NATIONAL ENERGY AUTHORITY

Papua New Guinea's Independent Regulator of the Electricity and Downstream Energy Sector

ICT Policy

www.nea.gov.pg

Harnessing Energy for Life

NATIONAL ENERGY AUTHORITY

ICT Policy

Revision Status Tracker

DOCUMENT CONTROL

This ICT has been reviewed, approved, and authorized for implementation within the Authority. It is intended to guide all employees and stakeholders in the management, use, and maintenance of NEA-owned or leased motor vehicles. This policy will be effective as of the date of approval and will remain in force until the next scheduled review or until further amendments are approved by authorized personnel.

Contents

Acronym

NEA – National Energy Authority

DICT – Department of Information & Communication Technology

ICT – Information & Communication Technology

DTO – Digital Transformation Officer

EM – Executive Manager

CAD – Corporate Affairs Division

MD – Managing Director

CCTV – Closed-Circuit Television

MFA – Multi-factor Authentication

LAN – Local Area Network

WAN – Wide Area Network

IDS – Intrusion Detection System

HR – Human Resource

CSP – Cloud Service Providers

Section 1: Introduction

The National Energy Authority (NEA) is established under the NEA Act 2021, which grants it the authority to set its own employment terms, conditions, and policies, provided they align with the laws and regulations of Papua New Guinea. This framework allows NEA to manage its operations independently while ensuring compliance with relevant legal requirements.

The NEA relies heavily on Information and Communication Technology (ICT) systems to support its mission and objectives. This policy outlines the framework for managing, acquiring, and using ICT resources responsibly to ensure secure and efficient operations across the organization.

Section 2: Scope

This document is consistent with the industrial standards listed below and outlines comprehensive Information & Communication Technology Policy NEA develops.

- ISO/IEC 27001 – Information Security Management Systems (ISMS)
- ISO/IEC 27002 – Code of Practice for Information Security Controls
- ISO/IEC 27017 – Cloud Security
- ISO/IEC 20000 – IT Service Management
- NIST Cybersecurity Framework – National Institute of Standards and Technology
- Digital Governance 2020 Act – PNG compliance
- PNG Digital Transformation Policy – National Digital Initiatives
- PNG Data Governance & Data Protection Policy 2023

This policy applies to all employees, Board members, trainees, contractors, and third-party service providers who were granted permission to use NEA's ICT resources. It governs all aspects of ICT services, including management of computer hardware, and software, network systems, data, and communication tools.

Section 3: Governance and Oversight

The governance and oversight of the NEA ICT policy ensure the policy is implemented effectively, regularly reviewed, and compliant with national standards. The NEA Board holds the responsibility of vetting and approving the policy, while the ICT/Admin branch under Corporate Affairs Division serves as its custodian.

Policy

3.1 The NEA Board is responsible for approving, reviewing, and updating the ICT policy as required.

3.2 The ICT/Admin branch under Corporate Affairs Division is the custodian of the policy, ensuring day-to-day operational compliance.

3.4 Any updates or amendments to this policy must be approved by the NEA Board.

3.5 The Corporate Affairs Division must present the ICT policy for Board approval every two years or as required by operational needs.

3.6 The Manager ICT/Admin is responsible for maintaining records of all policy amendments and communicating changes to relevant stakeholders.

3.7 The Executive Managers must review the policy to ensure effectiveness and alignment with NEA's corporate objectives.

Section 4: Roles and Responsibilities

The proper management of ICT resources is critical for NEA's operations. Clear roles and responsibilities for ICT management ensure that all levels of the organization support efficiently and secure ICT practices.

Policy

4.1 NEA Board: Approves and oversees ICT policy governance.

4.2 Managing Director: Grants final approval for the ICT policy's management and implementation to ensures its alignment with NEA's corporate goals. Furthermore, MD has the power to delegate responsibilities as necessary

4.3 Executive Manager Corporate Affairs: Provides management of ICT policy and implementation to ensure its alignment with overall corporate objectives and strategies.

4.4 Manager ICT/Admin: Implements the ICT policy and oversees ICT operations and compliance.

4.5 Executive Managers (EM): Ensure that staff under their supervision adhere to the ICT policy.

4.6 NEA Employees: Must follow the ICT policy and report any issues or breaches to their immediate supervisor or EM Corporate Affairs.

4.7 NEA Guess Users: The respective divisions EMs are responsibility for ensuring that their division's guest or visitor(s) is compliant to NEA's ICT standards and procedures

Section 5: National Digital Transformation Compliance

The digital governance 2020 Act provides for the digital government for the use of ICT. The digital governance also enables the streamlining, planning, coordination, development and implementation across the whole of government of digital services, digital infrastructure, digital transformation, digital skills and all other aspects of digital governance.
The Digital Transformation Officers are mandated by the Digital Governance 2022 to implement whole digital governance initiatives or other related matters coordinated by Department of ICT. The Act allows for the Head of Organization to nominate an officer to perform the role of DTO. Digital Transformation Officers are pivotal in navigating the complexities of the digital age and ensuring that government agencies effectively harness the benefits of digital innovation for the betterment of Papua New Guinea society.

Policy

5.1 NEA's ICT strategy must incorporate digital transformation initiatives that align with the PNG Digital Transformation Policy.

5.2 The Managing Director shall appoint the Manager ICT/Admin to perform the role of DTO to coordinate all digital initiatives in alignment with the Digital Government Act 2022

5.3 All ICT acquisitions and services must follow established standards and guidelines to ensure security and efficiency.

5.4 ICT systems must prioritize digital service delivery, robust data governance, and cybersecurity.

5.5 The Manager ICT/Admin as the DTO is responsible for coordinating and developing a digital transformation roadmap for NEA. This roadmap must align with the PNG Digital Transformation Policy and the Digital Government Act 2022, ensuring the integration of digital services, infrastructure, and skills across NEA.

5.6 All ICT acquisitions, including hardware, software, and services, must adhere to the standards and guidelines set by the PNG Digital Governance 2020 Act. The Manager ICT/Admin will ensure that all procurement is efficient, secure, and in compliance with the relevant digital governance policies.

5.7 ICT systems must prioritize the security of digital services and robust data governance. The Manager ICT/Admin will implement strong cybersecurity measures, regularly review systems, and ensure that data protection protocols are consistently upheld.

5.8 The Manager ICT/Admin will conduct regular reviews of all digital transformation initiatives, reporting progress to the NEA Board through EM CAD. These reviews will assess alignment with NEA's corporate objectives and compliance with national digital governance mandates.

Section 6: Data Management

Data is a critical asset for NEA, and it must be managed securely and efficiently. This section outlines the policies and procedures for data classification, access control, storage, and disposal.

Policy

6.1 All NEA data must be classified based on its sensitivity (Public, Internal, Confidential, Highly Confidential).

(a) Data classification must be done at the point of creation, with access restrictions based on job roles.

6.2 Access to sensitive data is restricted to authorized personnel.

6.3 Data must be securely stored and regularly backed up.

(a) Daily/Weekly backups must be performed for all data, stored both on-site and in secure off-site locations.

6.4 In case of a data breach, employees must immediately report the incident to the Manager ICT/ Admin. The ICT/Admin team will initiate an investigation and implement the required remediation steps.

6.5 NEA will collect, use, and store information only for legitimate business purposes and in compliance with applicable data privacy laws.

6.6 All sensitive or confidential data, must be protected from unauthorized access at all stages, including collection, storage, and disposal.

6.7 All employees and contractors handling information must adhere to NEA's data privacy and protection guidelines.

6.8 Highly confidential data must be encrypted both at rest and transit to ensure its integrity and prevent tampering with the original information

6.9 All obsolete data must be disposed of securely through digital shredding or other approved methods, ensuring no retrieval is possible.

6.10 The ICT/Admin team is responsible for conducting quarterly reviews of data access controls, ensuring compliance with NEA's data retention and privacy policies.

6.11 Employees handling personal data must ensure that all collected information is securely stored, and access is restricted to authorized personnel only.

6.12 Authority's confidential data must not be shared with third parties without proper authorization, and all data sharing must comply with applicable privacy laws.

