AUTHORIDADE REGIONAL
REGULADORA DE ELETRICIDADE DA CEDEAO

ECOWAS REGIONAL
ELECTRICITY
REGULATORY AUTHORITY

AUTORITÉ DE RÉGULATION
RÉGIONALE DU SECTEUR DE
L'ÉLECTRICITÉ DE LA CEDEAO

Energy Commission Building, Ghana Airways Avenue, Airport Residential Area, PMB 76 Ministries Post Office, Accra – GHANA
TEL: (+233) 0302 817 047 (+233) 0302 817 049 FAX: (+233) 0302 817 050 WEBSITE: www.erera.arrec.org EMAIL: info@erera.arrec.org

RESOLUTION Nº 019/ERERA/26
Adoption of the ICT Policies and Procedures Manual

At the meeting of the Regulatory Council held on 27 February 2026, in Cotonou, Republic of Benin, the Regulatory Council:

(a) Recalling that ERERA, as a specialized institution of ECOWAS established in 2008, is mandated to regulate cross-border electricity exchanges and support the development of the Regional Electricity Market;

(b) Considering the growing reliance of ERERA on Information and Communication Technologies (ICT) for regulatory, administrative, financial, and coordination functions;

(c) Recognizing the need to institutionalize a comprehensive ICT governance framework to ensure the confidentiality, integrity, availability, and resilience of ERERA's information systems and digital assets;

(d) Taking note of the work carried out by the ICT Unit and the IT Steering Committee, including the review of the draft ICT Policies and Procedures and the incorporation of proposed amendments for finalization;

(e) Considering further that the ICT Policies and Procedures Manual consolidates governance principles, operational standards, security controls, compliance requirements, and implementation mechanisms in alignment with international best practices and ECOWAS institutional frameworks

(f) Having reviewed the final version of the ICT Policies and Procedures Manual;

RESOLVED THAT

1. The ICT Policies and Procedures Manual, copy attached to this Resolution, is hereby approved, and adopted by the Regulatory Council as the official and binding framework governing ICT management, security, operations, data governance, and compliance within ERERA.

2. The ICT Unit shall ensure the effective implementation, communication, monitoring, and periodic review of the Manual in accordance with the established ICT Policy Management Lifecycle.

3. All ERERA staff, consultants, contractors, and third-party service providers granted access to ERERA's ICT environment shall comply with the provisions of the ICT Policies and Procedures Manual of ERERA.

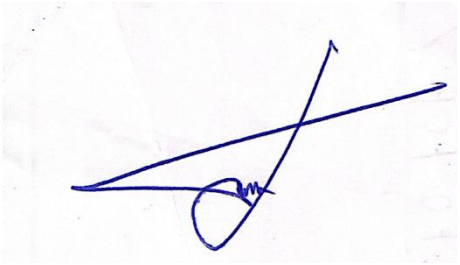
4. The Manual shall enter into force on the date of adoption and shall be published in the ERERA Official Bulletin and on the official website of ERERA.

Made in Cotonou, Republic of Benin, on February 27, 2026

Charles NDIAYE

Council MEMBER, Legal

Kocou Laurent Rodrigue Tossou



Chairman

ICT POLICIES AND PROCEDURES MANUAL

Document Control

Version	Effective Date	Description of Change	Status
1.0	29/09/2015	Initial Release	Approved
2.0	27/02/2026	Major Review	Approved

TABLE OF CONTENTS

1 INTRODUCTION

1.1 Background and Rationale

The **ECOWAS Regional Electricity Regulatory Authority (ERERA)** is a specialized institution of the Economic Community of West African States (ECOWAS), established in 2008 by decision of the Authority of Heads of State and Government. ERERA's principal mandate is to regulate cross-border electricity exchanges and to facilitate the establishment of a regional electricity market through harmonized regulation and support to national regulators.

As ERERA's operational and strategic responsibilities expand within the evolving West African Power Pool (WAPP) framework, the role of Information and Communication Technologies (ICT) becomes increasingly critical. ERERA relies on ICT systems to perform a wide range of regulatory, administrative, technical, and coordination functions. These include electronic communication, data analysis, stakeholder collaboration, regulatory monitoring, remote service delivery, and support for complex applications such as **ECOLINK (SAP)** and **Microsoft 365**.

