NAO Information Technology (IT) Policy Document

Presented by: Alieu Jaiteh & Seringe Saine

Version 1.0

Date Approved: 15th/04/2020

Contents

Version Control

Date	Version	Author	Comments
February 28, 2020	Draft	IT Support Unit	Formulate an up to date ICT policy as required in NAO 2020 strategic priorities
March 13th, 2020	Revised Draft	Senior Management	Draft policy revised comprehensively and subjected to change in future to match our ICT operating environment
	2.0		

I. Introduction

The purpose of the IT Policy is to ensure the effective protection and proper usage of the computer systems in National Audit Office (NAO). The IT investment of the institution is considerable, and the dependency on computer technology in the delivery of NAO services is high. The IT Policy shall assist in maintaining systems at operation level. Violations of the IT Policy could seriously disrupt the operation of NAO therefore any breaches shall be treated seriously.

In the absence of a solid network, essential access to information may be lost or delayed. This can cause a severe breakdown in operations, negatively affecting productivity. Therefore, proper implementation of formal policies and procedures are an effective tool for management. When the procedures and policies are implemented properly, all the effort of the employees is geared towards accomplishing the objectives of the organization, and the result of every employee's work in NAO is predictable and can be easily managed.

II. Computer Systems

A. Local Area Network (LAN)

1. Network management, administration and maintenance within NAO are the responsibility of the IT Support Unit.
2. Network points are segmented for easy management – The network sockets label "D" are use as data point and network sockets label "T" are used for voice points.
3. All computer systems are to be assigned DHCP IPs from the DHCP Server pool.
4. NAO network is setup with VLANs, not all network points have access to internal resources.
5. Access to and usage of the Servers is restricted to authorized staff only.
6. Personal or other network devices not belonging to NAO shall not be connected to the LAN without prior written authorization from head of IT Support Unit.
7. It is prohibited to use personal routers or switches to be connected on the NAO network for the purpose of extending connectivity to nonofficial devices.
8. All computers own by the National Audit Office remain the property of the NAO and should only be used for National Audit business. Any inappropriate deviation from this could result in disciplinary action being taken against the culprit.
9. Equipment holders are not permitted to transfer their IT assets to another staff of the National Audit Office without the completion of the appropriate

forms supplied by IT Support Unit and the IT asset storekeeper must be made aware.

10. Eating and drinking tea or any form of liquid beside computer system should be avoided

B. Hardware (PCs, Laptops, Printers, etc)

1. The requirement for IT equipment shall normally be identified within the context of an IT strategy and budget for NAO and more specifically within a planned programme of computer equipment replacement.
2. The recommendation for purchase, installation, configuration and maintenance of computer equipment are the responsibility of the IT Support Unit.
3. Computer equipment registers shall be maintained by the IT Support Unit to ensure full tracking of equipment.
4. Requirements for new hardware shall be discussed in advance with the IT Support Unit to assess the detailed specification.
5. The deployment of new equipment or re-deployment of existing equipment is undertaken by the IT Support Unit after consultation with senior management.
6. Equipment holders must present mobile assets such as laptops and tablets to their IT asset storekeeper for auditing purposes within one week of request. Equipment may be audited at any time.
7. The relocation of hardware within or outside NAO premises shall be discussed with the IT Support Unit in advance to ensure good reason for relocation, determine the most appropriate means of relocation and to ensure computer equipment registers are updated.
8. The security and safekeeping of portable and other equipment used outside NAO offices is the responsibility of the member of staff using it. Loss/Damage of portable or other equipment outside of NAO Offices shall be reported through Department Head to Admin/HR. Admin/HR shall use necessary General Security Guidelines to recover equipment or register loss and advise IT Support Unit to remove from inventory register if necessary.
9. All staff are responsible for the proper usage, care and cleanliness of the computer equipment they use. Directors shall ensure that staff maintains the cleanliness of their machines.
10. Personal computer holders must make every effort to ensure that the equipment marking is not damaged or destroyed whilst in their care.
11. Report to the IT Support Unit any equipment which is damaged or not working.
12. Staff members are expected to protect Office laptops from damage and theft.
13. Problems with hardware shall be promptly reported to the IT Support Unit.

14. The IT Support Unit shall ensure that users are aware of any restrictions and limitations on the usage of computer systems of NAO.

15. Users or Visitors bringing or taking out IT Equipment such as PCs, Laptops and Printers which are not the property of NAO shall follow the appropriate administrative procedures to register the item with Security and/or Head of Unit.

16. Users shall not connect external devices such as USB drives and external Hard Drives to computer equipment without prior written approval from their Head of Department.

17. Staff members will not be held responsible for computer problems resulting from regular office-related use; however, a staff member will be held personally responsible for any problems caused by their negligence as determined by the management.

