The Republic of Liberia
Environmental Protection Agency
(EPA)

INFORMATION COMMUNICATION TECHNOLOGY (ICT)POLICY

Version:[2026-2027]

Document status: Draft

Prepared by: [EPA-ICT Unit]

Date review: [March 30,2026]

Review by: [Senior Management Teams]

Date for issued: [April 1, 2026]

Approved by: [ENVIRONMENTAL PROTECTION AGENCY BORD OF DIRECTORS

Contents

FOREWORD

It is my pleasure to introduce the Environmental Protection Agency's ICT Policy. This document represents a major step forward safeguarding the Agency's information assets, improving service delivery, and strengthening our ability to fulfil our mandate to protect Liberia's environment.

Information and communication technology is now central to how we deliver programs, manage environmental data, coordinate research, engage stakeholders, and administer our operations. This policy sets out clear, practical and enforceable measures to ensure our ICT environment is secure, resilient, efficient and user-focused. It establishes standards for data protection, regular backup and recovery, malware and antivirus controls, access and password management, secure network use (including cloud access), asset procurement and disposal, email and communication usage, and ICT support and staff development. These measures are designed to protect the confidentiality, integrity and availability of environmental and financial data while enabling timely access to information for legitimate business needs.

The Policy further emphasizes governance, risk management and accountability. Roles and responsibilities are clearly defined so that the ICT Unit and staff users understand their obligations. Regular testing, monitoring and review are mandated to ensure backup and recovery processes meet our recovery time and point objectives and that security practices evolve alongside emerging threats and technologies. Equally important, the strategy commits to capacity building and service excellence, investing in staff skills, user training and collaborative arrangements that will improve the quality, accessibility and reliability of our ICT services.

Implementation of this policy will require commitment across the Agency and partnerships with external providers where appropriate. I urge all employees, contractors, visitors and partners to familiarise themselves with the policy, adhere to its requirements, and support its implementation. Compliance is not optional: breaches will be addressed in accordance with Agency procedures.

I am confident that, together, we will realize the benefits of a secure, modern and sustainable ICT environment.

Emmanuel K. Urey Yarkpawolo, PhD.
Executive Director/CEO

OVERVIEW

In an era where data drives decisions, powers services, and underpins environmental stewardship, the EPA's ICT Policy is the safety net that keeps the Agency resilient. This policy transforms backup and recovery from a technical checkbox into a strategic capability: *ensuring critical environmental data remains available, accurate, and secure when it matters most—during incidents, outages, or cyber threats*. It frames backup and recovery as an essential part of mission delivery, not merely an IT responsibility.

At its heart, the policy sets out a clear, organization-wide approach: define what must be protected, how often it must be backed up, where copies are stored, and how fast systems and data can be restored. It balances regulatory compliance and international best practices with practical, efficient procedures tailored to the EPA's diverse operations. By standardizing roles, schedules, retention rules, and testing regimes, the policy turns uncertainty into predictable outcomes and reduces the time between disruption and recovery.

Beyond technical controls, the policy promotes a culture of shared responsibility. Staff, visitors, and ICT teams each play distinct roles, preventing incidents, reporting anomalies, and validating recoveries—so that individual actions contribute to collective resilience. Continuous monitoring, periodic testing, and documented recovery plans ensure the policy evolves with changing threats and technologies.

The outcome is straightforward but powerful: sustained protection of the Agency's data integrity, confidentiality, and availability; minimized downtime for critical environmental programs; and confident compliance with legal and sector-specific expectations. In short, this policy ensures that EPA's data, the basis for sound decisions and public trust, remains protected, recoverable, and ready when needed.

OBJECTIVE AND SCOPE

This ICT Policy provides the EPA with clear guidance for managing its information and communications technology (ICT) infrastructure, services, and tools used by staff and clients. It sets out principles and practices for data backup and recovery that align with internationally recognized best practices while remaining adaptable to the EPA's diverse operational needs. The policy covers all devices and systems that connect to the EPA network, including wired, wireless, modem, VPN, and satellite (e.g., Starlink) connections, and applies to all data stored, processed, or transmitted on those systems. Key areas addressed include backup scheduling and retention, recovery procedures, delineation of roles and responsibilities, and controls to mitigate risks of data loss, corruption, or unauthorized access.

