NIGERIAN PORTS AUTHORITY

INFORMATION AND COMMUNICATION TECHNOLOGY POLICY

1. Introduction

In order to execute its mandate, the Nigerian Ports Authority (herein after referred to as "NPA") utilizes Information and Communication Technology (ICT) services to enhance its efficiency. In providing its services, the NPA is committed to ensuring that adequate resources are deployed towards the implementation of a reliable and appropriate IT infrastructure. In view of the acquisition of these resources and the subsequent usage, it has become apparent that there is a need to develop an ICT policy to regulate the acquisition and utilization of these resources to ensure its optimal efficiency.

To address this need, NPA has developed this ICT policy in line with the extant Government policies, legal and regulatory framework

1.1 Scope

This policy covers the following but is not limited to ICT facilities, equipment, hardware, software and services provided by the NPA ICT Division.

1.2 Objectives

This policy seeks to:

a. Ensure provision of adequate and reliable ICT Infrastructure in NPA;
b. Provide guidelines on the use of ICT software, hardware and services in NPA;
c. Ensure information security of systems and data within the NPA;
d. Promote efficient utilization of information systems within the NPA;
e. Ensure application of best practices and standards;
f. Promote the spirit of awareness, co-operation, trust and consideration for others;
g. Ensure that confidentiality is not breached, so that information may be accessed only by those authorized to do so.

1.3 Focus of the Policy

This policy is expected to achieve the following:

a. a better understanding on the part of all key stakeholders of their roles and responsibilities with respect to the management of ICT in the Organization;

b. strengthen management of ICT across NPA and better decision-making at all levels, thus ensuring that ICT supports service delivery and provides value for money;
c. increased use of common or shared ICT assets and services by departments and subsidiaries for better efficiency; and
d. responsive services enabled by cutting edge technology.

1.4 Responsibility

The General Manager, Information and Communication Technology (GM, ICT) has the responsibility for the implementation of this policy. Management team of NPA ICT Division are responsible for the maintenance and regular update of the policy document.

All users of the NPA ICT Systems are required to comply with this policy.

All user activities on NPA ICT Systems are monitored to the extent necessary and justifiable for business purposes.

2. POLICY

2.1 Planning

a. The ICT Division must establish and maintain an ICT strategic planning procedure.
b. An assessment of the ICT Strategy shall be carried out in the last quarter of every year to ensure that the strategy evolves with technological change.
c. The strategy shall also be revisited and aligned with changes in business if necessary.
d. The strategy shall be taken into consideration in the production of the yearly ICT budget.
e. ICT Standards shall be defined and reviewed periodically in order to determine how ICT assets are to be configured, used and managed.
f. ICT Division must adopt a project methodology for all ICT projects.

2.2 ICT Acquisition

a. The initiation of the procurement process for all ICT facilities, equipment, hardware, software, services, radios (UHF & VHF),

telephones, peripherals, accessories, consumables and other communication gadgets and devices must be by the NPA ICT Division

b. The subsequent licensing and other subscription on the above-mentioned items where applicable should be carried out by the ICT Division.
c. All request for ICT solutions by User Departments shall be accompanied by the business requirement with a formal definition of information requirements. The requirements must be auditable. ICT Division is to design a template for the requirements.
d. A technological feasibility study shall be conducted to ensure that the proposed ICT solutions will be compatible with the ICT architecture.
e. ICT Division shall ensure that the software licensing / subscription requirements are considered prior to project commencement.
f. ICT Division shall ensure that services acquired are covered by Service Level Agreement (SLA) for all projects with Third-party service providers. This should be referred to in the formal legal agreement with the authority.
g. All ICT acquisition (software licenses, subscription etc.) done on behalf of the Authority by a third party must be registered in the name of the NPA. Access to such acquisition must be provided to NPA before payment, and a local warranty should be obtained on all procured items.

2.3 Application Development

a. All applications development must provide the following documents as part of software development lifecycle (SDLC) that translates business requirements into detailed design specifications:

- Input requirements definition and documentation
- Interface definition
- Source data collection design
- Program specification
- File requirements definition and documentation
- Processing requirements
- Output requirements definition
- Source code when applicable
- Internal controls and audit trial

- Security and availability
- Testing requirements

b. The impact of any new ICT deployment or changes in ICT deployment must be assessed for their impact on the ICT environment before deployment with respect to performance, capacity planning, tuning, integration and security.
c. Establish user procedures manuals, operations manual and training materials as part of any new applications development.
d. Define an implementation plan encompassing roll-out/installation procedures, incident handling, feedback procedure, distribution controls, storage of software, as well as handover from development to testing to production.
e. Specify a test plan and define roles, responsibilities and success criteria including final acceptance criteria.

