty restrictions, the IT Unit shall not install Agency-owned software on non-approved hardware. The IT Unit shall not also be responsible for repairs to such devices.

2.3 Relocation of Hardware: Except for mobile computer equipment allocated to the staff, employees may not remove hardware from the Agency or transfer equipment to other locations within the Agency without approval of the Head of IT. Prior to an asset being moved, the employee and/or his/her supervisor responsible for the asset shall contact the IT Unit to advise of the move. Only IT staff responsible for hardware shall be allowed to move hardware equipment from their current location to a new location.

2.4 User Responsibility for Hardware: Users shall avoid subjecting PCs to excessive vibration or bumps. Hard jolts while a PC is running can damage the hard disk drive. Smoke, heat, magnetic fields, and excessive dust can also damage LAN equipment. All PCs should be connected to a surge protector.

Section 3. Software Acquisition Policy

3.1 Purpose of the Policy: Unauthorized software programs, even those seemingly provided by reputable vendors and trusted companies, can introduce viruses and Trojan programs that aid hackers' attempts to illegally obtain sensitive, proprietary and confidential data. Protecting the Agency's computers, systems, data and communications from unauthorized access and guarding against data loss is of paramount importance.

Allowing employees to install software on Agency computing devices opens the Agency to the risk of conflicting file versions or DLLs which can prevent programs from running, the introduction of malware from infected software, copyright violations due to unlicensed software and programs which can be used to hack the Agency's network. These risks require associated policies.

3.2 Purchase of Software: All software shall be purchased by the Head of IT Unit. All purchases of software must be from reputable vendors and be supported by the necessary warranties and be compatible with the Agency's server and other computing systems. All purchases of software shall comply with the provisions of the Financial Rules and Regulations. The budget for new software acquisitions must include the cost of the software as well as associated costs such as installation, training, updates, third-party products that may be necessary for the operation of the software and cost of any specialized hardware or equipment that is required.

In the event that open source or freeware software is required, approval from the Head of IT Unit must be obtained prior to the download or use of such software. All open source or freeware software must be compatible with the Agency's hardware and software systems. Any change in the above requirements must be authorized by the Head of IT Unit.

3.3 Software Development: The IT Unit may function as advisors or participate in software development projects as project managers or provide technical resources as available or undertake the development, if there is capacity to do so. No User department shall engage contractors to design and develop systems without due consultation and consent of the Head of IT Unit and the Director General.

3.3 Software Licensing

3.3.1 No software shall be installed on the Agency's equipment without proper licenses or other forms of authorization from the copyright owner. The unauthorized acquisition, duplication or use of software copies is prohibited. Any employee who acquires, copies or uses unauthorized copies of software on the Agency's computing equipment shall be subject to disciplinary action. Privately owned software shall not be included in the list of approved software for employees. Where an employee is aware of a breach of the use of software in accordance with this policy, they must notify the Head of IT Unit immediately.

3.3.2 The IT Unit shall reserve the right to refuse to install any software application when there are questions about the legality of the software. The Head of the IT Unit shall keep a repository of approved software which he/she shall compare to any software installation request.

3.3.3 The IT Unit shall reserve the right to refuse service and/or disconnect any system that does not adhere to this policy.

3.3.4 Where an employee is aware of a breach of the use of software in accordance with this policy, they are obliged to notify the Head of IT Unit immediately. In the event that the breach is not reported and it is determined that an employee failed to report the breach, then that employee shall be subject to disciplinary action.

3.3.5 The Head of IT Unit is responsible for performing a software audit of the entire Agency's systems twice a year to ensure that software copyrights and license agreements are complied with.

3.4 *Software Installation*:

3.4.1 Only assigned staff in the IT Unit shall install software applications in the Agency's computer systems. This includes Agency-owned laptops and other portable computing devices under the control of staff members. Under no circumstances shall software be installed or copied by any other employee. The IT Unit shall reserve the right to uninstall any unapproved software.

3.4.2 Staff members shall obtain approval from the Head of the IT Unit for installation of job-specific software.

3.4.3 Only software obtained in accordance with this policy shall be installed on the Agency's computers.

3.4.4 All software shall be registered with the copyright owner where this is a requirement. WAMA shall be the registered owner of all software.

Section 4: Information Technology Security Policy

4.1 Purpose of the Policy: This policy provides guidelines for the protection and use of information technology assets and resources within the Agency. The wide range of information available on the Agency network, as well as on the Internet, and the nature and risks associated with the use of the Internet raises concerns about security, integrity, confidentiality, monitoring and proper use of Agency information. Failure to adequately secure information opens the Agency to reputational and financial risks.