The policy aims to ensure the EPA adopts a consistent, organization-wide approach to backup and recovery that balances legislative compliance, industry best practices, and operational efficiency. By defining standardized processes and controls, the policy seeks to reduce the likelihood and impact of data incidents and to ensure timely and reliable restoration of critical information and services. To maintain system integrity and reduce risk, all computers connected to the EPA network must run supported antivirus software that is active, scheduled for regular scans, and maintained with up-to-date virus definitions. Any suspected infections or virus detections must be reported to the ICT Department immediately.

Overall, the policy supports the EPA's mission by protecting the confidentiality, integrity, and availability of its data and by ensuring ICT resources are used appropriately to support institutional goals. It also clarifies user responsibilities for safeguarding EPA ICT resources, promotes efficient use of network bandwidth and other ICT assets, and establishes controls to ensure regular backups and recovery activities are performed and verifiable.

What This Policy Does

This policy is our official guide for:

- Buying, setting up, using, and taking care of all our technology.
- Protecting the EPA's information, especially sensitive environmental data and personal records.
- Keeping our key tech services up and running.
- Using standard tools so our systems can work together smoothly as we become more digital.

- Making sure we follow all Liberian laws, regulations, and best practices from around the world.

Who and What's Covered

This policy applies to everyone and everything at the EPA:

- Our People: All EPA staff (permanent, contract, temporary), interns, consultants, and volunteers.
- Our Places: All EPA facilities, including our main office, regional and county offices, labs, and monitoring sites.

Our Tools: All technology the EPA owns, leases, or manages. This includes:

- Computers, servers, networks, mobile phones, and other hardware.
- Software, apps, databases, and cloud services.
- All electronic communication, like email, messaging, and video calls.
- Specialized systems for environmental monitoring, like sensors, IoT devices, and GIS.

Specific objectives:

- Protect EPA data by establishing consistent backup and recovery controls to enable timely, reliable restoration.
- Ensure ICT resources are used appropriately to support the EPA's mission and operational objectives.
- Define user responsibilities and rights for protecting EPA ICT resources and data.
- Preserve the confidentiality, integrity, and availability of data stored on EPA systems.
- Optimize network bandwidth and ICT resource allocation for authorized users to perform work effectively.
- Enforce regular backups, retention, and recovery procedures and assign clear roles for oversight and response.

PART I : ANTI-VIRUS

Purpose

Malicious software (malware)—including viruses, worms, Trojans, ransomware, spyware, crypto miners and other hostile code—poses serious risks to EPA operations, data integrity, service availability, financial resources, and public trust. This policy defines mandatory technical controls, operational procedures, governance responsibilities, and user behaviors to prevent infections, rapidly detect and contain incidents, ensure effective remediation and recovery, and preserve forensic evidence.

The policy's objectives are to:

- Reduce the probability and impact of malware infections.
- Detect malware quickly and accurately.
- Contain and eradicate infections with minimal operational disruption.
- Restore systems and data from trusted backups.
- Maintain compliance with legal, regulatory, and contractual obligations.
- Educate staff and promote consistent, secure behavior across the Agency.

Scope

This policy applies to:

- All computing devices that connect to or process EPA data: EPA-owned desktops, laptops, servers, mobile devices, virtual machines, cloud instances, IoT and OT devices, and personally owned devices that access EPA resources (BYOD) via wired, wireless, modem, VPN, or satellite (e.g., Starlink).
- All storage media: removable media (USB drives, external disks, SD cards), network shares, cloud storage, and email attachments.
- All systems and services managed by third-party vendors that integrate with EPA networks.

- All EPA personnel, contractors, consultants, temporary staff, partners and suppliers with access to EPA ICT assets.

1.1 Removable Media Controls

- Disable autorun/autorun.inf functionality on all endpoints.
- Configure endpoints to block or restrict unapproved removable media types.
- Require scanning of all removable media on approved systems and enforce write restrictions where feasible.
- Log removable media usage and maintain an inventory of approved devices.

1.2 Backup and Recovery Hardening

- Employ immutable and versioned backups stored offsite or in a segregated environment inaccessible from production networks.
- Implement offline/air-gapped backup copies for critical systems to reduce ransomware risk.
- Test restoration procedures at least quarterly for critical systems and annually for all other systems.

1.3 Network Security Controls

- Segment the network to isolate critical systems, reduce lateral movement, and apply micro-segmentation where practical.
- Implement network-level blocking of known malicious IPs/domains and content categories.
- Apply IDS/IPS detection tuned for malware C2 patterns, lateral exploit signatures, and anomalous traffic

Gidelines

- All computers attached to the **EPA** network must have standard, supported anti-virus software installed. This software must be active, be scheduled to perform virus checks at regular intervals, and have its virus definition files kept up to date.
- If an employee receives what he/she believes to be a virus, or suspects that a computer is infected with a virus, it must be reported to the ICT Unit immediately.