However, as ICT grows in scope and sophistication, so do the risks—ranging from cyber threats and data breaches to system downtime, misconfigurations, and vendor dependency. To ensure that ICT continues to serve as an enabler of ERERA's strategic goals rather than a source of vulnerability, the organization must institutionalize a robust ICT governance and policy framework.

The **development of the ICT Policies and Procedures Manual** is both a response to these organizational needs and a proactive step toward institutional resilience, compliance, and efficiency. The manual aims to define a coherent structure for managing ICT resources, mitigating ICT-related risks, aligning ICT services with ERERA's mission, and supporting continuous improvement in performance and accountability.

1.2 Purpose of the ICT Policies and Procedures

This manual is the definitive guide for all matters related to ICT governance, operations, security, and compliance at ERERA. It consolidates principles, directives, best practices, and operational procedures that together serve to:

- **Establish governance clarity**: Define who is responsible for what, from strategic leadership to day-to-day operations;
- **Standardize ICT practices**: Provide a uniform approach to service delivery, change management, cybersecurity, procurement, and user behavior;
- **Protect digital assets**: Ensure confidentiality, integrity, availability, and resilience of information and systems;

- **Ensure legal and regulatory compliance**: Meet internal ECOWAS regulations and international standards (e.g., ISO/IEC 27001);
- **Promote efficient ICT resource utilization**: Optimize infrastructure, software, personnel, and vendor performance;
- **Support strategic alignment**: Link ICT investments and operations with ERERA's regulatory and development goals.

The manual is a living document, designed to be updated periodically in response to new technologies, emerging risks, and evolving institutional priorities.

1.3 Scope and Applicability

This policy and procedures manual applies comprehensively to the use, management, and oversight of ICT resources across ERERA. It governs all individuals, systems, and processes that interact with the organization's ICT environment. Specifically, it applies to:

- **ERERA Personnel**: Full-time staff, consultants, interns, contractors, and any individuals granted access to ERERA ICT systems;
- **Infrastructure and Platforms**: Hardware, servers, storage systems, networking devices, cloud platforms, and mobile devices;
- **Software Systems**: All applications used for administrative, regulatory, financial, HR, and communications purposes (including ECOLINK, Microsoft 365, antivirus platforms, etc.);
- **Data and Communications**: All forms of data (structured and unstructured), including regulatory submissions, emails, backups, logs, metadata, and user-generated content;
- **Third-Party Vendors**: Any service providers or contractors involved in ICT services, software development, cloud hosting, or IT support.

The scope covers both on-premises and remote/cloud-based systems and is applicable regardless of geographic location, as long as the activity pertains to ERERA's operations.

1.4 Reference Standards and Strategic Alignment

The manual is designed in accordance with best practices and compliance requirements drawn from the following international, regional, and institutional frameworks:

- **ISO/IEC 27001:2022** – For establishing an Information Security Management System (ISMS), focusing on protecting data confidentiality, integrity, and availability;
- **ISO/IEC 20000-1** – For IT Service Management, ensuring that ICT services meet business needs and expectations;

- **COBIT 2019** – For comprehensive ICT governance, aligning ICT processes with enterprise objectives and value creation;
- **ITIL v4** – For operational excellence in ICT service delivery, change management, incident handling, and capacity planning;
- **ECOWAS Institutional Frameworks**, including:
    - The **ECOWAS Procurement Code** (2021), guiding acquisition and vendor management;
    - The **ECOWAS Records and Asset Management Policies**, influencing data handling, record-keeping, and infrastructure control, Records management, Assets Management…

In addition, this manual is aligned with ERERA's existing internal documents, including the **2015 ICT Policy Framework** and builds upon them to ensure continuity, relevance, and expansion.

1.5 Intended Users and Institutional Impact

This manual is intended for a diverse audience within ERERA, including:

- Senior Management and the Regulatory Council (for governance and oversight);
- ICT Unit (for implementation, monitoring, and technical administration);
- Department Heads (for aligning ICT usage with operational needs);
- All Staff (for guidance on acceptable use, data handling, and incident reporting);
- External Consultants and Vendors (to understand compliance obligations).

The broader institutional impact of this manual includes strengthened cybersecurity posture, improved service delivery, regulatory compliance, efficient resource management, and enhanced institutional credibility in the ECOWAS energy regulatory landscape.