This policy provides the guiding principles and details responsibilities necessary to safeguard the integrity, confidentiality and availability of the Agency's information systems and to mitigate risks related with theft, loss, misuse or damage to those systems.

4.2 Physical Access

4.2.1 Physical access privileges to all Agency server rooms, data centers and offsite backup facilities must be documented and managed by the Head of IT Unit. He/she shall keep a visitor register for logging the movement of employees and contractors, to and from the Agency's IT facilities. The visitors register should be reviewed regularly by the Head of IT Unit.

4.2.2 Access to restricted server rooms, data centers and offsite backup facilities shall only be granted to employees whose job responsibilities require access to those facilities.

4.2.3 The process of granting key access to server rooms, data centers or backup sites must include approval from the Head of IT Unit.

4.2.4 Secured access devices such as keys, access cards or lock combinations must not be shared with or loaned to others by authorized users.

4.2.5 Lost or stolen keys and access cards must be reported to the Head of IT Unit immediately.

4.2.6 All server rooms, data centers and backup facilities must be kept locked when not occupied by an authorized staff person.

4.2.7 The Head of IT Unit must review card and or key access rights for the IT facilities on a periodic basis and remove access for individuals that no longer require access.

4.3 Environmental Controls

4.3.1 Adequate air conditioning, fire extinguisers and humidifiers must be installed, operative and maintained in order to prevent long-term heat damage and equipment failure.

4.3.2 All network equipment and systems in network facilities must be connected to an uninterrupted power supply in order to prevent power spikes, brownouts, and subsequent damage to data, software and hardware.

4.4 Information Security

4.4.1 All data held in the Agency's network systems is to be backed-up. It is the responsibility of the Head of IT Unit to ensure that data backups are conducted and that the backed up data is kept in a secure location.

4.4.2 Data held and managed locally in departments and units is excluded unless departments and units have entered into specific arrangements with the IT Unit. All members of staff are reminded that they are individually responsible for safeguarding data held locally on their desktop or laptop computers and are strongly encouraged to perform backups of all personal files on a regular basis. Employees are also reminded that the information they produce in the course of their work is the property of the Agency and that all sensitive and valuable data must be stored on the Agency network.

4.4.3 Full backups of all Agency data are to be performed weekly. Full backups are retained for three months before being overwritten.

4.4.4 Incremental backups of all Agency data shall be performed daily. The incremental backups are retained for one month before being overwritten.

4.4.5 Backups should be stored in a secure offsite facility for disaster recovery purposes.

4.4.6 The Head of IT Unit is responsible for testing data restore procedures and ensuring that they work.

4.4.7 All Agency equipment must have anti-virus software installed. It is the responsibility of the Head of IT Unit to install all anti-virus software and ensure that the software remains up to date.

4.4.8 The Agency shall prepare a Business Continuity Plan that will be implemented and tested at least twice a year to provide an effective solution that can be used to recover critical business processes within the quickest possible time using data stored on its off-site backup facility. The Director General is responsible for putting this into effect.

4.5 User Identification Codes and Passwords

4.5.1 Every employee shall be issued with a unique user identification code to allow access to the Agency's computer equipment and shall be required to set a password for access every six months. The user identification code must conform to a standard naming convention as determined by the Agency.

4.5.2 All passwords should be reasonably complex and difficult for unauthorized persons to guess. Employees should choose passwords that are at least eight characters long and contain a combination of upper and lower case letters, numbers, and punctuation marks and other special characters. No default passwords shall be allowed on any system or device.

4.5.3 Employees shall not share their passwords with other employees. Where there is a need for several employees to share a single password, for instance those working collaboratively on a project, approval must be obtained from the Head of the IT Unit.

4.5.4 The Head of IT Unit is responsible for issuing the user identification code and the initial password for all employees. This initial password must be changed as quickly as possible by the employee.

4.5.5 Employees should take steps to avoid phishing scams and other attempts by hackers to steal passwords and other sensitive information. All employees will receive training on how to recognize these attacks.

4.5.6 Where an employee forgets his/her password or is “locked out” of the systems because of previous failed attempts to login, the Head of IT Unit has responsibility to reissue a new initial password after a formal application by the staff member. The staff member shall be required to change the password when he/she logs in using the new initial password.

4.6 Intrusion Detection

4.6.1 The IT Unit shall implement processes for operating systems, user accounting and software audit logging on all host and server systems.

4.6.2 The It Unit shall implement alert functions for firewalls and other network perimeter access controls.

4.6.3 Audit logging of firewalls and other network perimeter access controls and logs must be reviewed daily from the perimeter access control systems.