- Any activities with the intention to create and/or distribute malicious programs onto the Entity network (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.) are strictly prohibited.
- Any virus-infected computer will be removed from the network until it is verified as virus-free.

Rules for Virus Prevention

- All computer Users of **EPA** always run the standard anti-virus software provided by **EPA**
- Files with certain filename extensions shall be blocked by the e-mail system.
- Never copy, download, or install files from unknown, suspicious, or untrustworthy sources or removable media that are not verify by **EPA** or ICT Unit.
- Avoid direct disk sharing with read/write access. Always scan a flash disk for viruses before using it.
- Regularly update virus protection on personally-owned home computers that are used for **EPA** purposes.

ICT Unit Responsibilities

- The ICT unit is responsible for maintaining and updating this Anti-Virus Policy. Copies of this policy will be available within the ICT Unit.
- The ICT unit will apply any updates to the services it provides that are required to defend against threats from viruses.
- The ICT unit will install anti-virus software on all **EPA-owned** and installed desktop workstations, laptops, and servers.
- The ICT unit will assist **EPA** employees in installing anti-virus software according to standards on personally-owned computers that will be used for **EPA** purposes. The ICT unit will provide anti-virus software in these cases that are approve by the Entity.
- The ICT unit will perform regular anti-virus sweeps of all **EPA** computers.
- The ICT unit will attempt to notify users of the **EPA** systems of any credible virus threats via e-mail or telephone messages. Virus reports will not be acted upon until validated. All Employees should not forward these or any virus warning messages in order to keep network traffic to a minimum.

EPA Staff Responsibilities

The following activities are the responsibility of EPA departments and employees:

- All staff must ensure that all computers on the EPA network have virus protection in keeping with the standards set out in this policy.
- All Staff must not attempt to either alter or disable anti-virus software installed on any computer attached to EPA network without the express consent of the ICT unit.

All Staff are responsible for taking reasonable measures to protect against virus infection

PART II: EPA E-MAIL USE and Account Removal

Purpose

E-mail is a critical mechanism for business communications at the Environmental Protection Agency (EPA). Use of EPA e-mail systems and services is a privilege, not a right, and must be exercised responsibly to make sure our EPA email system is secure and used only by current staff. It outlines how we promptly remove accounts that are no longer needed. and in support of EPA's mission and goals.

The objectives of this policy are to:

- Define appropriate and inappropriate use of EPA e-mail systems and services
- Minimize disruptions to EPA services, operations, and activities
- Ensure compliance with applicable EPA policies, regulations, and laws

Scope

This policy covers everyone who uses an EPA email account, including permanent and temporary staff, consultants, project managers, project staff and contractors.

When an Employee Leaves:

Resignation

When an employee resigns, their email account will be:

- Disabled at the end of their last working day.
- Scheduled for permanent removal from the system and all mailing lists within 5 business days, unless the Executive Director provides written approval to extend it.

Termination

If an employee is terminated, their email account will be:

- Disabled immediately.
- Permanently removed from the system and all mailing lists within 24 hours.

Saving Records
Before any account is permanently deleted, all email records will be preserved and managed according to the EPA's official record-keeping and legal requirements.

Inactive Accounts

What We Consider Inactive:
Any email account that hasn't been used for three (3) consecutive months will be flagged as inactive.

Notification
The IT unit will send a written notice to the account holder and their director for department, warning them that the account will be removed in 5 business days.

Removal
If the user doesn't log in or if we don't receive a valid reason from their director to keep the account open, it will be disabled and then permanently removed from our system and mailing lists.

Setting Up New or Replacement Accounts

To get a new EPA email account for a new hire or to replace an account that was removed, the department head must submit a request to the Executive Director/CEO.

The request should include:

- The new staff member's name and role.
- A brief reason why they need email access.

The IT unit will only create or reactivate an account after the Executive Director (or their official delegate) has approved the request.

Who Does What

- Human Resources (HR): Must notify IT immediately about all resignations and terminations.
- IT Department: Disables and removes accounts as outlined in this policy and monitors for inactive accounts.
- Supervisors & Managers: Must inform HR and IT about any changes in their staff's employment status and respond to inactivity notices if an account needs to stay active.
- Executive Director: Approves all requests for new or replacement email accounts.

Standardized email signature policy plus a bit of technical setup.