2 DEFINITIONS AND ACRONYMS

This section provides a common understanding of key ICT-related terms and abbreviations used throughout the ERERA ICT Policies and Procedures Manual. Standardized definitions ensure consistent interpretation and application across all departments, users, and external partners.

2.1 Glossary of Terms

Term	Definition
Access Control	Mechanisms and processes that restrict access to systems, networks, or data to authorized users only.
Application	A software program used by ERERA to perform specific functions such as communication, data analysis, or regulatory monitoring.
Asset	Any item of value to ERERA's ICT operations, including hardware, software, data, or services.
Authentication	The process of verifying the identity of a user, device, or system before granting access.
Backup	A copy of data made to restore information in case of loss, corruption, or system failure.
Business Continuity (BC)	The ability of ERERA to maintain essential functions during and after a disruption.
Change Advisory Board (CAB)	A governance group responsible for evaluating and approving significant ICT changes.
Confidentiality	Assurance that information is accessible only to those authorized to have access.
Configuration Item (CI)	A component (hardware, software, documentation) that is subject to configuration management.
Data Classification	Categorization of data based on its level of sensitivity and the impact to ERERA if compromised.
Data Custodian	Technical personnel responsible for maintaining the infrastructure supporting specific data.
Data Integrity	The accuracy, consistency, and reliability of data throughout its lifecycle.

Term	Definition
Data Owner	An individual or department accountable for data access, quality, and classification.
Data Protection Officer (DPO)	A designated role responsible for ensuring ERERA's compliance with data protection regulations.
Disaster Recovery (DR)	A set of procedures for restoring ICT systems and operations after a major disruption or failure.
Encryption	The process of converting information into a coded format to prevent unauthorized access.
Group Policy Object (GPO)	A set of rules applied within Active Directory to control user and system behavior.
Incident	Any event that threatens the confidentiality, availability, or integrity of ERERA's ICT environment.
Information Security	The practice of protecting information from unauthorized access, use, disclosure, disruption, modification, or destruction.
IT Infrastructure	The combined set of hardware, software, networks, and facilities used to support ICT services.
Malware	Malicious software, such as viruses, worms, trojans, or spyware, intended to damage or disrupt systems.
Multi-Factor Authentication (MFA)	A security mechanism that requires more than one method of authentication to verify user identity.
Patch	A software update that addresses security vulnerabilities or corrects functionality issues.
Policy	A formal rule or directive that guides decisions and behavior related to ICT use and governance.
Procedure	A set of documented steps to implement policies and carry out operational tasks.
Recovery Point Objective (RPO)	The maximum amount of data loss (measured in time) that ERERA can tolerate during a disruption.
Recovery Time Objective (RTO)	The maximum allowable time for restoring a system or process following an incident.

Term	Definition
Risk Assessment	The process of identifying, analyzing, and evaluating ICT-related threats to operations.
Service Level Agreement (SLA)	A formal contract that defines performance expectations between ERERA and a service provider.
Single Point of Failure (SPOF)	A component whose failure would cause a complete system or service outage.
System of Record (SoR)	The authoritative source of a specific piece of business data.
User	Any individual authorized to access ERERA ICT systems, including staff, consultants, or partners.
Vulnerability	A flaw or weakness in a system that could be exploited to cause harm or unauthorized access.

2.2 Acronyms

Acronym	Meaning
AD	Active Directory
AUP	Acceptable Use Policy
BC/DR	Business Continuity / Disaster Recovery
CAB	Change Advisory Board
CI	Configuration Item
COTS	Commercial Off-The-Shelf Software
DR	Disaster Recovery
DPO	Data Protection Officer
ECAB	Emergency Change Advisory Board
ERERA	ECOWAS Regional Electricity Regulatory Authority
ECOWAS	Economic Community of West African States
ERP	Enterprise Resource Planning

Acronym	Meaning
GPO	Group Policy Object
HR	Human Resources
ICT	Information and Communication Technology
IDS	Intrusion Detection System
IP	Internet Protocol
ISMS	Information Security Management System
ISO	International Organization for Standardization
ITIL	Information Technology Infrastructure Library
LAN	Local Area Network
MFA	Multi-Factor Authentication
MTD	Maximum Tolerable Downtime
NDA	Non-Disclosure Agreement
OS	Operating System
PIA	Privacy Impact Assessment
RFC	Request for Change
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SAP	Systems, Applications, and Products (ECOLINK)
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SoD	Segregation of Duties
SoR	System of Record
SPOF	Single Point of Failure
SSID	Service Set Identifier