18. Staff members will provide access to any laptop computer, equipment, and/or accessories they have been assigned, upon request from management.

19. Any employee found to have violated this policy may be subject to disciplinary action.

C. Software & Software Applications

1. The requirement for new software shall normally be identified within the context of an IT strategy for NAO and more specifically within a planned software upgrade programme.
2. The recommendation for purchase, installation, configuration and support of all software and software applications used within NAO are the responsibility of the IT Support Unit.
3. Software, including tool bars, must not be installed by users without prior authorization from the IT Support Unit. This includes programs downloaded from the Internet.
4. Software registers shall be maintained by the IT Support Unit to ensure compliance with the IT Policy of NAO.
5. Requirements for new software/software applications shall be discussed in advance with the head of IT to assess the detailed specification and implications.
6. Problems with software shall be promptly reported to the IT Support Unit.
7. Request for modifications, enhancements and upgrades of existing software applications shall be discussed with the head of IT in consultation with senior management.

D. Data/Electronic Information

1. Department Heads are responsible for maintaining the quality of the computer-held data processed by their staff.
2. Department Heads are responsible for ensuring compliance with Data protection regulations with regards to data processed within their Departments. The IT Support Unit shall keep abreast of data protection regulations, advice accordingly and ensure applications and databases are structured in accordance with the internal organizational data management policies.
3. All information/data held on the institution's systems is deemed the property of NAO.
4. All staff are required to consent to the examination of the use and content of all data/information processed and/or stored by the staff member on the institution's systems as required.
5. None official data found to be stored in any NAO's system without knowledge of IT Support Unit or not due procedure as per this policy will be removed immediately and other necessary measures will follow.
6. Users shall not store personal files or media content to the institution servers or computer systems unless they relate to one's work.
7. Users shall not copy information or data from institution's servers or systems to external devices such as USB drives or to external systems on the Internet without prior written approval from their Head of Department.

E. Back up Systems

1. The IT Support Unit is responsible for ensuring the implementation of an effective back-up strategy for server-held software and data.
2. All staffs shall avoid storing data on their local hard drives. Data stored may be lost if a problem develops with the PC, and the IT Support Unit may not be able to assist in its recovery. Data shall be stored in users' profile and frequently copied to their map network drive.
3. Remote and laptop PC users must ensure they backup their data regularly. The IT Support Unit shall provide advice and assistance where required.
4. The IT Support Unit in consultation with senior management should ensure disaster recovery site is setup and maintain for secure off-site data backups.

F. Anti-Virus Protection

1. The IT Support Unit is responsible for the implementation of an effective virus security strategy. All machines, network servers and standalone, shall have license and up-to-date anti-virus protection.
2. The installation of anti-virus software on all machines is the responsibility of the IT Support Unit.
3. Remote users and users of portable machines shall comply in the upgrade of anti-virus software in accordance with specified mechanisms agreed with the IT Support Unit, e.g. Internet updates.
4. Staff shall virus-scan all media (including flash drives and CDs) before first use. The IT Support Unit shall help in providing training where required.
5. On detection of a virus, staff shall notify the IT Support Unit who shall provide aid.
6. Under no circumstances shall staff attempt to disable or interfere with the virus scanning software.

G. Removable media policy

This policy aims to ensure that the use of removable media devices is controlled in order to:

1. Enable the correct data to be made available where it is required.
2. Maintain the integrity of the data.
3. Prevent unintended or deliberate consequences of disruption to the stability of National Audit Office's computer network.
4. Build confidence and trust in the data that is being shared between systems.
5. Maintain high standards of care in ensuring the security of Protected and Restricted information.
6. Prohibit the disclosure of information as may be necessary by law.

III. PBX (IP Phone) Systems

A. Allocation of IP Phones

1. NAO PBX system is a core business application. It shall not be used for business or commercial purposes not related to NAO.
2. The requirement for an IP Phone shall have to be identified by the Department Head. Request for new IP Phones shall be discussed in advance with the Head of IT to assess detail requirement.
3. Staff members are responsible for the security of the IP Phone assigned to them. Secret pins are given to phones that can dial outside phone numbers. Staff members are responsible for the security of their pin which they shall not divulge even to colleagues.
4. Abuse of access to dial outside line shall be considered a serious offence. Minor abuse shall lead to removal of the privilege to dial out. Serious cases where the phone bill is exceedingly high, staff member shall be liable to pay for all nonofficial calls.
5. Senior management shall decide allocation of phones to individuals or team members with advice from IT Support Unit.