Section 7: Technology Hardware Acquisition

This section ensure that all hardware technology acquired by the NEA is standardized, cost-effective, and compatible with existing ICT infrastructure. This policy aims to minimize hardware diversity while ensuring that all hardware meets the operational and strategic needs of the NEA. Additionally, the policy ensures that all hardware assets are responsibly tracked, maintained, and disposed of in accordance with best practices. This policy applies to all hardware purchases and lifecycle management, including desktop systems, portable devices, servers, and mobile phones, across all NEA branches and divisions.

Policy

7.1 All hardware acquisitions must be approved by the manager ICT/Admin to ensure standardization, compatibility with existing infrastructure, and compliance with NEA's operational requirements.

7.2 All hardware must be tracked through an inventory system that records the hardware's location, assigned user, and status. This ensures assets are accounted for throughout their lifecycle.

7.3 Hardware must be maintained according to a scheduled maintenance plan to ensure longevity and optimal performance. Service contracts must be managed for timely repairs and replacements.

7.4 Obsolete or damaged hardware must be securely disposed of following approved procedures, which include secure data erasure. All disposals must be documented for auditing purposes.

Hardware Specification

7.5 Desktop Systems

a) Only HP, Dell, Acer, and Lenovo models running Windows operating systems are permitted.

b) Systems must have a minimum of:

i) i5/i7 processors

ii) 500 GB RAM, Wi-Fi capabilities

iii) Two or more USB ports, HDMI capabilities

iv) 23-inch and above monitors

c) All desktop systems must include Windows 10 Professional and above

d) All desktop purchases require approval from the Managing Director.

e) Hardware must be purchased from recommended suppliers and include manufacturer guarantees and warranties.

7.6 Portable Devices (Laptops & Tablets)

a) Portable devices such as laptops and tablets must meet the same performance standards as desktops.

b) Devices must be compatible with NEA's network and server systems.

c) All portable devices must be purchased from authorized suppliers and meet the NEA's operational requirements.

7.7 Servers

a) Only the ICT Manager or an authorized ICT professional is permitted to procure servers.

b) All servers must be compatible with the NEA's data infrastructure and existing systems.

c) Servers must support current and future data management needs.

7.8 Mobile Phones

a) Mobile phone purchases are restricted to officers as per their employment contract terms and

conditions.

b) Phones must be purchased from approved suppliers (e.g. Fone Haus) and be compatible with NEA's internal communication systems.

c) Other purchases of mobile phones must come with a justification and MD must approve the quote for payment if the justification serves the corporate interests of NEA operation

7.9 Needs Assessment

Before any new hardware is purchased, a needs assessment must be conducted by the ICT/Admin team to determine the operational requirements and ensure there is no unnecessary duplication or waste.

7.10 Asset Tracking

Upon acquisition, all hardware must be recorded in an asset tracking system. The system will document the location, assigned user, and operational status of each piece of hardware to facilitate effective lifecycle management.

7.11 Regular Service & Repairment

a) Hardware must undergo regular maintenance as part of a scheduled plan to extend its lifecycle and ensure optimal performance.

b) Service contracts must be actively managed to ensure timely repairs and replacements when required.

7.12 Secure Disposal

a) When hardware becomes obsolete or damaged, it must be wiped of all data using secure erasure techniques before disposal.

b) Documentation of all disposals must be maintained for auditing and accountability purposes.

c) The manager ICT/Admin is responsible for recommending the disposal of all ICT assets to the Managing Director.

Section 8: Software Procurement and Management

This policy ensure that all software acquired and managed by the NEA is secure, compatible with NEA's systems, compliant with licensing agreements, and protected against security vulnerabilities. This policy governs the acquisition, deployment, usage, and management of software throughout its lifecycle to ensure alignment with NEA's operational needs and legal obligations.

This policy applies to all software acquisitions, usage, and management within NEA, including proprietary, open-source, and freeware software. It covers procedures for requesting, procuring, deploying, and managing software as well as ensuring ongoing compliance and security.

Policy

8.1 All software acquisitions must be reviewed and recommended for approval by the Manager ICT/ Admin to ensure compatibility with NEA's systems, licensing compliance, and security requirements.

8.2 All software must comply with licensing agreements and NEA's financial policies.

8.3 Unauthorized software is prohibited on NEA ICT systems.

8.4 Software updates, patches, and security fixes must be applied regularly to protect against vulnerabilities and ensure continued compliance.

8.5 Software that reaches the end of its life must be replaced or upgraded promptly to avoid any potential security risks or operational disruptions.

8.6 Software, including open-source and freeware, must pass thorough security assessments to ensure they meet NEA's security and operational standards.

8.7 (a) All software purchases must be made from reputable vendors and align with NEA's financial policies.

(b) Open-source or freeware software requires explicit assessment from the ICT/Admin team to ensure it meets security requirements and aligns with NEA's operational needs.

8.8 Only authorized personnel are permitted to install or configure software on NEA systems. This ensures that all installations comply with security policies and licensing agreements.

8.9 The ICT/Admin team must conduct quarterly software audits to ensure compliance with licensing agreements and detect any unauthorized software installations. Audits will also ensure that all software meets NEA's security requirements.

8.10 (a) All installed software must be kept up-to-date with the latest patches and security updates to mitigate any security vulnerabilities.

(b) Regular updates must be applied promptly as part of NEA's ongoing cybersecurity efforts.

8.11 When software reaches its end-of-life, it must be promptly replaced or upgraded to avoid security and operational risks. The replacement or upgrade process must be documented and align with NEA's operational goals.

Section 9: Cloud Services

This policy outlines that the NEA leverages cloud services effectively, while maintaining the highest standards of data integrity, security, and compliance. Cloud services offer NEA scalability and flexibility but require careful management to safeguard sensitive data and ensure adherence to legal and regulatory requirements.

This policy applies to all cloud services utilized by NEA, including data storage, software as a service (SaaS), and infrastructure as a service (IaaS). It governs access, security, data management, and compliance in all cloud environments used by the organization.

Policy

9.1 Access to cloud services is restricted to authorized personnel only, and all users must use multi-factor authentication (MFA) for secure login.

9.2 All data stored in the cloud must be encrypted both during transmission (in transit) and while stored (at rest) to ensure data integrity and protection against unauthorized access.

9.3 Regular security audits and compliance reviews must be conducted to ensure that cloud service providers meet NEA's data protection standards and align with legal requirements, such as data privacy laws.

9.4 In the event of potential breaches, the ICT personnel must respond inline with the cloud security incident response guide per DataCo for reporting, escalation, and mitigation.

9.5 The manager ICT/Admin must vet and approve all cloud service providers prior to engagement. This vetting process must include:

a) Verification of compliance with international and local security standards

b) Assessment of the provider's ability to meet NEA's operational, security, and data protection requirements.

9.6 (a) Weekly backups of all data stored in the cloud must be performed, with regular testing of backup integrity to ensure the data can be restored effectively in the event of loss or corruption.

(b) Backup data must be encrypted and stored securely to maintain confidentiality and integrity.

9.7 The ICT/Admin team must conduct quarterly reviews of cloud service usage and data protection practices to ensure ongoing compliance with NEA policies and relevant regulations. This review includes:

(a) Ensuring that all data is encrypted, and access controls are being adhered to.

(b) Verifying that backups are functioning properly and that recovery tests have been successful.

(c) Reviewing access logs and audit trails for any signs of unauthorized access or anomalies.

9.8 The ICT/Admin team must implement real-time security monitoring and set up automated alerts to detect any suspicious activities, such as unauthorized access attempts or unusual data transfer volumes within the cloud environment.

Section 10: Electronic Door Access

This policy ensures that the NEA maintains a high level of physical security by controlling access to its facilities using electronic door access systems. This policy governs the management of electronic access to restricted areas to protect sensitive operations and assets.

This policy applies to all NEA facilities that utilize electronic door access systems. It covers access control, management of access credentials, logging and auditing, and response to security incidents.

Policy

10.1 Access to restricted areas within NEA facilities must be managed and secured using electronic door access systems. Access is granted only to authorized personnel based on their job roles and responsibilities.

10.2 Access logs must be automatically generated and securely stored to facilitate auditing and investigation. Logs should capture details such as employee identification, date and time of access, and door location.