Acronym	Meaning
UPS	Uninterruptible Power Supply
VPN	Virtual Private Network
WAN	Wide Area Network
WAPP	West African Power Pool

3 POLICY GOVERNANCE AND OVERSIGHT

The effective management of information and communication technology (ICT) is essential for ERERA to fulfill its mandate as the regional electricity regulatory authority. This section provides the governance framework that defines how ICT policies are created, approved, implemented, reviewed, and enforced. It ensures that all ICT policies are strategically aligned, operationally practical, and institutionally accountable.

3.1 Governance Structure

ERERA's ICT governance is structured across three levels to ensure full oversight, policy coherence, and cross-departmental engagement.

- **Strategic Oversight**

At the apex, the **Regulatory Council** and **Executive Management** provide strategic direction. They are responsible for endorsing ICT policies, approving ICT budgets, and ensuring ICT initiatives support ERERA's regulatory and institutional priorities.

- **Operational Management**

The **ICT Department / Unit** is the central policy custodian. It develops and implements ICT policies, manages technology services, monitors compliance, and serves as the technical adviser to senior leadership. It also coordinates across departments to support digital transformation, risk mitigation, and service delivery.

- **Internal Control and Support Functions**

Other departments such as **Finance**, **Legal Unit**, **Internal Audit**, and **Human Resources** provide technical input, risk reviews, legal vetting, and compliance support throughout the policy lifecycle.

Governance Level	Entities Involved	Key Responsibilities
Strategic Oversight	Regulatory Council,	Approve policies, ensure strategic alignment, oversee ICT investments
Operational Management	ICT Department	Draft policies, manage ICT services, train users, monitor compliance
Internal Support & Control	Legal, Audit, Finance, HR	Provide legal vetting, financial oversight, and audit assurance

Table 1 ICT Governance Structure

3.2 ICT Governance Policy

3.2.1 Purpose

The purpose of the ICT Governance Policy is to establish a structured framework for the strategic direction, management, and oversight of information and communication technology (ICT) within ERERA. The policy ensures that ICT is governed in a way that aligns with ERERA's regulatory mandate, institutional priorities, and regional commitments under ECOWAS.

This policy is necessary to:

- Improve accountability in ICT decision-making;
- Align ICT investments and services with organizational goals;
- Minimize risk through structured governance controls;
- Promote transparency and performance-driven ICT management.

3.2.2 Scope

This policy applies to:

- All ICT activities conducted within or on behalf of ERERA;
- All departments and units using ERERA ICT infrastructure and services;
- All ICT systems, including hardware, software, cloud-based services, and data assets;
- All personnel, including staff, consultants, vendors, and temporary workers with access to ERERA's ICT environment.

Excluded from this policy are ICT systems managed independently by ECOWAS Commission entities unless explicitly delegated to ERERA for oversight.

3.2.3 Roles and Responsibilities

Role	Responsibility
Regulatory Council	Final approver of ICT governance policy and strategic ICT investments
IT Steering Committee	Reviews and endorses ICT governance policies and initiatives; aligns ICT strategy with organizational goals; prioritizes major ICT investments and projects
IT Officer / ICT Unit	Drafts and updates policy; ensures implementation and reporting
Internal Audit	Reviews effectiveness and compliance of ICT governance practices
Legal Unit	Verifies policy compliance with ECOWAS and national ICT laws
Departmental Heads	Ensure local ICT practices comply with governance directives

All Users (Staff, Vendors)	Adhere to governance policy and participate in ICT-related compliance activities

Table 2 Key Roles and Governance Responsabilities

3.2.4 Policy Statement

ERERA commits to implementing a proactive, integrated, and performance-driven ICT governance model. This policy sets out the high-level expectations for how ICT will be directed, controlled, and evaluated across the organization.

The objectives of this policy are to:

- Ensure that ICT investments deliver measurable value to ERERA and its stakeholders;
- Align ICT initiatives with the regulatory and business needs of the Authority;
- Establish clear accountability for ICT decision-making, risk management, and service delivery;
- Promote sustainability, innovation, and ethical use of technology across the institution.