B. Class of Services Assignment (COS)

1. Department Heads shall be given access on their IP Phones to call all Phone services within the country.
2. Request for access to call international lines shall be discussed in advance with the Senior management for Department Heads to assess the need.
3. Receptionist will be allocated phone and external call facilities base on the advice from AG or Senior management.
4. In the case that a member of staff needs to call all phone networks within the country or international number, Their Department Head shall discuss in advance with the AG to assess the needs.

IV. E-mail Systems

A. E-mail address Assignment

1. The NAO e-mail system is a core business application. It shall not be used for political, business or commercial purposes not related to NAO.
2. The Admin Department shall inform the IT Support Unit of new members of staff so that email accounts shall be created for them.
3. The Admin Department shall also notify the IT Support Unit to disable Email account of staff(s) no more in service of NAO.
4. New NAO email address is to be created base on the first letter of the name and surname of the member of staff i.e. asaine@nao.gm [Alieu Saine]
5. In the case two staff members share the same name and surname the middle name of one of the staff members shall be use with their new email accounts.
6. Limited personal use of email could be allowed in case the official email server is down. Directors shall ensure there is no abuse of this privilege.
7. All staff members shall consent to the examination of the use and content of their email accounts as required.
8. Staff shall minimize the number of messages in their email in-box to ensure maximum efficiency of the delivery system. Folders shall be setup and messages filed accordingly.
9. Staff shall utilize the archiving facility within the Email system.
10. Confidential material sent by e-mail shall be so marked but sent only with caution.
10. E-mail signatures shall be provided to all staff members by the IT Support Unit to be used when sending official emails.
11. NAO retains the right to access and view all Emails sent and received by the Email system. This right is exercised solely through the IT Support Unit on the instructions of a Department Head in consultation with the Auditor General (AG).
12. 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) is prohibited.
13. Staff shall use their official email in their work-related communication, however the use of personal email to send mail.
14. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages is prohibited.
15. Unauthorized use, or forging, of email header information is criminal.
16. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

17. Use of unsolicited email originating from within NAO's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by NAO or connected via NAO's network.

B. Global Distribution List (groups)

1. Global distribution lists shall be used appropriately. Email to all staff (spamming) shall be used only when appropriate.
2. Global distribution lists shall be created for the entire department to enable easy information sharing within departments and a global list for all members of staff shall be used to send relevant information to everyone.
3. Requirement for new distribution list shall be discussed in advance with the head of IT to assess the need.

C. Mail Client vs. Webmail

1. Staff members are advice to use mail clients on their PCs if they are the only one using the assigned PC.
2. Users that share a single computer shall use the Round cube web client to access their emails.

D. E-mail Backup

1. The IT Support Unit is responsible for ensuring the implementation of an effective back-up strategy for Round cube web clients.
2. Staff using the mail client should ensure a weekly backup is taken and stored in the NAO server and IT support can be contacted for any needed help in this process.
3. All email backups shall be saved at the NAO Server systems. If any staff member wishes to keep his/her own backup, it is his/her responsibility to make available the backup in case of problem with the PC.

V. Internet Usage

A. Access to the Internet

1. The use of National Audit Office's Internet and e-mail systems is intended for National Audit Office's business including research by staff, communication, and professional development within the broad business objectives of the Office.
2. NAO retains the right to monitor Internet usage by staff and this right is solely exercise by the IT staff. There is a monitoring system in place that keeps track of your browsing history and records of all visited web sites. Employers must know that they are using public network and hence there is no guarantee for personal privacy data transmission. This monitoring tool is primarily setup to monitor internet bandwidth consumption and it's abuse by staff.
3. Staff shall not make inappropriate use of their access to the Internet. They must not use NAO systems to access pornographic, illegal or other improper material.
4. Programs including movies, music, must not be downloaded from the Internet without authorization from the IT Support Unit.

5. It is a condition that all staff consent to the examination of the use and content of their Internet activity as required in ***section A*** and ***sub bullet number 2*** above.
6. Abuse of Internet access shall be dealt with severely proportionately to seriousness. Minor abuse shall lead to removal of the privilege of access from an individual's workstation.
7. No employee should use the office internet facilities knowingly to download or distribute pirated software or data. The use of file swapping software on NAO computers and networks is prohibited.
8. Each employee using the Internet facilities of NAO's shall identify himself or herself honestly, accurately and completely (including one's company affiliation and function where requested) when participating in chats or newsgroups, or when setting up accounts on outside computer systems.
9. No employee should use NAO's Internet facilities knowingly to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.

B. Accessing Social sites

1. Staff shall not subscribe to chat rooms, dating agencies, messaging services or other on-line subscription Internet sites unless they pertain to work duties.
2. NAO has implemented a proxy server to block selected sites during working hours. Staff members shall not try to circumvent the blocked sites as any individual caught accessing these sites during the time, they are blocked will be escalated to senior management for necessary action to be taken.