10.3 Any unauthorized access attempts or breaches must be promptly referred to the ICT/Admin branches for investigation.

10.4 The ICT/Admin team is responsible for maintaining an up-to-date database of all employees authorized to access restricted areas. This includes assigning and managing access levels based on job roles and ensuring that the electronic access control system is regularly updated to reflect personnel changes (e.g., new hires, terminations, or role changes).

10.5 Access logs must be reviewed monthly by the ICT/Admin team to detect any unauthorized access attempts or suspicious patterns of activity. If any discrepancies or unauthorized attempts are identified, the issue must be escalated to HR for further investigation.

10.6 In the event of a lost or stolen access card, the employee must immediately report the incident to the ICT/Admin team. Upon receiving the report:

(a) The manager ICT/Admin will authorize deactivating the lost/stolen card to prevent unauthorized access.

(b) A replacement access card will be issued to the employee after the necessary security checks.

10.7 (a) Access cards for employee leaving NEA or changing roles that no longer require access to restricted areas must be deactivated immediately.

(b) New cards are issued only after verifying the user's clearance level and ensuring that the system is updated with the latest access permissions.

10.8 The electronic door access system must be integrated with real-time monitoring tools to alert the ICT/Admin team of any unauthorized access attempts or system anomalies. Immediate actions must be taken to investigate and secure the premises in the event of a breach.

Section 11: CCTV Systems

This policy is to ensure that CCTV systems are used effectively to enhance security and safety at NEA facilities. This policy governs the installation, management, and secure handling of CCTV systems and footage to ensure that NEA's security operations align with privacy and data protection standards.

This policy applies to all CCTV systems installed at NEA facilities and covers the processes for installing, accessing, storing, and reviewing CCTV footage.

Policy

11.1 CCTV systems must be installed in high-security, critical, and sensitive areas to provide comprehensive monitoring of NEA's operations and facilities.

(a) The ICT/Admin team is responsible for the installation and regular maintenance of CCTV systems to ensure they remain fully operational and capable of capturing clear and reliable footage. Systems must be inspected periodically to identify and address any technical issues, such as camera malfunction or storage capacity concerns.

11.2 Access to live CCTV feeds and recorded footage is strictly limited to authorized personnel only, in accordance with NEA's data privacy and security policies.

11.3 CCTV footage must be reviewed periodically by the ICT/Admin team to detect any security incidents or suspicious activities. The review must include an analysis of footage from high-security areas to ensure that any potential risks are addressed promptly. Any identified incidents must be escalated to HR or the appropriate department for further action.

11.4 Requests to access CCTV footage for investigative purposes must be submitted to and approved by the Manager ICT/Admin. Access is granted only to authorized personnel involved in the investigation, and all access must be logged for auditing purposes. The release of footage to external parties must comply with NEA's legal and privacy requirements and be approved by the Managing Director for EM CAD and Manager ICT/Admin to facilitate

11.5 CCTV footage must be securely stored in a designated, restricted-access area. Footage must be retained for a minimum of one year, or longer if required by legal, operational, or investigative needs. Footage must be encrypted to safeguard its confidentiality, and retention policies must be reviewed periodically to ensure compliance with legal and operational requirements.

11.6 All CCTV footage must be handled in compliance with NEA's data protection policies and relevant privacy laws, ensuring that the footage is used solely for security and investigative purposes.

11.7 In the event that an incident occurs, the divisional EMs are responsible to authorize two of their staff to review and make report of the incident

11.8 Any security incidents identified through CCTV footage must be reported immediately to the EM CAD for investigation. The ICT/Admin team must collaborate with HR to address the incident

Section 12: Network Security

The purpose of this policy is to ensure that the NEA protects its ICT infrastructure from internal and external threats. This policy governs the use of firewalls, intrusion detection systems (IDS), access controls, and regular monitoring to maintain robust network security.

This policy applies to all NEA network systems, including LAN, WAN, and cloud-based systems. It outlines the methods and practices used to secure the network against unauthorized access, data breaches, and other security threats.

Policy

12.1 NEA's network must be protected by firewalls, intrusion detection systems (IDS), and other security tools designed to detect and prevent unauthorized access and attacks.

(a) The manager ICT/Admin or designated ICT personnel is responsible for configuring and maintaining firewalls, IDS, and other network security tools. These systems must be regularly updated and patched to protect against evolving security threats. Firewall rules must be reviewed periodically to ensure they reflect current security needs, and IDS systems must be fine-tuned to detect the latest intrusion tactics

12.2 Access to NEA's network is restricted to authorized personnel only, with access granted based on job roles and responsibilities. Multi-factor authentication (MFA) must be enabled for all users to enhance security.

12.3 Network activity must be continuously monitored to detect and respond to any security incidents in real-time. Monitoring tools must be configured to flag any unusual or suspicious activity, ensuring immediate action can be taken to mitigate potential threats.

(a) Network security audits must be conducted every quarter by the ICT/Adminteam. These audits should include vulnerability scans, penetration testing, and a review of access controls to ensure compliance with NEA's security standards.

Any vulnerabilities detected during the audit must be addressed immediately, with priority given to high-risk issues that could compromise the network.

(b) Any network security breaches or incidents must be reported immediately to the Manager ICT/Admin, who will initiate a response plan to contain the breach and mitigate any potential damage.

The breach must also be reported to HR for investigation in accordance with HR compliance policies. A full incident report must be compiled and shared with relevant stakeholders, outlining the cause, impact, and remediation steps taken.

12.4 NEA must perform regular vulnerability assessments and security audits to identify and address potential weaknesses in the network infrastructure. Quarterly audits must be conducted to ensure that all systems are secure and compliant with NEA's security policies.

12.5 Access to firewall administration and configuration settings must be strictly controlled. Only authorized personnel, specifically designated by the Manager ICT/Admin, are permitted to have administrative access to the firewall.

12.6 Administrative access to the firewall and endpoint security systems must be secured using strong passwords that comply with NEA's password policy. Passwords should be complex, regularly updated, and securely stored. Multi-factor authentication (MFA) must be enabled for additional security.

12.7 All administrative access to firewall and security systems must be logged, and access logs should be

regularly reviewed to detect unauthorized or suspicious activity. The ICT team must maintain these logs for auditing and compliance purposes.

12.8 Endpoint security tools, including antivirus software and intrusion detection systems (IDS), must be deployed across all NEA devices to safeguard against malware, ransomware, and other cyber threats. These tools must be regularly updated and monitored by the ICT team.

12.9 Firewalls and endpoint security systems must receive timely security patches and updates to protect against vulnerabilities. The ICT/Admin team is responsible for scheduling and applying these updates.

12.10 When an employee with firewall or security system access changes roles or leaves the organization, their access rights must be immediately revoked. Passwords must be reset to ensure that no unauthorized access is possible post-departure.

12.11 The ICT/Admin team must manage user access to the network, ensuring that access permissions are aligned with the user's job role and responsibilities. Access privileges must be regularly reviewed and updated, particularly for employees who change roles or leave NEA.

Multi-factor authentication (MFA) must be enforced for all users accessing NEA's network, particularly for remote access and cloud-based systems.

12.13 All NEA employees must receive regular security awareness training, particularly regarding network security best practices. This includes recognizing phishing attempts, proper use of authentication methods, and understanding the importance of safeguarding login credentials.

Section 13: User Access

This policy aims to ensure that NEA staff have appropriate levels of access to ICT systems and data based on their job roles and responsibilities. This policy governs the creation, management, and revocation of user access, ensuring alignment with security standards and organizational requirements.

This policy applies to all NEA employees, contractors, and external partners who are granted access to NEA's ICT systems. It covers account creation, access control, permission reviews, and account deactivation when an employee leaves or changes roles.

Policy

13.1 User access to NEA's ICT systems must be determined based on the employee's job role and responsibilities. Access levels should be aligned with the principle of least privilege, granting users only the permissions necessary to perform their duties.

(a) The manager ICT/Admin, in collaboration with HR, is responsible for creating user accounts when new employees are onboarded. The account setup must include assigning appropriate access levels based on the employee's role and responsibilities.

HR must notify manager ICT/Admin of any changes to an employee's status, including promotions, transfers, or role changes, so that access privileges can be adjusted accordingly.

13.2 Regular reviews of user access rights must be conducted to ensure compliance with organizational needs and security requirements. This ensures that only authorized personnel retain access to sensitive data and systems.