This governance model shall be applied uniformly to all ICT-related initiatives, projects, services, and third-party engagements.

3.2.5 Guiding Principles / Key Directives

This policy is guided by the following COBIT 2019-aligned and ERERA-specific principles:

- **Strategic Alignment**: ICT planning and activities must align with ERERA's business strategy and regulatory goals.
- **Value Delivery**: All ICT projects and services must be assessed for return on investment and business impact.
- **Risk Management**: ICT-related risks (cybersecurity, legal, operational) must be proactively identified, assessed, and mitigated.
- **Resource Optimization**: ICT resources must be allocated and utilized efficiently and transparently.
- **Governance & Management Separation**: Strategic oversight and operational execution must be clearly delineated.
- **Performance Measurement**: ICT service levels, user satisfaction, and policy compliance must be regularly monitored and reported.

These principles also reflect ECOWAS ICT governance expectations and are intended to promote uniformity and interoperability across institutions.

3.2.6 Compliance and Enforcement

ERERA enforces this policy through a combination of oversight, audit, and training. Compliance will be ensured through the following mechanisms:

- **Annual Governance Audits** conducted by Internal Audit;
- **Quarterly Performance Reports** from the ICT Department/Unit to Executive Management;

- **Policy Awareness Training** delivered to all staff annually;
- **Procurement Reviews** to ensure ICT purchases comply with governance controls;
- **Monitoring Tools** to track KPIs such as system availability, policy violations, and user support metrics.

Failure to comply with this policy may result in:

- Written warnings or disciplinary action for staff;
- Suspension or termination of vendor contracts;
- Escalation to the Regulatory Council for systemic governance violations.

3.2.7 Supporting Procedures

The following procedures support the effective implementation of the ICT Governance Policy:

Procedure	Purpose
ICT Policy Development Procedure	Outlines steps for drafting, reviewing, approving policies
ICT Strategic Planning Procedure	Guides annual ICT planning in alignment with business needs
ICT Budgeting and Procurement Procedure	Ensures cost-effective, compliant ICT purchasing
ICT Performance Measurement and Reporting SOP	Defines KPIs and reporting timelines
ICT Risk Management Procedure	Establishes ICT risk identification, scoring, mitigation
Vendor and Contract Governance Checklist	Ensures vendors meet ERERA's governance expectations
ICT Governance Review Template	Used for periodic governance assessment and improvement

Table 3 List of Supporting Procedures

These procedures are maintained by the ICT Unit and are reviewed in line with the governance policy's review cycle.

3.3 ICT Strategy and Business Alignment

To ensure ICT investments contribute directly to ERERA's mission, all technology decisions must be aligned with business needs. This is operationalized through:

- An **ICT Strategic Plan**, reviewed every 3–5 years;
- Annual ICT work plans developed in collaboration with all departments;
- Strategic mapping of ICT initiatives to regulatory and operational priorities.

ICT alignment is assessed using a **Business-IT Alignment Matrix**, which maps each major ICT initiative to:

- Functional goals (e.g., improved reporting, better stakeholder engagement);
- Compliance goals (e.g., GDPR, ISO/IEC 27001);
- Efficiency goals (e.g., automation, reduced downtime).

3.4 ICT Budget Planning and Management

ICT budget management ensures that financial planning for technology is proactive, transparent, and aligned with performance expectations.

Key Budgeting Principles:

- ICT budgets cover both **capital** (e.g., equipment) and **operational** (e.g., licensing, support) expenditures;
- Budget requests are submitted annually and must include justifications, cost estimates, and implementation timelines;
- All procurement activities are conducted under the **ECOWAS Procurement Code**;
- Major expenditures are tracked quarterly against defined Key Performance Indicators (KPIs).

Category	Examples
Capital Expenditure (CapEx)	Laptops, servers, network switches, data centers
Operational Expenditure (OpEx)	Software licenses, cloud subscriptions, support
Services	Training, IT consulting, cybersecurity services
Contingency and Risk	Disaster recovery, emergency repairs

Table 4 ICT Budget Components

3.5 ICT Policy Management Lifecycle

ICT policies are not static documents—they must evolve with technology, laws, and institutional needs. ERERA follows a structured lifecycle for all ICT policies.