The first step is to create a consistent, professional template that everyone at the EPA will use. For instance:

First Last Name, Degree(s)
Title | Office/Division
[Program/Branch (if applicable)]
Environmental Protection Agency
Address Line 1
Phone: (xxx) xxx-xxxx
Mobile: (xxx) xxx-xxxx (if appropriate)
Email: last first@epa.gov
Website: https://www.epa.gov.lr

Official EPA Disclaimer (if required)

All users are required to understand and comply with this policy as a condition of being granted access to EPA e-mail systems.

PART III: PASSWORD USAGE

Purpose
Passwords are a critical component of computer and information security. Poorly chosen or poorly protected passwords can result in unauthorized access to EPA systems and data, leading to potential misuse, disclosure, or loss of information.

The purpose of this policy is to:

- Establish a standard for creating strong passwords.
- Ensure consistent protection of passwords across all EPA systems.
- Better safeguard the personal, confidential, and sensitive information entrusted to the EPA.

Scope

- All EPA employees, contractors, interns, and temporary staff.
- All visitors and third parties who are granted access to EPA information systems.

- Any user account or access method that requires a password on systems that are:
- Owned, managed, or operated by the EPA, or
- Connected to the EPA network, or
- Used to access EPA information or services (including cloud services and remote access).

Password Objectives

The following are the objectives:

- Defend against unauthorized access of EPA systems that could result in a compromise of personal or institutional data.
- Ensure that ICT resources are used in an appropriate fashion, and support the Environmental Protection Agency (EPA) mission and institutional goals.
- Encourage users to understand their own rights and responsibilities for protecting their passwords.
- Protect the privacy and integrity of data stored on the EPA network.

Password Responsibilities

Users are responsible for assisting in the protection of the network and computer systems they use. The integrity and secrecy of an individual's password is a key element of that responsibility. Each individual has the responsibility for creating and securing an acceptable password per this policy. Failure to conform to these restrictions may lead to the suspension of rights to Environmental Protection Agency (EPA) systems or other action as provided by EPA Policy.

Guidelines & Procedures

- Passwords must be changed every 90 days.
- The "reset password" process will be applied to users who logs in for the first time
- Each successive password must be unique. Re-use of the same password will not be allowed.

Strong Password Construction Guidelines

- Are at least eight alphanumeric characters long
- Passwords do not contain user ID
- Contain no more than two identical characters in a row and are not made up of all numeric or alpha characters
- Contain at least three of the five following character classes:
- Lower case characters

- Upper case characters
- Numbers
- “Special” characters (e.g. @#$%^&*() _+|~-=\` {} []:”;’<>/ etc.)
- Contain at least eight alphanumeric characters.

PART IV: EQUIPMENT ACQUISITION, MANAGEMENT, AND DISPOSAL

PURCHASING OF ICT EQUIPMENT, SOFTWARE AND SERVICES

EPA encourages the appropriate and timely acquisition of ICT equipment to support the EPA operations, including research, programs, reports, services and activities.

This section provides guidance to **EPA** in purchasing ICT equipment, software and ICT services to suit the entity needs.

The EPA ensures that all ICT equipment, software and services are used and disposed of in an ethical and responsible manner and recognises the need to be consistent, cautious and thorough in the way that these tools support the EPA operations.

This section ensures that:

- **EPA** provides quality, reliable and up-to-date equipment and software to its employees in order to provide quality Environmental services.
- The EPA complies with both legislative requirements and ethical obligations in the purchase and use of equipment, licences and other ICT supportive services.
- All staff, Board members, Projects, Contractor, Consultant and Intern students understand their responsibilities in relation to purchasing ICT equipment.

4.1 ICT tools

As defined in Section 1.3 of this policy, **EPA** identifies different types of ICT tools; this includes:

- **ICT equipment:** electronic hardware items that include computers, tablets, printers, multi-function copiers, mobile/smart phones, cameras, and data projectors.
- **ICT software:** electronic software items that include programs, operative systems, Environmental data management systems, Financial Management system and antivirus software programs.
- **ICT services:** include internet services, web hosting, website development, and IT support.

ICT purchasing or acquisition principles

The general principle underpinning this policy is that ICT purchases are made for a valid reason, in an approved way, and in alignment with the ICT Strategy.

EPA is committed to purchasing the most cost-effective ICT goods and services primarily with regard to price, but also relating to quality, reliability, service, delivery and efficiency. This may mean, for example, that a slightly higher priced item or service might be chosen if it is from a supplier that has proven to be reliable in the past.