(a) The manager ICT/Admin or designated ICT personnel must conduct quarterly reviews of all user accounts and access permissions to ensure that access levels remain appropriate for each employee. The review should include:

(i) Verifying that access aligns with the employee's current job role.

(ii) Identifying and revoking access for inactive accounts or accounts with unnecessary privileges.

(iii) Any discrepancies must be corrected promptly, and the review results documented for auditing purposes.

13.3 When an employee leaves NEA or transitions to a new role that no longer requires specific access, their access must be revoked immediately to prevent unauthorized use of ICT systems.

a) When an employee leaves NEA, HR must inform manager ICT/Admin immediately. The Manager ICT/Admin is responsible for ensuring that the employee's access to all ICT systems is revoked within 24 hours ofdeparture.

(b) A formal confirmation must be provided to HR once the access has been revoked. This includes disabling login credentials, email accounts, and access toshared drives, cloud services, and any other ICT systems.

13.4 (a) The ICT/Admin team must implement monitoring tools to track user account activity, including login attempts and access to sensitive data. Alerts should be triggered for any suspicious activity, such as unauthorized access or attempts to use disabled accounts.

(b) Any security incidents related to user accounts must be investigated and reported in line with NEA's incident management procedures.

13.5 (a) Temporary access may be granted to contractors or external partners based on specific project requirements. Access must be limited in scope and duration, and accounts should be deactivated once the project is completed.

(b) All third-party access must be reviewed and approved by the Manager ICT/Admin before being granted.

Section 14: Data Retention

This policy aims that the NEA complies with legal, regulatory, and operational obligations by retaining and securely storing data for the required duration. This policy governs how long data is retained, under what conditions, and the processes for secure deletion or disposal.

This policy applies to all data created, collected, and managed by NEA. It includes data storage, classification, retention, and disposal across both physical and digital formats. The policy applies to all employees, contractors, and third-party service providers with access to NEA data.

Policy

14.1 All NEA data must be classified based on its legal, regulatory, and operational importance. Each data type must be retained for a specific period.

(a) The ICT/Admin team will maintain a data retention schedule that aligns with legal requirements. This schedule will include retention periods for different data types, such as internal reports, emails, contracts, and confidential records.

(b) All NEA data must be backed up weekly, with copies stored both on-site and off site to ensure disaster recovery and business continuity.

14.2 Data must be securely stored and regularly backed up to prevent loss or corruption. Sensitive and confidential data must be encrypted during storage and transmission to protect against unauthorized access.

(a) Backups must be encrypted and stored in a secure environment to protect the integrity and confidentiality of the data.

(b) Regular tests must be conducted to ensure that backup and restoration processes are functioning properly.

14.3 Data that has reached the end of its retention period or is no longer needed must be securely deleted or disposed of in compliance with NEA's data retention schedule and relevant regulations. This applies to both digital and physical records.

(a) When data reaches the end of its retention period or is no longer required, it must be securely deleted from all systems and devices. This includes:

(i) Digital data: Secure deletion must involve data wiping tools that ensure the information cannot be recovered.

(ii) Physical records: Paper-based records must be shredded or disposed of through certified methods to prevent unauthorized access.

(b) The Manager ICT/Admin is responsible for overseeing the secure deletion process, ensuring that the removal is verified, and maintaining documentation for audit purposes.

14.4 Sensitive or confidential data, including personal information, must be encrypted and protected from unauthorized access throughout its lifecycle, including storage, access, and disposal.

14.5 Any breach, loss, or unauthorized access to data must be reported immediately to the Manager ICT/Admin, who will escalate the incident to HR and the relevant legal or compliance teams for investigation.

14.6 The ICT/Admin team must regularly review compliance with the data retention policy. This includes auditing retention schedules, reviewing backup processes, and verifying that obsolete data is securely deleted.

These reviews should be documented and used to update the data retention schedule or procedures as needed.

Section 15: Email Policy

Electronic email is a primary communication tool used throughout NEA for both internal and external purposes. However, improper use of email can introduce significant legal, privacy, and security risks. It is essential that all employees of the NEA email system understand the appropriate use of email to avoid misuse and protect the organization's interests.

This policy is designed to ensure the proper use of NEA's email system and to define acceptable and unacceptable practices. It outlines the minimum requirements for using NEA's email system in alignment with organizational goals and compliance standards.

It therefore applies to all NEA employees, contractors, and third-party service providers who are granted access to the NEA email system. It covers all emails sent from an NEA email address and any actions performed using NEA's email system.

Policy

15.1 All email communication must be consistent with NEA's policies on ethical conduct, safety, compliance with laws, and proper business practices. NEA's email system should primarily be used for business-related purposes. Limited personal use is permitted but should not interfere with work responsibilities or breach organizational policies. Non-NEA related commercial activities using the NEA email system are strictly prohibited.

15.2 NEA data shared via email must be secured in line with NEA's Data Management Standards (Section 10). Sensitive or confidential information must not be transmitted through email unless appropriate security measures, such as encryption, are in place. Employees are responsible for ensuring that email content, particularly attachments, are secure and sent to authorized recipients only.

15.3 Emails should be retained only if they qualify as an NEA business record. A business record is defined as email that has an ongoing, legitimate business purpose. Emails identified as business records must be retained according to the NEA Data Retention standards (section 14). Employees are responsible for ensuring the appropriate retention and management of business-related emails.

15.4 The NEA email system must not be used to create or distribute offensive or disruptive content, including comments related to race, gender, religion, politics, sexual orientation, or any other discriminatory material. Any employee who receives an email containing such content must report it immediately to their supervisor or the HR department for investigation.

15.5 Users are prohibited from automatically forwarding NEA emails to third-party email systems such as Gmail, Yahoo, or Hotmail. NEA business transactions and communications should only occur within the NEA email system, and no confidential information should be forwarded to or stored in third-party email accounts.

15.6 A reasonable amount of personal email use is permitted within the NEA email system, but non-work-related emails must be stored in a separate folder from work-related communications. Sending chain letters, jokes, or similar emails through the NEA system is prohibited.

15.7 Employees should not expect privacy in emails sent, received, or stored within the NEA email system. NEA may monitor email communications without prior notice as part of its duty to safeguard organizational resources and ensure compliance with its policies. While monitoring is not obligatory, NEA reserves the right to review emails as needed.

15.8 Employees must exercise caution when opening emails from unknown senders, particularly those with attachments or suspicious links. Any suspicious emails must be reported immediately to the ICT/Admin team for investigation to prevent phishing or malware threats.

15.8 Any misuse of NEA's email system will result in disciplinary action in line with the organization's HR policies. Non-compliance with this policy, particularly regarding security breaches or the transmission of inappropriate content, will be subject to investigation and corrective actions, which may include suspension of email privileges or further disciplinary measures.

Section 16: Email Retention Policy

This policy outlines the appropriate retention of email correspondence to ensure compliance with NEA's record-keeping policies and legal requirements. Mismanagement of email can lead to data loss, security risks, and non-compliance with internal and legal regulations. Employees must be familiar with the classification of email information and follow the proper guidelines for retention.

This serves to help employees determine the retention requirements for emails sent or received via the NEA email system. This includes categorizing and retaining emails for appropriate periods in line with NEA's business record-keeping and operational needs.

It therefore applies to all employees, contractors, and third-party service providers using the NEA email system. All email information is categorized into four main classifications, each with specific retention guidelines:

Administrative Correspondence: **Retained for 4 years and deleted when no longer required**

Fiscal Correspondence: **Retained for 4 years and deleted when no longer required**

General Correspondence: **Retained for 1 year and deleted when no longer required**

Ephemeral Correspondence: **Retained until read and then destroyed when no longer required.**

Policy

16.1 Administrative correspondence includes emails relating to NEA's policies, procedures, legal matters, and internal communications, such as holiday schedules, employee policies, and intellectual property guidelines. Administrative correspondence must be retained for 4 years and should be copied to a designated mailbox or hard drive for retention and oversight.

16.2 Fiscal correspondence covers all emails related to NEA's financial matters, including revenue, expenses, budgets, and financial reports. These emails must be retained for 4 years and must be copied to the designated fiscal mailbox or hard drive for centralized retention by the ICT team.