2.4 Software Licensing

a. The installation of software not licensed by NPA onto NPA assets is not permitted.
b. Installations onto NPA assets are to be done by the staff of ICT Division.
c. Only licensed Software shall be installed onto NPA ICT assets.
d. Duplication of NPA Licensed software for use outside NPA premises is not permitted except with the permission of the Executive Management.
e. Installation of Licensed Software must be in conformity with the license agreement.
f. A register of software and the software licensing details must be maintained and updated on a regular basis.

2.5 ICT Services (SLA)

a. ICT Division shall enter into Service Level Agreement (SLA) for all projects/support contract with third party providers. The SLA must include the establishment of a service catalogue, service descriptions and comprehensive and measurable service.
b. Service level standards must be established for provision of ICT services to internal customers.

c. Service level standards shall be regularly evaluated, and service improvement programs implemented to address service level deviation where it exists.
d. A regular review of service level agreements and underpinning contracts with internal and external customers must be carried out periodically to ensure that they are effective and up to date.
e. ICT shall create a service desk function that serves as a single point of contact to register, communicate, dispatch and analyze all reported incidents, service requests and information demands. ICT Division must create a knowledge base of issues and resolution.
f. An escalation process must be applied that ensures that reported issues are acted on based on their agreed service levels.

2.6 ICT Asset Management

a. NPA ICT assets shall be managed across its full lifecycle encompassing acquisition, deployment, storage and disposal.
b. An inventory of all NPA ICT assets including and not limited to hardware e.g. servers, workstations, laptops, PDA's, modems, switches, routers, firewalls, printers, telephones, radios (UHF & VHF) shall be maintained and kept up-to-date.
c. In the event of a disposition, an employee shall not move with any ICT Asset in his/her charge to the new location.
d. If an employee resigns or is terminated from service, all ICT Assets under his/her charge shall be handed over to his/her immediate supervisor/Head of Department.
e. On no account shall any ICT Asset be moved from their allocated office because of a disposition, resignation or termination;
f. Only the GM ICT or the Head of ICT in Port Locations can authorize the re-allocation of any ICT Asset within the Authority.

2.7 Network Cabling / Wireless Local Area Network (LAN)

a. NPA ICT Division manages the installation, maintenance and certification of all communication network. User Departments shall not manage or install alternative network.

b. The extension of the Network to integrate third party network must be carried out with the approval of the Executive Management.
c. NPA ICT shall be contacted and its approval given in writing before any network installation shall be altered, removed or relocated as part of any construction projects.
d. Executive Management must approve the use of any of NPA's network conduit systems by any department or outside the organization.
e. All installed network termination points (face plates), patch panel and cabling system must be labelled.
f. All installed network shall be capable of transmitting data, video, audio and voice traffic.
g. The installation of wireless access point is the sole responsibility of the NPA ICT Division, no other persons or division should connect wireless access point to the NPA network or within the NPA premises without authorization.
h. When deemed necessary, the NPA ICT shall conduct a site survey to determine the appropriate placement of new or additional access points.
i. All access point broadcast frequencies and channels shall be set and maintained by the ICT Division. Any device or equipment found to be interfering with access point signals may be subject to relocation or removal, including cordless phones, microwave ovens, cameras, light ballasts, etc.

2.8 Security and Information Access Control

a. Unique user identification and authentication systems must be applied to prevent unauthorized access to internal resources.
b. User account management must be enforced, and a formal process must be established by NPA ICT for requesting, approving, issuing, suspending, modifying and closing user accounts.
c. Access rights shall be reviewed and confirmed periodically.
d. Access privileges shall only be granted on a need to use basis and in accordance with the relevant user's requirements necessary to carry out its job function.

e. All connections to the Internet or other public networks must be protected by firewalls configured to filter traffic and ensure against cyber-attack and unauthorized access to internal resources.