4.6.4 The IT Unit shall review audit logs for servers and hosts on the internal, protected network at least once per week.

4.6.5 The IT Unit shall check host-based intrusion tools at least once per week and shall review trouble reports for symptoms that might indicate intrusive activity or an incident.

4.6.6 The IT Unit shall work with heads of department and unit to train employees to report anomalies in system performance and signs of wrongdoing to the Head of the IT Unit.

4.7 Information Classification

All Agency information and all information obtained from third parties fall into one of four classifications shown below:

4.7.1 Public: This is information that has been approved for publication and should be accessible to all members of the public. This includes annual reports, bulletins, economic reviews, brochures and other publications available on the Agency's website.

4.7.2 Internal Use: This refers to information normally accessible only to WAMA staff whose disclosure outside the Agency would be inappropriate. Examples include internal correspondence, task force, working group and committee papers, meeting minutes, training materials, data from Member Central Banks. This information would normally not be marked, but should be treated with care at all times and not disclosed, without authority, to third parties.

4.7.3 Restricted: Such information is normally accessible only to specified members of staff who have a legitimate need to see it. This includes senior management meeting minutes, some personal staff data,

4.7.4 Confidential: This is information accessible only to specified members of staff. This may be applied to information where loss or disclosure would result in damaging consequences for the Agency. It should be subject to the highest levels of confidentiality, integrity and restricted availability. This includes administrator passwords, sensitive correspondence, proceedings of the Committee of Governors and legal correspondence, pre-release publications, personal staff data.

There is no need to label public or internal use information. However, restricted and confidential information should be marked by the heads of department/unit responsible for the information.

Section 5. Internet Use

5.1 Purpose of the Policy: The purpose of the policy is to define the appropriate uses of the Internet by employees of the Agency. All employees using the WAMA IT network to access the Internet shall adhere strictly to guidelines concerning appropriate use of network resources.

5.2 Disclaimer of liability for use of the Internet: WAMA is not responsible for any material viewed or downloaded by employees from the Internet. The Internet is a worldwide network of computers that contains millions of pages of information. Users are cautioned that many of these pages include offensive, sexually explicit and inappropriate material. In general, it is difficult to avoid at least some contact with this material while using the internet. Even harmless or inoffensive search requests may lead to sites with highly offensive content. Employees giving out their personal information (including email addresses) on the Internet do so at their own risk.

5.3 Employees' Duty of Care: WAMA employees shall endeavor to make each electronic communication truthful and accurate. They should use the same care in drafting email and other electronic documents as they would any other written communications. Employees should keep in mind that anything created or stored on the Agency's computer systems may, and will likely, be viewed by the Agency.

5.4 No expectation of Privacy: The computing equipment and accounts given to employees are to assist them in the performance of their duties. Employees should not have an expectation of privacy in anything they create, store, send or receive on the Agency computer systems. The Agency may monitor messages without prior notice.

5.5 Blocking of inappropriate content: The Agency may use software to identify offensive or sexually explicit Internet sites. Such sites may be blocked from access by the Agency. In the event staff encounter offensive or sexually explicit material while browsing the Internet, he or she should immediately disconnect from the site regardless of whether the site was subject to Agency blocking or not.

5.6 Prohibited Activities: The Agency email system shall not to be used for the creation, distribution, downloading, viewing or storage of any disruptive or offensive messages, including offensive comments about race, gender, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any WAMA employee should immediately report the incident to the Head of IT Unit.

5.7 Games and Entertainment Software: Employees shall not use the Agency's Internet facilities to download games or any other entertainment software. Employees shall not play games over the Internet during working hours.

5.8 Illegal Copying: Employees shall not illegally copy material protected under copyright law or make that material available to others for copying. Employees are responsible for complying with copyright law and applicable licenses that may apply to software, files, images, documents, messages and other material they download or copy. Staff should not license or download any material for which a registration fee is charged without first obtaining the express written permission of the Agency.

5.9 Accessing the Internet: To ensure security and avoid the spread of viruses, employees accessing the Internet through equipment attached to the Agency's network must do so through an approved Internet firewall. By-passing the Agency's firewall is strictly prohibited.

5.10 Virus Detection: Files downloaded from sources outside the Agency, including from discs from home, email attachments, files downloaded from the Internet, social media, newsgroups, or other online services and files provided by customers and vendors, may contain dangerous computer viruses that may damage the Agency's network. Employees shall not download files from the Internet, accept email attachments from outsiders, or use disks from non-Agency sources, without first scanning the material with the Agency's approved anti-virus checking software. Any suspicions that a virus has been introduced into the Agency's network shall be brought to the attention of the Head of IT Unit.