16.3 General correspondence pertains to operational and customer interactions that are necessary for daily NEA functions. This category is the responsibility of individual employees, and these emails should be retained for 1 year. Employees must ensure emails containing important operational decisions are appropriately saved for future reference.

16.4 Ephemeral correspondence includes non-business-related or informal communication, such as personal emails, project updates, and general requests. These emails do not require long-term retention and should be deleted once read or when no longer needed.

16.5 Instant messaging used within NEA's approved systems may contain administrative or fiscal information and should be copied into email form and saved accordingly.

16.6 Encrypted emails should be stored and handled in compliance with NEA's Data Protection and Security policies. In general, where possible, secure information should be stored in a decrypted format to enable compliance with internal audits and records management.

16.7 NEA retains email backup drives for disaster recovery purposes.

16.8 All NEA employees must use the approved NEA email system for official communication, and unauthorized email systems, such as personal accounts, must not be used for business purposes. Employees are responsible for the proper retention and secure handling of emails, ensuring compliance with NEA's policies on data security and encryption.

16.9 Non-compliance with this policy may result in disciplinary action. Employees are expected to adhere strictly to email retention guidelines, and any violations will be referred to HR and dealt with in accordance with NEA's disciplinary procedures.

Section 17: Lost, Stolen and Damaged ICT Assets

This policy ensure that all ICT assets owned by the NEA are properly managed when lost, stolen, or damaged. This policy aims to safeguard organizational resources, protect sensitive data, and ensure the timely reporting and resolution of incidents involving ICT assets.

This policy applies to all NEA employees, contractors, and third parties who use NEA-owned ICT assets, including laptops, mobile phones, tablets, and other digital devices. It outlines the reporting, investigation, and mitigation procedures for lost, stolen, or damaged ICT assets.

Policy

17.1 (a) Any loss, theft, or damage of NEA ICT assets must be reported immediately to the manager ICT/Admin and the employee's direct supervisor within 24-hours to ensure timely action and data protection. The report must include details such as the type of asset, the last known location, and the circumstances surrounding the loss, theft, or damage.

(b) Upon receiving a report, the ICT team will initiate an investigation to determine the cause of the incident and assess any potential risks to NEA's data or infrastructure. An incident report must be completed, detailing the findings of the investigation, and submitted to HR for further review and potential action. The report should include:

(i) A description of the incident.

(ii) The steps taken to secure the device and data.

(iii) Recommendations for preventing similar incidents in the future.

17.2 An incident report must be completed for all lost, stolen, or damaged ICT assets and submitted to HR for further investigation and a copy to manager ICT/Admin. This ensures that the circumstances of the incident are properly documented, and any follow-up actions are initiated.

17.3 In cases where a device is lost or stolen, NEA's ICT team must remotely wipe all sensitive information from the device and disable access to prevent unauthorized use. This action must be completed within 24 hours of the incident being reported. The remote wiping process must ensure that all personal and organizational data is unrecoverable, minimizing the risk of data breaches or unauthorized access.

17.4 Damaged or lost ICT assets must be replaced in accordance with NEA's standard procurement procedure, as outlined in the Acquisition of ICT Products & Services Policy (Section 15).

17.5 The replacement of lost, stolen, or damaged ICT assets must follow the standard procurement process. This includes:

(a) Conducting a needs assessment to determine whether the asset requires immediate replacement.

(b) Following NEA's procurement procedures to ensure that the replacement asset meets technical, security, and financial requirements.

(c) The cost of replacement may be reviewed and, in certain cases, shared with the employee if negligence is determined to have contributed to the loss or damage.

17.6 The ICT team must maintain a detailed log of all incidents involving lost, stolen, or damaged ICT assets, including the outcomes of investigations and any corrective actions taken. This log will be used during audits and reviews to identify trends and recommend improvements to asset management and security practices.

17.7 The custodian of NEA asset is responsible to provide crime/police report from the nearest police station to claim new asset or else the employee will be liable for its cost

Section 18: Acceptable Use of ICT Resources

The purpose of this policy is to outline the acceptable use of computer equipment and other electronic devices at NEA. These rules are in place to protect the employees and NEA. Inappropriate use exposes NEA to cyber risks including virus attacks such as ransomware, compromise of network systems and services, data breach, and legal issues.

It applies to the use of information, electronic and computing devices, and network resources to conduct NEA business or interact with internal networks and business systems, whether owned or leased by NEA, the employee, or a third party. All employees, contractors, consultants, interns, and other workers at NEA and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with NEA policies and standards, and local laws and regulation.

It applies to employees, contractors, consultants, interns, and other workers at NEA, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by NEA.

Policy

18.1 NEA's ICT resources, including email, internet, and communication systems, must be used for official business purposes that support NEA's operational and strategic goals.

18.2 Limited personal use of ICT resources is permitted if it does not interfere with an employee's official duties, negatively impact productivity, or result in excessive costs to NEA.

18.3 The use of NEA's ICT resources for illegal activities, the dissemination ofinappropriate content, or engaging in unethical behaviour is strictly prohibited. This includes accessing, distributing, or storing offensive, defamatory, or discriminatory material.

18.4 Employees are responsible for ensuring that their use of ICT resources does not compromise the security of NEA's systems or data. Sharing login credentials or allowing unauthorized individuals to access NEA ICT systems is forbidden.

18.5 (a) Employees must not share their login credentials, passwords, or other access information with unauthorized individuals. Access to NEA's ICT systems must be limited to authorized personnel only.

(b) Employees must immediately report any suspicious activity or unauthorized access attempts to the Manager ICT/Admin for investigation and mitigation.

18.6 (a) The ICT team is responsible for monitoring the use of NEA's internet and communication systems to ensure compliance with the acceptable use policy. Monitoring may include reviewing internet traffic, email logs, and other communication tools to detect inappropriate or unauthorized activity.

(b) Any illegal or inappropriate activities detected through monitoring must be reported to HR for investigation. HR will determine the appropriate disciplinary action, if necessary.

18.7 (a) Employees must remain vigilant against phishing attacks and othercybersecurity threats. Any suspicious emails, links, or requests for sensitive information must be reported to the Manager ICT/Admin immediately for review and response.

(b) The ICT team must provide regular training on phishing prevention and cybersecurity best practices to ensure employees understand how to protect NEA's data and systems.

18.8 Employees who become aware of violations of this policy, such as misuse of ICT resources or security breaches, must report the incident to the Manager ICT/Admin or HR immediately. Confidential reporting channels must be maintained to encourage reporting without fear of retaliation.

Section 19: Policy Violation

The purpose of this policy is to establish guidelines for the identification, reporting, and investigation of ICT policy violations at the NEA. This policy ensures that all breaches of ICT policies are managed appropriately and referred to ICT/Admin and HR for investigation, disciplinary action, and compliance management.

This policy applies to all employees, contractors, and external partners who have access to NEA's ICT resources. It governs the process for reporting and addressing violations of any ICT-related policies, including unauthorized access, misuse of resources, and security breaches.

Policy

19.1 All ICT policy violations must be reported immediately to HR for investigation. This includes incidents such as unauthorized access, misuse of NEA's ICT resources, and any breaches of security or data protection protocols.

(a) Employees who become aware of any ICT policy violation must report it to their direct supervisor and the Manager ICT/Admin as soon as possible. The report should include details of the violation, such as the nature of the breach, when it occurred, and the individuals involved.

The Manager ICT/Admin will complete an incident report that documents the violation and forward it to HR for review and investigation.

(b) Upon receiving the incident report, HR will initiate an investigation to determine the cause, impact, and severity of the policy violation. The investigation process may involve interviews with involved parties, analysis of ICT systems, and a review of relevant documentation to establish the facts surrounding the violation.

(c) Based on the findings, HR will determine the appropriate disciplinary action, which may include:

(i) A formal warning.

(ii) Suspension.

(iii) Termination of employment or contract.

(iv) Legal action, if applicable.

(d) (i) All investigation findings, including incident reports, interviews, and conclusions, must be thoroughly documented by HR. This ensures a clear record of the violation and the steps taken in response.

(ii) Disciplinary actions taken because of the investigation must also be documented and retained in the employee's file. These records will be maintained for auditing purposes and as part of NEA's compliance and governance frameworks.