Coordination with IT and Procurement

- All purchases of ICT equipment, software and related services must be coordinated between the Procurement Unit and the IT Department.

- No department or individual may purchase ICT items directly without prior involvement of IT and Procurement.

Bulk Purchasing of Standard Equipment

- Standard ICT equipment (e.g., laptop computers, desktop computers, printers, antivirus licenses, and printer cartridges/toner) must be purchased in bulk where possible in order to:

  - Ensure compatibility with existing systems.

  - Standardize equipment across the organization.

IT Configuration and Assignment

- The IT Department is responsible for:

- Selecting models that comply with organizational standards

- Installing and configuring operating systems, software, and security tools (including antivirus)

- Ensuring the device meets security and network requirements

- Only after IT has fully programmed and configured the computer may it be assigned to the approved user.

Non-Standard ICT Purchases

- Any request for non-standard ICT equipment, software or services must be:

- Justified in writing by the requesting department

- Reviewed and recommended by IT

- Approved by the Executive Director (or a designated authority)

- Procurement will proceed only after the necessary approvals are obtained

EPA has a commitment to consider environmental and ethical manufacturing issues wherever possible

PART V: IT ASSET DISPOSAL

Purpose

The purpose of this policy is to establish and define standards, procedures, and restrictions for the disposal of non-leased IT equipment in a legal, cost-effective manner. EPA surplus or obsolete IT assets and resources (i.e. desktop computers, printers, routers, switches, servers, databases, etc.) must be discarded according to The General Services Agency (GSA) of Liberia is the sole authority responsible for the physical disposal of government assets, including vehicles and equipment, aimed at ensuring transparency and preventing private conversion of public property. The process involves inspecting "written off" assets, establishing disposal methods (sale, donation, or destruction), and often utilizing the Asset Disposal Unit (ADU).

Therefore, all disposal procedures for unutilized IT assets must adhere to GSA - approved methods.

Scope

This policy applies to the proper disposal of all non-leased EPA ICT hardware, including PCs, printers, handheld devices, servers, databases, hubs, switches, bridges and routers. Environmental Protection Agency (EPA)-owned surplus hardware, obsolete machines, and any equipment beyond reasonable repair or reuse are covered by this policy. Where applicable, it is desirable to achieve some residual value of the IT asset in question through reselling, auctioning, donation, or reassignment to a less-critical function**.**

Guidelines

Disposal procedures of all IT assets and equipment will be centrally managed and coordinated by the Environmental Protection Agency (EPA) ICT Unit. The ICT Unit is also responsible for backing up and then wiping clean of EPA data on all IT assets slated for disposal, as well as the removal of EPA tags and/or identifying labels.

Transparent Disposal Methods:

Public Auction/Sale: Sale proceeds are typically returned, often with fixed prices determined by the GSA.

Transfer: Property can be transferred to other agencies to maximize government utility.

Destruction/Recycling: If items are not usable, they are sent for environmentally sound disposal.

Anti-Corruption Measures: Disposal must be transparent, non-discriminatory, and adhere to due process, ensuring public property is not converted to private use.

IT Asset Specialization: IT equipment requires specific handling, including data sanitization, in alignment with GSA guidelines and donor agency requirements.

Documentation: All disposals must be properly documented to ensure accountability and compliance with government auditing standards.

PART VI : ICT NETWORK

EPA understands that a quality internal communication network is a crucial component to ensure communications and business are carried out inside the Agency to allow all staff members to achieve the EPA goals and outcomes on Environmental Business

Purpose

The purpose of this policy is to provide guidance to **EPA** staff members into how the entity accesses, manages and updates the internal network.

The following processes ensure that staff members of **EPA**, Senior Management, Contractors, Consultants and volunteers' worker are provided with a reliable and stable **EPA** ICT network. This policy ensures that:

- Staff members are able to work in a shared network environment
- **EPA** Platforms files are current, secure and up-to-date
- Back-up systems and procedures are in place to protect internal documentation and Environmental Data of the Institution.
- Private and confidential information is appropriately managed according to this policy
- The network is used in a manner that is consistent with the organisation's values, legal requirements, related policies, and code of conduct.

Using Our Network and the Internet

Network Management

Our IT team manages and secures all of the EPA's networks, from the Wi-Fi in our offices to the VPN you use when working remotely. We handle all network equipment from a central point to keep things as secure as possible. You'll also see separate networks, like one for guests, which we use to add another layer of protection.