2.9 Physical Security

a. The data center and switch rooms are restricted areas and must be protected by sufficient physical barriers. Doors, windows, elevators, docking stations, air vents and ducts and other methods of access to the computer facilities rooms must be adequately secured.
b. An appropriate alarm system must be installed in the data center.
c. Access to computer facilities rooms shall be controlled and logged. Third party companies working in the data center shall be escorted into the data center and reasons for entry shall be logged.
d. Administrators shall login with administrative rights when performing duties that require administrative privileges.
e. Official Secret Act on confidentiality of information is also applicable to electronic and digital documents.
f. NPA retention policy is also applicable to electronic / digital documents.
g. Hazardous or flammable materials shall not be stored in the data center.
h. Eating, drinking or smoking is strictly prohibited in the data center.
i. Fire prevention and detection systems shall be installed in the data center and shall be tested regularly.
j. Power protection controls shall be installed to prevent power outages or surges e.g. uninterrupted power supply systems, automatic voltage regulator, phase reversal, lighting conductors and backup generators.
k. Air conditioning, ventilation and humidity controls shall be installed and kept at optimum levels.
l. Safety and health measures shall be implemented in the data center e.g. clearly marked escape routes and first aid kits.

2.10 Password Use

a. Users shall not keep copy of password in any written form or electronic form. Passwords of critical user accounts (Administrator) shall be maintained securely.
b. Users shall change passwords whenever there is any indication of possible system or password compromise.
c. Users shall change temporary passwords at first logon
d. Users shall not include password in any automated logon process.
e. Users shall not share their passwords with anyone
f. Users shall always lock their desktop screen, when leaving their systems.
g. Wireless access points shall be secured with the help of a security key
h. Passwords shall be alphanumeric with at least 6 digits.
i. NPA devices are programmed to lock themselves with a password or PIN if left idle for five minutes. After five failed login attempts, the device will lock, and you will need to contact NPA ICT to regain access.

2.11 Virus Control

a. All Users shall act in accordance with best practices to ensure that at all times:
    - The integrity of software and data is safeguarded.
    - The integrity and availability of IT services is maintained.
b. All devices connected to NPA network shall be protected by NPA's antivirus software.
c. When a virus infection is detected either through virus protection software or suspected due to abnormal response from the PC, the User shall immediately stop working and report the NPA ICT Division.
d. Users are to ensure external storage media are scanned before connecting to NPA devices.

2.12 Bring Your Own Device (BYOD)

a. All the policies applicable to NPA owned devices are applicable to employee devices when used within NPA Network.
b. Devices shall be presented to NPA ICT for antivirus installation check, job provisioning and configuration of standard applications, such as

browsers, office productivity software and security tools, before they can access the network.

c. The employee's device shall be remotely wiped if 1) the device is lost, 2) the employee terminates his or her employment, 3) NPA ICT detects a data or policy breach, a virus or similar threat to the security of the company's data and technology infrastructure.

2.13 Business Continuity and Disaster Recovery (DR)

a. A Business continuity and disaster recovery plan shall be established, maintained and periodically tested for all critical information resources.

b. The plan shall define:
   - Procedures for assessing damage, escalation procedures and declaring a disaster.
   - Roles and responsibilities of disaster recovery team members, including third parties, their contact details and communication procedures.
   - Prioritized recovery procedures based on the critical nature of information resources.
   - Backup procedures, manual procedures, alternative processing facilities and safety and health procedures.

c. The ICT DR plan shall be stored in hard and soft copy in a place of safe storage and shall be accessible in the event of failure.

d. The ICT DR plan shall be securely distributed and available only to authorized personnel.

e. Backups shall be performed based on a defined cycle.

f. Backup media shall be clearly labelled, prevented from overwriting, appropriately stored.

g. Backups shall be checked periodically to determine whether recovery is possible.

h. Essential 'hot' spares shall be stored and be easily retrievable in the event of a disaster.

i. Disaster recovery simulations sessions shall be conducted to ensure preparedness for a disaster.
j. Daily health checks shall be conducted on critical ICT resources. The checks shall include, amongst others disk capacity, network bandwidth, buffer sizes, database size, error logs, WAN and LAN connectivity checks.
k. Performance reporting shall occur on all critical IT resources on a regular basis.