19.2 Violations may include, but are not limited to:

(a) Unauthorized access to restricted systems or data.

(b) Misuse of ICT resources, including personal use beyond acceptable limits.

(c) Engaging in illegal activities using NEA's ICT infrastructure.

(d) Failure to adhere to security policies, including sharing credentials or allowing unauthorized access.

19.3 HR is responsible for determining and implementing appropriate disciplinary actions for policy violations. Disciplinary actions will vary depending on the severity of the violation and may range from warnings to termination of employment.

19.4 All reports of policy violations must be treated confidentially to protect the integrity of the investigation and the privacy of involved parties. HR must ensure that there are clear, confidential channels available for employees to report violations without fear of retaliation.

19.5 Following a policy violation, the ICT/Admin team and HR may review existing policies and procedures to identify any gaps that could have contributed to the breach. Based on these reviews, policies may be updated, and additional training may be provided to employees to prevent future violations.

Section 20: Mobile Phone Usage

This policy aims to establish guidelines for the use of NEA-issued and personal mobile phones for work purposes. This policy ensures that mobile phone usage complies with NEA's security standards and organizational goals, while safeguarding sensitive data.

This policy applies to all NEA employees who are issued mobile phones by the organization, as well as employees who use personal mobile phones for business purposes. It governs the appropriate use, security, and management of mobile devices in alignment with NEA's ICT policies.

Policy

20.1 NEA-issued mobile phones must be used primarily for business purposes that align with the organization's operational needs. Minimal personal use is permitted, provided it does not interfere with work responsibilities or incur excessive costs to NEA.

(a) Employees eligible for NEA-issued mobile phones will be determined based on their role, job responsibilities, and business requirements. Eligibility criteria will be defined by the HR branch in coordination with manager ICT/Admin.

The procurement team will facilitate the acquisition of mobile phones for eligible employees in accordance with NEA's procurement policy and guidelines.

(b) Employees must use NEA-issued mobile phones responsibly, ensuring that they comply with NEA's acceptable use policies. This includes:

(i) Avoiding the download of unauthorized or non-business-related applications.

(ii) Refraining from using mobile phones for personal gain or activities that could harm NEA's reputation.

(iii) Employees are prohibited from making any modifications to the phone's security settings without prior approval from the manager ICT/Admin.

(c) If a NEA-issued mobile phone is lost or stolen, employees must notify the Manager ICT/Admin immediately. The ICT/Admin team will take the following actions:

(i) Remotely wipe all data from the device to prevent unauthorized access to NEA's systems and information.

(ii) Disable the phone to ensure that it cannot be used by unauthorized individuals.

(iii) A formal incident report must be completed, documenting the loss and actions taken, and submitted to HR for review.

20.2 All NEA-issued mobile phones must be secured with password protection and encrypted to safeguard organiational data. This ensures that sensitive information remains protected from unauthorized access in case of loss or theft.

20.3 Employees who use personal mobile phones for work-related tasks must comply with NEA's security standards, including:

(a) Enabling password protection on their device.

(b) Encrypting all sensitive business data stored on or transmitted through the phone.

(c) Avoiding the use of unauthorized apps that could pose security risks to NEA's data.

(d) Employees using personal devices must ensure compliance with NEA'smobile device management policies and must not store sensitive data on unapproved platforms.

20.4 Employees must report lost or stolen NEA-issued mobile phones immediately to the manager ICT/Admin to initiate security protocols, including remote wiping and disabling the device.

Section 21: Communication

The purpose of this policy is to ensure that all forms of communication, whether verbal, non-verbal, digital, external, visual, or formal, within and outside NEA are conducted professionally, securely, and in alignment with the organization's corporate goals. Effective communication is vital for fostering transparency, maintaining professionalism, and ensuring consistency in NEA's messaging.

This policy applies to all NEA employees, contractors, and third-party service providers.

Policy

21.1 All verbal and non-verbal communications must reflect professionalism, respect, and courtesy. In face-to-face interactions, meetings, and other verbal communications, employees should maintain a tone and demeanour that aligns with NEA's values. Non-verbal cues, such as body language, should also be consistent with this standard.

21.2 All digital communications, including WhatsApp, email, internal messaging, and social media, must adhere to the highest standards of professionalism. Employees must:

(a) Use formal language for business emails and avoid slang or informal abbreviations pursuant to section 15 of this policy document.

(b) Address all recipients correctly, ensuring emails and digital messages are appropriately directed to the intended audience.

(c) Limit personal use of NEA's digital communication tools, ensuring such usage does not interfere with work responsibilities.

21.3 External communication, including public statements, press releases, and other outward-facing messages, must be aligned with NEA's corporate and strategic objectives and values. The Communications Team is responsible for:

(a) Managing external communication to ensure that all messaging aligns with NEA's brand.

(b) Providing guidance on public statements, interviews, and media engagements.

(c) Ensuring that all external communications, including official correspondences, are approved by the Managing Director in line with NEA's internal guidelines (Ref: NEAMDO 01/2024).

21.4 All written communications, including memos, letters, reports, and internal documents, must be clear, concise, and well-structured. Employees must:

(a) Ensure the content is aligned with NEA's goals and that the correct tone is maintained throughout.

(b) Use official NEA letterheads and formats for all external correspondence.

(c) Avoid disclosing sensitive information without proper authorization.

21.5 Formal presentations, reports, and visual communications (e.g., slides, videos, infographics) must be professional, fact-based, and align with NEA's brand and corporate messaging. All visual content must undergo a review to ensure it conveys accurate information and is presented in a manner consistent with NEA's standards.

21.6 Sensitive and confidential information, whether communicated verbally, digitally, or in writing, must not be disclosed without prior authorization.

21.7 Employees must take appropriate measures to secure communication channels and protect against unauthorized access.

21.8 The ICT/Admin team is responsible for ensuring communication systems are secured to prevent breaches.

21.9 The personal use of NEA's communication systems, pursuant to section 23 & 24 of this policy must

be limited and should not interfere with professional responsibilities. Personal conversations or messages that compromise work efficiency or productivity are discouraged.

21.10 Any breach of this Communication Policy, including unauthorized disclosure of confidential information or inappropriate communication, is a serious disciplinary matter. Disciplinary actions will be handled according to NEA's HR policies and Managing Director's memo (Ref: NEAMDO 01/2024).

21.11 All official communications, including letterheads, memos, and external correspondences, must be approved and issued by the Managing Director, as per Managing Director's memo (Ref: NEAMDO 01/2024).

21.12 The ICT/Admin team is responsible for monitoring communication systems and ensuring compliance with this policy. Breaches will be reported to HR, and appropriate disciplinary actions will be taken. This Communication Policy will be reviewed periodically to ensure it remains relevant and aligned with NEA's corporate objectives, technological advancements, and security requirements.

Section 22: Website and Social Media

The purpose of this policy is to establish guidelines for the creation, management, and security of the NEA's online presence, including its website and social media platforms. This policy ensures that all content reflects NEA's mission and values, while maintaining professionalism, accuracy, and security across all digital channels.

This policy applies to all NEA employees and authorized personnel responsible for managing NEA's website and social media platforms. It governs the publication of content, access control, and the handling of user-generated content to ensure that NEA's online presence remains secure, professional, and aligned with organizational goals.

Policy

22.1 All content published on NEA's website and social media channels must be professional, accurate, and reflect NEA's mission, values, and strategic objectives. Content must be reviewed and approved by designated personnel/committee before publication.

(a) The ICT/Admin team will coordinate with relevant divisions to ensure that all website and social media content is accurate, up-to-date, and aligned with NEA's strategic objectives.

(b) Content must be reviewed and approved by the committee team or designated content manager(s) before being posted on any platform.

(c) Divisions providing content must ensure that it is consistent with NEA's mission and values and that it adheres to the organization's branding and communication guidelines.

(d) Website and social media account access must be strictly controlled by a designated team of authorized personnel. The ICT/Admin team must maintain a log of all users with access and ensure login credentials are managed securely.

22.2 Access to NEA's website and social media management tools must be restricted to authorized personnel only. All accounts must be secured using multi-factor authentication (MFA) and robust password management practices to protect against unauthorized access.