Internet Access

We provide internet for all your work needs—research, collaborating, training, and staying in touch. Feel free to use it for quick personal tasks, just as long as it doesn't interfere with your responsibilities or slow down the connection for everyone else.

Setting up user access to the ICT systems

When a new staff member (or other authorized user) commences with the Environmental Protection Agency (EPA):

- Notification by supervisor

The new user's supervisor must notify the ICT Unit Head that a new user account is required. This should be done as early as possible before the user's start date.

- Request details

The supervisor provides the ICT Unit with the following information:

- Full name
- Position title and business unit
- Employment type (ongoing, temporary, contractor, etc.)
- Start date (and end date, if applicable)
- Required systems and level of access
- Any special access requirements (e.g. shared mailboxes, specific applications)

- Account creation

The ICT Unit Head (or delegate) arranges for:

- Creation of a new login on the EPA network platform
- Allocation of appropriate access rights based on the user's role
- Creation of email and any other required system accounts

- Credentials and induction

- ICT securely provides login credentials to the new user.
- The user is briefed on ICT usage policies, security requirements (passwords, MFA, etc.), and their responsibilities under EPA's ICT policies.

- Record-keeping

ICT records the account creation details and retains the supervisor's request for audit and compliance purposes.

The **ICT unit** will undertake the following tasks:

- Ensure the new user has access to the network, all EPA Platforms, including the Integrated automatic and Finical management system of EPA.
- Create a new network user account with the appropriate access levels.
- Ensure the new user has printer access
- Create a new email account
- Allocate a log-in for other internal systems

- Assist the new user to set up their email access through **EPA Email server** and to change passwords
- Explain to the new user the network and filing map, how to use the smart phone (if applicable.
- Provide a copy of this policy and explain where to find information or seek assistance about particular issues relating to EPA ICT policy.
- Support new users to use other internal ICT equipment and systems

Deleting a user or removing their access to the EPA ICT systems

When a staff member/or other user is no longer employed/contracted by EPA**,** or when directed by the Executive heads to disable a current user's account, the **ICT unit is** to undertake the following tasks:

- Disable the user's access/delete their log-in details in relation to the computer network and other internal systems
- Consult with the Executive Director as to whether emails to the former user should be forwarded to another staff member or whether the account should be deleted
- Remove the user's name from the internal EPA email system.

Levels of access

EPA server(s) consists of 500TB of drive(s) with certain access restrictions. This is set out in Section 3.4 of this policy. The **ICT unit** is to ensure that individual staff members or other users are provided with the appropriate levels of access.

Unauthorised access to or interference of data

Unauthorised access or deliberately modifying or damaging **EPA** data is a violation of this policy and the organisational Code of Conduct, and may result

Accessing the Cloud base network Platform from home

EPA staff may access the network from home by connecting to the EPA integrated ERP Server, from our host provider server once authorised to do so. Log-in details are provided by the ICT unit.

Staff working offsite should be aware that they have a responsibility to comply with EPA ICT policies. This means they cannot jeopardise the information security, privacy and confidentiality of the network. Wherever possible, they do not access the network on computer equipment systems that are readily accessible by, or shared with, the general public. Where staff access the network from home, they must ensure passwords for access are secure from other regular or occasional users of that computer, including friends and family.

Maintenance of ICT equipment
Staff are required to take reasonable precautions to protect EPA IT equipment from damage, loss or theft.

If staff members want to change or modify equipment that is provided to them by the organisation for work purposes, they must seek approval from their manager through the Executive Director and the ICT unit.
Here is a concise draft you can adapt as a "Confidentiality Bond / Agreement" for ICT Administrators and ICT Staff managing EPA systems and information.

ICT CONFIDENTIALITY BOND / AGREEMENT

Purpose

The purpose of this Agreement is to ensure that all ICT Administrators and ICT staff who have access to EPA information systems, networks, applications, and data understand and accept their obligations to protect the confidentiality, integrity, and availability of EPA information.

Scope

This Agreement applies to:

- All EPA ICT systems, networks, servers, applications, databases, cloud services, communication systems, and related infrastructure.

- All information processed, stored, transmitted, or accessed using EPA ICT resources, whether in electronic or hard-copy form.

- All EPA-related information, including but not limited to:
  - Environmental data, research, and reports.
  - Regulatory, enforcement, and compliance information
  - Personal data of staff, contractors, and stakeholders
  - Procurement, financial, and contractual information
  - Any information marked or reasonably understood to be confidential

Confidentiality Obligations

The Employee agrees to:

Non-disclosure

- Not disclose, share, or discuss any EPA information with unauthorized persons, whether inside or outside the Agency, during or after employment.
- Not post or share EPA confidential information on social media, public forums, or any non-approved platform.