5.11 Acceptable Personal Use: WAMA computer systems are for business use. However, when certain criteria are met, employees may use the internet for personal activities on a limited basis. All personal internet use through the WAMA network are subject to the following restrictions:

i. It must not degrade or otherwise impede normal job performance.
ii. It must not incur direct costs to WAMA.
iii. Since use of WAMA equipment and facilities may be perceived by others to represent WAMA, employees must not use the internet for any purpose that could reflect negatively on the Agency or its employees.
iv. Personal opinions expressed over the course of online communications activities should include a disclaimer that they do not reflect official positions of the Agency.
v. Personal use of the Agency's internet facilities is restricted to approved users and does not extend to family members or other acquaintances.
vi. No files or documents may be sent or received that may cause legal liability for, or embarrassment to WAMA.

5.12 Unacceptable use of the Internet: Employees shall not use WAMA internet either during working hours or on personal time, to:

i. Access, retrieve, or print text and graphics information that violate the Acceptable Use Policy
ii. Engage in unlawful activities or other activities that could in any way discredit the Agency.
iii. Engage in personal commercial activities, including offering services or merchandise for sale, non-business-related online purchasing, and personal commercial advertising.
iv. Engage in any activity that would compromise the security of systems, resources or networks.
v. Engage in any fundraising activity, endorse any product or services, participate in any lobbying activity, or engage in any active political activity.
vi. Access or transmit sexually explicit material.

5.13 Security: WAMA employees who identify or perceive an actual or suspected security problem shall immediately contact the IT Unit. WAMA employees shall not reveal their account passwords to others or allow any other person, employee or not, to use their accounts. Similarly, employees shall not use other employees' accounts.

Employees shall not attempt to circumvent or subvert security measures on either the WAMA network or any other system connected to or accessible through the internet.

Access to WAMA network resources shall be revoked for any user identified as a security risk or who has a demonstrated history of security problems.

5.14 Breach: Any employee violating these policies or applicable local laws while using the WAMA network shall be subject to loss of network privileges and any other disciplinary actions deemed appropriate.

Section 6. Email Policy

6.1 Purpose of the Policy: Email is extensively used in the Agency and is often the primary means of communication with stakeholders. However, misuse of email can post legal, privacy and security risks. Thus it is important for employees to understand the appropriate use of email. The purpose of this email policy is to ensure the proper use of email systems and make employees aware of what is acceptable and unacceptable use of the Agency email system. This policy outlines the minimum requirements for use of email within the Agency.

6.2 No Expectation of Privacy: Email privacy cannot be guaranteed. For security reasons, messages transmitted through the WAMA email system or network infrastructure are the property of WAMA and can therefore, be inspected by the Agency as warranted.

6.3 Acceptable use of email:

6.3.1 WAMA employees are not permitted to forward confidential business email or attachments to personal accounts managed by public email or internet service providers where the information might be compromised.

6.3.2 WAMA employees may make incidental personal use of email. Any incidental use may not interfere with official duties, must have a minimal effect on the Agency and must be consistent with the WAMA Code of Conduct for Staff.

6.3.3 WAMA employees shall not send, forward, receive or store confidential or sensitive official information utilizing non-WAMA accredited mobile devices. Examples of mobile devices include, but are not limited to laptops, smartphones, tablets etc.

6.4 Unacceptable use of email: The WAMA email facilities shall not be used to:

i. Send email intended to intimidate or harass.
ii. Conduct personal business.
iii. Conduct political lobbying or campaigning.
iv. Violate copyright laws by inappropriately distributing protected works.
v. Systems users shall not pose as anyone other than themselves when sending email, except when authorized to send messages for another employee when serving in an administrative support role.
vi. Send messages that carry malicious, provocative, ethnical, racial discrimination or other profane content.

To prevent unnecessary disruption or degradation of network communications and the efficient operations of email systems, employees shall not:

i. Send or forward chain letters.
ii. Send unsolicited messages to large groups, except as required when conducting official business.
iii. Send or forward email that is likely to contain viruses.

6.5 Email Security:

6.5.1 All inbound and outbound email shall be scanned for viruses and other malicious content.

6.5.2 Content scanning software shall be in place to block any inbound or outbound email messages that carry provocative, ethnical, racial discrimination or other profane content. The content filter shall be reviewed and updated quarterly.

6.5.3 Certain file attachments (with extensions such as .EXE, .HTML and other files with suspicious extensions) in email messages shall be forbidden and/or explicitly blocked by content scanning/end point protection software.