C. Proxy

1. All NAO internal internet access shall pass through the NAO proxy Server systems.
2. NAO proxy System is an essential part of the IT strategy of the corporation. Staff shall not attempt to by-pass the proxy settings.
3. The proxy server systems shall be used to monitor, filter and limit the access the use of the internet not relating to NAO.

VI. Computer Users

A. User Accounts

1. Department heads in consultation with Admin shall notify the IT Support Unit of new members of staff in advance to allow the creation of network and e-mail accounts and system permissions.
2. Department heads shall notify the IT Support Unit of the departure of staff to allow the deletion of network and e-mail accounts.
3. All computer systems shall be added to the NAO domains except if required otherwise.
4. All system users on desktop PCs shall be given user accounts with limited privileges unless otherwise requested by their Department heads.

B. Passwords

1. The IT Support Unit shall ensure pass-wording is part of the security strategy of NAO IT system.
2. Users shall change their passwords when prompted by the system in the case of networked machines or on monthly basis for standalone machines.
3. Staff are responsible for the security of their password which they shall not divulge, even to colleagues.
4. Problems with passwords shall be reported to the IT Support Unit.
5. The password to be use in NAO computer system must be at least eight character long with alpha numeric, combination of upper and lower.
6. All personal computers of NAO shall be set for 5 minutes of idle timeout upon logon
7. Passwords of NAO computer systems must be set to expire in one month, and last five old passwords should not be used.

C. System Usage

1. Users shall ensure their computers are fully shut down and turned off at the end of day.
2. Computers shall be locked or shut down when left unattended for any significant period.
3. With regards to file management, Department Managers shall determine the top-level folders/directories and associated permissions for their department and inform the IT Support Unit. The IT Support Unit shall create or modify the folders accordingly.

D. Health & Safety

1. Health and safety with regards to computer equipment and computer workstations shall be managed within the context of the general and any specific Health & Safety policies and procedures within NAO.

2. Heads of units are responsible for ensuring health & safety regulation and procedures with regards to computer equipment are implemented within their Departments.
3. The head of IT support unit shall keep abreast of IT-related regulation and advise accordingly.

E. Training

1. It is the responsibility of Heads of units to ensure appropriate computer training for their staff identified. The IT Support Unit can advise on computer-related training issues.

VII. Contravention of the IT Policy

1. Staff shall be aware of their responsibilities under the NAO IT policy. The IT Support Unit shall provide guidance where requested.
2. Contravention of the NAO IT Policy or any act of deliberate sabotage to NAO computer systems shall be considered a very serious offence.
3. Computer users shall not, by any wilful or deliberate act, jeopardize the integrity of the computing equipment, its systems programs or any other stored information to which they have access. Unauthorized access to a computer (such as the deliberate introduction of viruses) shall be considered a very serious offence.

VIII. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

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

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by NAO.
2. Unauthorized connection of personal computer equipment or other network devices not belonging to NAO to the office network (LAN).
3. Unauthorized copying of information or data from organization servers or systems to external devices such as USB drives or to external systems on the Internet.
4. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which NAO or the end user does not have an active license is strictly prohibited.

5. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
6. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
7. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
8. Using a NAO computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
10. Port scanning or security scanning is expressly prohibited unless prior notification to The IT Support Unit is made.
11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
15. Providing information about, or lists of, NAO Employees to parties outside NAO.

IX. ACRONYM

Dynamic host configuration protocol (DHCP): This is a protocol use for automatic assignment of IP address to computers

Local Area Network (LAN): This consist of computer system connected within the same location, example an office premises

Virtual Local Area Network (VLAN): This involve the separation of network communication for different services, example data and video services.

Network socket: This is connection point for any network equipment to the LAN Personal Computers

Class of service (COS): refers to the different service facility available in telephone system of the National audit office.

Private branch exchange (PBX): is a private telephone network use within a company or an organization, users can communicate internally or externally by using different voice channels.

Personal Computer (PC): is a computer that is used by one person at a time in a business, a school, or at home.

Auditor General (AG): Head of Audit office.

National Audit Office (NAO)

APPROVAL AUTHORITY

DATE: 15th/04/2020 **SIGNATURE**

FULL NAME: KAGAMI BO M IGUBY **DESIGNATION** AUDITOR GENERAL

NAO IT User Agreement

This is to certify that I, the undersigned, read, understand, and will **abide by NAO IT Policy** when using computer and other electronic resources and/or systems owned, or operated by NAO Limited.

I further understand that any violation of the regulations above is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked, disciplinary action may be taken appropriate legal action may be initiated.

Name: _____

Staff ID: _____

Title: _____

Department: _____

Signature: _____

Date: _____