22.3 Any inappropriate, harmful, or policy-violating content posted by external users on NEA's social media platforms or website must be removed immediately. NEA reserves the right to moderate and control user-generated content to maintain a positive and respectful online environment.

22.4 (a) The ICT/Admin team must conduct regular audits of NEA's website and social media content to ensure compliance with organizational policies and objectives. Audits should focus on ensuring that content is current, accurate, and professional.

(b) Any external user-generated content that violates NEA's policies or is deemed inappropriate must be flagged and removed immediately. The communications team must respond to user interactions that require clarification or moderation to maintain a respectful online community.

22.5 (a) The ICT team is responsible for implementing regular security checks on all NEA website and social media accounts. This includes monitoring for unauthorized access attempts, unusual activity, or security vulnerabilities.

(b) Security protocols must be updated regularly to protect NEA's online presence from cyber threats such as hacking, phishing, or account takeovers. Any incidents of unauthorized access or data breaches must be reported immediately, and corrective action must be taken to mitigate the risks.

22.6 (a) In the event of a security breach, inappropriate content posting, or any other incident affecting NEA's online presence, the committee team, in collaboration with ICT/Admin, must execute a crisis management plan to quickly address the issue and restore the integrity of the platforms.

(b) Communication with external stakeholders during such incidents must be handled carefully to protect NEA's reputation.

Section 23: Telephone System and CUG

This section outlines the policies governing the use of the NEA's telephone systems and the Closed User Group (CUG) service. These guidelines ensure responsible, cost-effective, and secure use of communication systems for official purposes.

Policy

23.1 The NEA's telephone systems, including landlines, mobile phones, and the Closed User Group (CUG) service, are provided for official business purposes only. Personal use of these systems should be kept to a minimum, and excessive personal calls may result in disciplinary action.

23.2 The CUG service is intended to facilitate secure, cost-efficient communication between NEA employees and approved external parties. Only authorized personnel are allowed to use the CUG service, and it must be used exclusively for business-related communication.

23.3 The ICT & Administration Branch is responsible for monitoring the use of the Authority's telephone systems, including tracking call logs, CUG usage, and associated costs. Any misuse of these systems, such as excessive personal calls or unauthorized use of CUG services, will be reported to HR and may result in disciplinary action.

23.4 Employees allocated with mobile phones under the CUG plan are required to use these devices for official communication purposes only.

The Managing Director, Executive Managers and Managers are entitled to unrestricted access to CUG services for official business purposes.

Other employees may be provided with CUG services based on their role and operational needs. Access is subject to the approval of the Managing Director.

23.5 All employees must practice professionalism and courtesy when using the Authority's telephone systems. Calls should be answered promptly, and the use of offensive language or inappropriate behaviour during calls is strictly prohibited.

23.6 Employees must maintain confidentiality when discussing sensitive business matters over the phone, especially in public or unsecured environments. Security protocols should be followed to prevent unauthorized access or disclosure of sensitive information.

23.7 The ICT & Administration Branch will regularly review telephone and CUG usage to ensure compliance with this policy and monitor costs. Any unauthorized or inappropriate use will be reported to HR for further action.

Section 24: Internet

The purpose of this policy is to ensure the secure and responsible use of the internet within NEA. This policy governs internet access and usage to protect the organization's digital infrastructure, maintain productivity, and prevent misuse.

It therefore applies to all NEA employees, contractors, and third-party service providers who access the internet using NEA's network.

Policy

24.1 NEA's internet resources must be used for business purposes only. Employees are prohibited from using the internet for personal activities that interfere with their work responsibilities. This ensures all employees must use the internet responsibly, such that all online activities comply with NEA's standards outlined herewith.

24.2 Accessing inappropriate, illegal, or unauthorized websites is strictly prohibited. This includes, but is not limited to, websites containing pornography, gambling, and sites that promote hate or violence.

24.3 NEA monitors internet usage, and any unauthorized or suspicious activity may be subject to investigation.

24.4 The ICT/Admin team must implement firewalls, web filters, and other security measures to restrict access to inappropriate websites and protect the network from threats.

24.5 Any employee who requires access to a restricted website for business purposes must request approval from their supervisor and the Manager ICT/Admin.

24.5 Employees must not download or install software or files from untrusted sources that could pose a security risk to NEA's network.

24.6 If any violation of this policy is detected, the incident will be reported to HR, and appropriate disciplinary measures may be taken.

Section 25: Printer Policy

This policy serves to ensure the responsible use and management of NEA's multi-purpose printers and other printing equipment. It aims to minimize waste, ensure efficient use of resources, and protect confidential information that may be printed.

The content therein applies to all NEA employees, contractors, and third-party service providers who have access to NEA's printers and printing equipment.

Policy

25.1 All NEA printers must be used for official business purposes only. Personal use of NEA's printing resources is strictly prohibited, and it may incur disciplinary measures as per HR standards unless approved by a supervisor.

25.2 Employees must handle print jobs containing sensitive or confidential information with care. They are responsible for collecting printed documents immediately after printing to prevent unauthorized access and must dispose of sensitive documents using a shredder if no longer needed.

25.3 All printers must be configured to default black and white, double-sided printing to conserve ink and paper. Employees should avoid printing large documents unless necessary. Opting for digital file sharing is highly recommended

25.4 Only authorized personnel are permitted to perform maintenance on printers or troubleshoot technical issues. Employees must report any printer malfunctions to the ICT/Admin team for resolution via the Helpdesk system Helpdesk.ICT@nea.gov.pg

25.6 Any non-compliance with this policy will be reported to HR, and disciplinary action may be taken as necessary.

Section 26: Training

The NEA is committed to ensuring that all ICT personnel maintain the highest standards of professional knowledge and competency. To achieve this, the Authority mandates that all current and future ICT personnel acquire and maintain specialized IT certifications relevant to their roles.

Policy

26.1 All ICT employees are required to possess or acquire certifications in specific areas critical to the Authority's operational success. These certifications include, but are not limited to:

(a) Microsoft Office 365: Certification is required to demonstrate proficiency in cloud-based productivity tools and services, essential for NEA's operations.

(b) CompTIA Security+: This certification ensures that ICT personnel understand key principles of cybersecurity, risk management, and threat mitigation.

(c) Cisco Certified Network Associate (CCNA): Certification in network fundamentals is essential for ICT staff responsible for maintaining and managing NEA's network infrastructure.

(d) Certified Information Systems Security Professional (CISSP): Required for advanced-level ICT personnel to ensure they have the knowledge to protect the Authority's systems and data.

(e) Microsoft Certified: Azure Fundamentals: This certification focuses on cloud services and infrastructure as the Authority continues adopting cloud solutions.

(f) CompTIA A+: A foundational certification that covers essential IT skills andtechnical support, such as hardware, operating systems, and networking.

(g) CompTIA Network+: Focuses on networking concepts, troubleshooting, operations, and infrastructure. It is essential for anyone working with on premises networking and hybrid cloud environments.

(h) CompTIA Security+: A globally recognized certification for establishing the basic knowledge of cybersecurity skills, a must-have for managing both on-premises and cloud environments.

26.2 All ICT staff must ensure they maintain the validity of these certifications by pursuing continuous learning and renewal of their credentials. The ICT/Admin branch will support and track compliance with certification requirements.

26.3 ICT employees are expected to participate in ongoing professional development programs, workshops, and specialized training sessions to stay current with emerging technologies and trends relevant to the NEA's digital transformation objectives.

26.4 All prospective ICT employees must meet the mandatory certification requirements as a precondition of employment. Candidates without the requisite certifications will not be considered unless they commit to acquiring the necessary qualifications within a defined period.

Section 27: Compliance and Monitoring

To ensure the effectiveness of the ICT policy, regular compliance checks and monitoring activities are essential. This section outlines how compliance will be monitored and enforced.

Policy

27.1 Regular monitoring of ICT systems and audits of policy compliance must be conducted.

27.2 Any non-compliance with ICT policies will result in disciplinary action as determined by HR.

27.3 Regular audits of ICT systems will be conducted, and a report submitted to Manager ICT/Admin who then will provide assessment to EM CAR or appropriate management.