2.14 Email Usage

a. The use of personal emails for work related communication is strictly prohibited. NPA staff can only use NPA email for official communication.
b. Email is a business communication tool and users shall use this tool in a responsible, effective and lawful manner.
c. The corporate email should be utilized for the following:
    - Monthly pay-slip
    - NPA monthly newsletter
    - Circulars, bulletin and notices
    - Performance Appraisal notification
    - Notification and invitation for training programs
d. Users shall archive his/her emails to a local device at regular intervals. All locally stored emails that are critical shall be protected by a password.
e. Users shall conduct the necessary housekeeping of their emails at regular interval.
f. Users shall promptly report all suspected security vulnerabilities or problems with the email system to the designated ICT Team.
g. Confidential information shall be secured before sending through e-mail by way of compression, password protection or other advanced cryptographic means.
h. Language used shall be consistent with other forms of business communications

i. Users shall treat electronic-mail messages like other official information.
j. Users shall avoid opening email from unknown users/sources and avoid opening suspicious attachments or clicking on suspicious links.
k. NPA ICT Division can restrict attachments size on the company mail system in line with the need of the user and storage space availability.
l. NPA reserves the right to monitor email messages and shall intercept or disclose or assist in intercepting or disclosing email communications to ensure that email usage is in conformity with this policy.
m. Users shall avoid sending or forwarding unsolicited email messages; "chain letters", "jokes", "junk mail", etc. from other internal users, external networks or other advertising material to individuals.
n. Users shall avoid any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
o. The use of third party email application shall be restricted on the NPA network.

2.15 Internet Usage

a. Internet use, during official hours is authorized to conduct official business.
b. Users should be aware that their information systems (computer, internet, email, messenger, FAX and telephone conversations), its usage and information exchanged are not private and the Authority reserves the right to monitor and audit these on an ongoing basis and during or after any security incident.
c. Users shall exercise restrain when using or accessing the internet for non-business purposes and restrict personal use to the minimum.
d. Users shall strictly avoid visiting offensive and unethical sites.
e. Users shall not use Internet facilities to:
    - Download or distribute malicious software or tools or to deliberately propagate any virus
    - Violate any copyright or license agreement by downloading or distributing protected material

- Upload files, software or data belonging to NPA to any Internet site without authorization.
- Share any confidential or sensitive information of NPA with any Internet site without authorization
- Users shall not post any NPA proprietary information.
- Post remarks that are offensive/aggressive/Insulting, obscene or not in line with NPA condition of service.
- Conduct illegal or unethical activities including gambling, accessing obscene material or misrepresenting the organization

f. Users shall ensure that they do not access websites by clicking on links provided in emails or in other websites. When accessing a website where sensitive information is being accessed or financial transactions are done, it is advisable to access the website by typing the URL address manually rather than clicking on a link.

g. Users shall ensure that security is enabled on the Internet browser as per guidelines given below:
   - Configure browser not to remember web application passwords.
   - Set browser security setting to medium.

h. NPA has the right to restrict access to websites that are deemed inimical to the overall interest of the Authority.

i. NPA has the right to limit or restrict access to social media sites (Facebook, Instagram, YouTube, etc.)

j. In case misuse of the Internet access is detected, NPA ICT shall terminate the users Internet access and shall report to HR to take relevant action.

2.16 ICT training and Manpower Development

a. ICT training policy shall fit into the overall general training policy of the Authority.

b. Technical and user training shall be conducted to complement the installation of ICT software, hardware, network and services.

c. All new ICT projects (software, hardware, network, communication and services) shall include training cost.

d. ICT training shall explore all available format for training (e-learning, classroom, on the job etc.).
e. Job induction for employees shall include ICT training especially for those that require ICT systems for their job roles.
f. In line with the ICT strategy, training shall be organized to keep employees abreast of new technologies especially ICT division staff.

2.17 Non-Compliance

NPA reserves the right to audit compliance with this policy from time to time. Employees or other users who do not comply with the provisions of this policy shall be disciplined in accordance with Conditions of Service of NPA. Any employee on becoming aware of any contravention of this policy shall promptly and confidentially advise the persons to whom they report, or their Head of Department. NPA reserves the right to suspend or permanently remove a user's access to some or all the electronic communication facilities.

This policy was approved by Executive Management at the 19th Executive Management Committee Meeting (Resumed Meeting) which held on Tuesday 16th July 2019.