Authorized Use Only

- Access EPA systems and information solely for official, authorized work purposes.
- Use only authorized user accounts, credentials, tools, and methods to access systems and data.

Protection of Credentials

- Keep usernames, passwords, tokens, encryption keys, and other access credentials strictly confidential.
- Not share accounts or login details with any person, including colleagues, supervisors, contractors, or vendors.

Data Handling and Storage

- Store and handle EPA data securely, in accordance with EPA ICT and Information Security Policies.
- Not copy, remove, transmit, or store EPA data on personal devices, external media, or third-party services without formal written authorization.

System Administration Responsibilities

- Exercise heightened care when performing system administration tasks (e.g., backups, user management, configuration, maintenance, and monitoring).
- Access logs, emails, files, or user data only where strictly required for official duties, and keep all such information confidential.

Third-Party and Vendor Access

- Ensure any third-party or vendor access to EPA systems is authorized, monitored, and consistent with EPA policies and relevant contracts.
- Not provide external parties with access or data without formal approval.

Return / Destruction of Information

- Upon request, or upon termination of employment or role change, return or securely destroy all EPA information and assets in the Employee's possession, including copies and backups, in line with EPA policy.

Compliance with Policies and Laws

The Employee agrees to:

- Comply with all EPA ICT, Information Security, Data Protection, Records Management, and related policies, procedures, and guidelines.
- Comply with all applicable national laws and regulations concerning privacy, data protection, cybersecurity, intellectual property, and public sector information.
- Attend and complete mandatory ICT security and confidentiality training as required by EPA.

Reporting Obligations

The Employee shall:

- Immediately report any suspected or actual information security incident, data breach, loss, or unauthorized access/use of EPA systems or information to the appropriate authority (e.g., ICT head,).
- Cooperate fully in any investigation, audit, or review related to ICT security or confidentiality incidents.

Duration of Obligations

- These confidentiality obligations take effect from the date of signing and continue:
  - For the entire period of employment or engagement with EPA; and
  - After cessation of employment or engagement, for as long as the information remains confidential or as otherwise required by law.

Breach and Consequences

The Employee acknowledges that:

- Any violation of this Agreement, or of EPA ICT and Information Security policies, may result in:
  - Disciplinary action (up to and including termination of employment);
  - Civil or criminal liability under applicable laws;
  - Personal liability for damages or losses suffered by EPA due to the breach (where permitted by law).

- EPA reserves the right to monitor, audit, and log use of its ICT systems in accordance with applicable laws and internal policies.

SERVER BACKUP

Environmental Data, including EPA websites, email data and Financial Data transactions are important assets. In order to protect this asset from loss or destruction, it is imperative that it be safely and securely captured, copied, and stored. The goal of this policy is to govern how and when data residing on the EPA cloud backup servers will be backed up and stored for the purpose of providing restoration capability. In addition, it will address methods for requesting backed-up data to be restored to individual systems.