27.4 Any detected non-compliance will be referred to HR for investigation and appropriate action.

Section 28: Staff Acknowledgement and Acceptance of Policies

This policy outlines that all NEA employees acknowledge and accept their responsibility to comply with the organization's ICT policies. By signing the acknowledgment form, employees confirm their understanding and commitment to adhere to the established ICT protocols.

It therefore applies to all NEA employees, contractors, and third parties who are granted access to NEA's ICT systems and resources. It governs the process for acknowledging the ICT policies and accepting responsibility for compliance.

Policy

28.1 All NEA employees must sign the End-user Agreement form confirming that they have read, understood, and accepted the terms of NEA's ICT policies. This agreement ensures that employees are aware of their responsibilities in adhering to the policies.

28.2 Failure to sign the acknowledgment form or to comply with the ICT policies may result in restricted access to NEA's ICT systems and resources. Employees who do not adhere to the policies may face disciplinary action, including revocation of access to critical systems.

28.3 (a) The HR department, in collaboration with the manager ICT/Admin, is responsible for distributing copies of the ICT policy to all employees. Each employee must be provided with a copy of the policy either in digital or printed form.

(b) Employees must be given sufficient time to review the policy and seek clarification from HR or the ICT/Admin team if they have any questions or concerns.

28.4 (a) All employees are required to sign the End-user Agreement Form (See attachment), confirming that they have read, understood, and accepted the ICT policy. This form serves as a formal acknowledgment of their responsibility to comply with NEA's ICT policies and procedures.

(b) HR will collect the signed forms from all employees and ensure they are properly completed.

28.5 (a) The HR department will retain the signed acknowledgment forms in each employee's personnel file. These records serve as proof of the employee's understanding and acceptance of NEA's ICT policies and can be referenced during audits or investigations.

(b) The retention of these forms ensures that NEA can demonstrate compliance with its internal policies and regulatory requirements.

28.6 (a) New hires and contractors must sign the agreement form as part of their onboarding process. ICT access will not be granted until the signed form is received by HR and filed.

(b) The HR department must ensure that new employees receive a copy of the ICT policy during orientation and are made aware of the importance of complying with all related procedures.

28.7 In the event of significant updates to the ICT policy, employees may be required to sign a new acknowledgment form reflecting their understanding of the revised policies. HR and ICT/Admin must ensure that employees are informed of changes and given the opportunity to review and sign the updated agreement form.

Section 29: Review and Update

This policy aims to ensure that the NEA's ICT policy remains current, effective, and aligned with technological advancements, legal requirements, and organizational changes. Regular reviews and updates are essential to maintaining the relevance and efficacy of the ICT policies.

This policy applies to the review and updating process of all ICT policies within NEA. It governs the procedures for conducting reviews, submitting updates for approval, and distributing revised policies to employees.

Policy

29.1 NEA's ICT policies must be reviewed and updated regularly to reflect advancements in technology, evolving legal requirements, and any changes in NEA's operational or organizational structure.

29.2 All updates to the ICT policy must be submitted to the NEA Board for review and approval before being implemented. This ensures that changes are thoroughly evaluated and align with NEA's strategic goals.

29.3 The ICT guidelines and procedures will be reviewed periodically by the Manager ICT/Admin and EM CAD for the MD to approve

Annexes

Annex 1: ICT End User Agreement Form

Annex 2: Employee ICT Exit Checklist Form

Annex 1: ICT End U?ser Agreement Form

National Energy Authority

ICT End-User Agreement Form

Employee Name: _____ **Job Title:** _____

Division: _____ **Date:** _____

I, *[Insert Name]*, agree to:

a) *Use NEA's computers, phones, and other equipment for work purposes only.*
b) *Avoid using NEA's systems for personal activities that may disrupt work or violate NEA policies.*
c) *Report any lost, damaged, or malfunctioning equipment to the ICT team immediately.*
d) *Keep work-related information private and only share it with authorized people.*
e) *Protect NEA's information by not leaving devices unattended and locking screens when not in use.*
f) *Report any suspicious activity or attempts to access private information to my supervisor or the ICT team immediately.*
g) *Use NEA-issued mobile phones or personal devices, when authorized, in line with NEA's rules.*
h) *Follow security measures like using passwords on devices and keeping NEA's information safe.*
i) *Notify ICT immediately if my NEA-issued device is lost or stolen.*
j) *Use the internet and email for work purposes only, in ways that support NEA's goals.*
k) *Avoid accessing inappropriate websites or sending personal or unauthorized emails.*
l) *Report any suspicious emails or messages that may be part of a phishing attack to ICT.*
m) *Any violation of these rules or misuse of NEA's systems may lead to disciplinary action by HR, which may include termination of employment.*

HARNESSING ENERGY FOR SUSTAINABLE DEVELOPMENT

National Energy Authority

ICT End-User Agreement Form

Employee Declaration

I hereby acknowledge that I have read and understood the National Energy Authority's ICT guidelines and agree to comply with them fully. I understand that failure to comply may result in disciplinary action.

Employee Signature: _____ **Date:** _____ **Manager Name:** _____

ICT USE ONLY

Device Assigned: _____ **Serial Number:** _____ **Access Granted (Yes/No):** _____

_____ _____

_____ _____

_____ _____

_____ _____

ICT Officer: _____ **Signature:** _____ **Date:** _____

Manager ICT/Admin: _____ **Signature:** _____ **Date:** _____

HARNESSING ENERGY FOR SUSTAINABLE DEVELOPMENT

Annex 2: Employee ICT Exit Checklist Form

Employee ICT Exit Checklist Form

Employee Information:

Name: _____ **Job Title:** _____ **Division:** _____ **Manager:** _____

Section 1: Hardware Return Checklist

Hardware Item	Returned (Yes/No)	Condition (Good/Fair/Poor)	Remarks
Laptop/Desktop			
Mobile Phone			
Tablet			
External Hard Drives			
USB Drives			
Chargers & Adapters			
Other (Specify)			

Section 2: Software/Account Access

Access Type	Revoked (Yes/No)	Date Revoked	Comments
Email Account (O365)			
Cloud Services (Azure, OneDrive)			
Internal Applications (Specify)			
VPN Access			
Network Account			
Door Access			
Other (specify)			

Section 3: Data & Security Review

Action Item	Completed (Yes/No)	Comments
Hard drive/data wiped securely		
Passwords for all accounts reset		
All work-related files backed-up		
Data transferred to relevant personnel		
Company sensitive information removed		
Door Access removed		
Other (specify)		

Section 4: Additional Notes/Actions

Notes/Actions

_____

_____

_____

ICT Use Only

ICT OIC: ……... Date: …….. Sign: ……

Manager ICT/Admin: …… Date: ……... Sign: ……...

Declaration: All access and devices must be returned or revoked before the employee's last day. Failure to comply may result in withholding final payments.

Notes

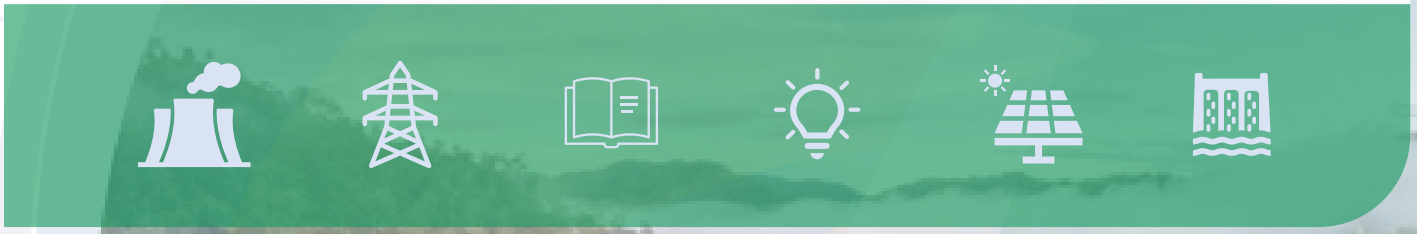
Contact Information

Office Address
Goada Herea Building
Section 58 Allotment 3
WAIGANI DRIVE, Port Moresby
Papua New Guinea

Postal Address
PO Box 494, VISION CITY 131, NCD

Contact
Phone: 3253233
Email: info@nea.gov.pg

Website
Website: https://www.nea.gov.pg



NATIONAL ENERGY AUTHORITY

www.nea.gov.pg

Harnessing Energy for Life