6.6 Standard Footers for Email: This footer should be appended to all email sent outside the Agency in respect of any confidential information relating to the Agency.

"This email and other files transmitted with it are confidential and are intended solely for the use of the individual or entity to which they are addressed. If you are not the intended recipient, be advised that you have received this email in error and that any use, dissemination, forwarding, printing or copying of this email is strictly prohibited. If you have received this email in error, please immediately notify the West African Monetary Agency by email address…………………. and delete it from your system."

Section 7. Website Policy

7 .1 Purpose of the Policy: Businesses, government agencies and individuals all over the world are using the Internet as a mass media tool to communicate with their stakeholders. Given the role of the Agency in leading the monetary integration process in West Africa, it is important that our stakeholders get the latest information about the activities of the Agency via the Agency website. This policy provides guidelines to ensure that timely and accurate content is posted to the Agency website. It also details the responsibilities for providing and amending content for the website.

7.2 Guiding Principles

7.2.1 Accuracy. The Agency website is an official source of information related to the ECOWAS monetary integration project. Its contents would be relied upon by member central banks, governments, ECOWAS citizens and other stakeholders in the conduct of their own activities. Therefore, the contents on the website should be accurate and properly verified before publication.

7 .2.3 Timeliness. It is important that the contents of the website are as up to date as possible in order to be of much use. Therefore, the content of the website shall be updated regularly.

7.2.4 Bilingual support. The content of the website should be available in both English and French.

7.2.5 Image: The Agency website must have a uniform look to ensure a consistent and cohesive image for the Agency.

7.3 Website Register:

7.3.1 The website register shall record, as a minimum, the following details:

i. List of domain names registered to the Agency

ii. Dates of renewal for domain names
iii. List of hosting service providers
iv. Expiry dates of hosting

7.3.2 Keeping the register up to date will be the responsibility of the Head of IT Unit. The Head of IT Unit shall also be responsible for any renewal of items listed in the register.

Website content: All content on the Agency website must be accurate, appropriate and current. This will be the joint responsibility of the Senior Management team. The following persons are authorized to make changes to the Agency website:

i. The Director General
ii. Head of the IT Unit
iii. Heads of Department and Units on information related to their functions

Section 8. IT Service Agreements Policy

8.1 Purpose of the Policy: This policy provides guidelines for all IT service agreements entered into with external service providers on behalf of the Agency.

8.2 Types of IT Service Agreement: The following IT service agreements can be entered into on behalf of the Agency:

- Provision of general IT services
- Provision of network hardware and software
- Repairs and maintenance of IT equipment
- Provision of business software
- Provision of mobile phones and data plans
- Website design and maintenance

8.3 Review and Approval Responsibilities

8.3.1 All IT service agreements must be reviewed by Head of IT Unit and the Agency’s legal adviser before the agreement is entered into. Once the agreement has been reviewed and recommendation for execution, the agreement shall be approved by the Director General.

8.3.2 All IT service agreements, obligations and renewals must be recorded in a register kept for the purpose by the Head of IT Unit.

8.3.3 Where an IT service agreement renewal is required, in the event that the agreement is substantially unchanged from the previous agreement, then this agreement renewal can be authorized by Head of IT Unit.

8.3.4 Where an IT service agreement renewal is required, in the event that the agreement has substantially changed from the previous agreement, it should first be reviewed by the Head of It Unit and the Agency's legal adviser before the renewal is entered into. Once the agreement has been reviewed and recommendation for execution received, then the agreement shall be approved by the Director General.

8.3.5 In the event that there is a dispute to the provision of IT services covered by an IT service agreement, it must be referred to the Director General who will be responsible for the settlement of such dispute.

INFORMATION TECHNOLOGY POLICIES AND PROCEDURES ACKNOWLEDGMENT FORM

After reading this policy, please sign the coverage form and submit it to Agency's IT Unit for filing. By signing below, the individual requesting access to the Agency's computing resources hereby acknowledges receipt of and compliance with the Information Technology Policies and Procedures. Furthermore, the undersigned also acknowledges that he/she has read and understands this policy before signing this form. Access to the Agency's network resources will not be granted until this acknowledgment form is signed by the individual's head of department or unit. After completion, the form is filed in the employee's human resources file (for permanent employees), or in a folder specifically dedicated to network access (for contract workers, etc.), and maintained by the IT Unit. These acknowledgment forms are subject to internal audit.

ACKNOWLEDGMENT
I have read the Information Technology Policies and Procedures. I understand the contents, and I agree to comply with the said Policy.

Name ____

Signature ____Date ___________________

Head of Department/Unit Signature ________________________Date ___________