Key principles and standards — why we do things this way

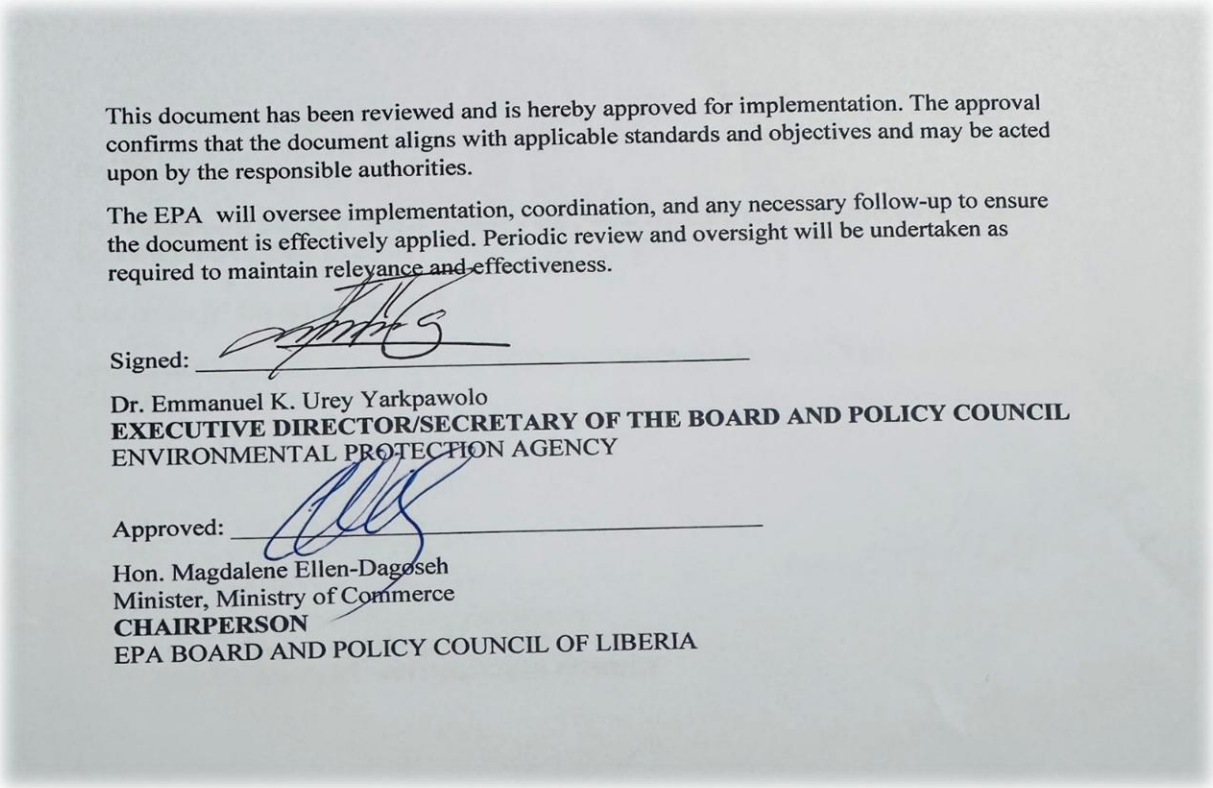
The EPA's ICT approach is grounded in international best practice to ensure robust, repeatable and auditable security outcomes. We follow ISO/IEC 27001 and ISO/IEC 27002 to establish an information security management system (ISMS) and to implement proven technical and organisational controls. These standards provide a structured framework for risk assessment, policy governance, control selection, continual improvement and formal audit — enabling the Agency to manage confidentiality, integrity and availability consistently across people, processes and technology. We also draw on the NIST Cybersecurity Framework and relevant NIST Special Publications (including the SP 800 series) for practical guidance on identifying, protecting, detecting, responding to and recovering from cyber threats; NIST SP 800-88, in particular, informs secure media sanitation and disposal practices.

At the national level, EPA aligns its procedures with Liberia's legal and administrative guidance to ensure compliance and public accountability. The Ministry of Justice IT Asset Disposal Guidelines and the General Services Agency (GSA) disposal rules define the lawful, transparent steps for retiring and disposing of government IT assets; our processes for sanitizing storage media, documenting disposals, and coordinating transfers or sales follow that guidance. The Civil Service Agency HR Policy Manual shapes how we integrate access control, onboarding, training and disciplinary measures into human resources practice, while the Public Procurement and Concessions Act governs how we source ICT goods and services in a manner that is fair, auditable and consistent with national procurement rules.

Combining international standards with Liberia-specific guidance gives the EPA a balanced approach: global technical rigor and resilient operational controls, plus legal conformity and local accountability. This combination helps protect environmental and personal data, preserves public trust, supports donor and partner requirements, and ensures that ICT decisions are defensible, auditable and sustainable.

Fundamental principles:

- Least privilege: access only for job needs.
- Defense in depth: multiple controls (endpoint, network, backup).
- Accountability and transparency: auditable records and documented decisions.
- People first: training, clear instructions and support.



This document has been reviewed and is hereby approved for implementation. The approval confirms that the document aligns with applicable standards and objectives and may be acted upon by the responsible authorities.

The EPA will oversee implementation, coordination, and any necessary follow-up to ensure the document is effectively applied. Periodic review and oversight will be undertaken as required to maintain releyance and effectiveness.

Signed: _____

Dr. Emmanuel K. Urey Yarkpawolo
EXECUTIVE DIRECTOR/SECRETARY OF THE BOARD AND POLICY COUNCIL
ENVIRONMENTAL PROTECTION AGENCY

Approved: _____

Hon. Magdalene Ellen-Dagoseh
Minister, Ministry of Commerce
CHAIRPERSON
EPA BOARD AND POLICY COUNCIL OF LIBERIA