Figure 1 ICT Policy Lifecycle Stages

Stage	Description
1. Drafting	The ICT Unit initiates the drafting process using relevant international standards (ISO/IEC, COBIT), ECOWAS practices, and internal consultations.
2. Validation	The draft is reviewed by Legal Unit (compliance), Internal Audit (controls), and HR (staff impact) for consistency and organizational fit.
3. Approval	Policy is submitted to Executive Management for review and then formally approved by the Regulatory Council.
4. Communication	Policy is shared via intranet, onboarding packages, departmental meetings, and staff orientation to ensure institutional awareness.
5. Implementation	ICT Unit coordinates rollout, monitors adherence, supports integration into business processes, and provides technical guidance.

6. Review	Formal reviews are scheduled every two (2) years, or earlier if triggered by legal, operational, or technological changes.
7. Amendment	Updates are made based on feedback, audits, or emerging needs, then passed through the same lifecycle stages: drafting → validation → approval.

Each policy must be accompanied by:

- Version history;
- Named policy owner;
- Reference to related procedures and standards;
- Archiving of obsolete versions.

3.6 Roles and Responsibilities

Effective policy governance depends on clear accountability. Each actor within ERERA has distinct responsibilities to ensure ICT policies are followed and continuously improved.

Role	Responsibilities
Regulatory Council	Final policy approval; strategic oversight
IT Steering Committee	Endorses policies; provides ICT strategic direction; oversees IT performance
Executive Management	Approves budgets; allocates resources; ensures compliance
IT Officer / Department	Drafts policies, leads implementation, reports compliance
Heads of Departments	Ensure departmental compliance; provide input for planning
Internal Audit	Audits effectiveness and policy implementation
Legal Unit	Verifies legal soundness; ensures ECOWAS alignment
All Staff	Comply with policies; participate in training; report breaches
Third-Party Vendors	Adhere to contractual ICT requirements; submit to compliance checks

Table 5 Roles and Responsibilities

3.7 Policy Review and Amendment Process

All ICT policies are subject to periodic review to ensure relevance, compliance, and performance effectiveness. The **review cycle is every two (2) years**, unless triggered earlier by:

- Major changes in legislation or ECOWAS regulations;

- Audit recommendations;
- Security incidents or operational gaps;
- User feedback or process evolution.

3.7.1 Amendment Process

- **Initiation**: Request submitted using the Policy Change Request Form.
- **Review**: Handled by ICT Unit, with input from Legal and Internal Audit.
- **Approval**: Cleared by Executive Management and endorsed by the Regulatory Council.
- **Publication**: Revised version replaces the previous edition in all official repositories.

All changes are documented in a **version control log**, which includes:

- Date of change;
- Summary of modifications;
- Author and reviewers;
- Approving authority.

4 ICT POLICY DOMAINS

This section presents the core domains that collectively form the foundation of ERERA's ICT governance, operational efficiency, risk management, and regulatory compliance. Each domain is designed to address a specific area of ICT management and service delivery, ensuring that policies are targeted, actionable, and aligned with both organizational needs and internationally recognized standards such as **ISO/IEC 27001**, **ITIL 4**, and **COBIT 2019**.

The domains reflect the diverse and evolving nature of ICT responsibilities within ERERA, ranging from cybersecurity and infrastructure management to data governance and business continuity. Each policy domain is structured to clearly outline the **objectives**, articulate the **relevant policies**, and provide a reference to the **supporting procedures** that guide daily operations and compliance.

By organizing policies thematically, ERERA aims to:

- Simplify policy interpretation and access for staff, partners, and vendors;
- Promote a risk-based approach to ICT management;
- Ensure consistency across departments and functions;
- Facilitate monitoring, auditing, and continuous improvement.

This modular structure also allows for easier updates and scalability as technology, threats, and institutional priorities evolve.

Structure of Each Domain

Each ICT policy domain will follow a consistent format:

- **Domain Objectives**
  A concise description of what the domain aims to achieve in support of ERERA's mission and operational integrity.
- **Relevant Policies**
  A list of specific policies that govern the domain's responsibilities, aligned with applicable standards and internal practices.
- **Supporting Procedures**
- A set of procedures that operationalize each policy, including workflows, responsibilities, and templates or forms required for compliance.

The domains outlined in this section are:

- **4.1 Information Security**
- **4.2 IT Operations, Infrastructure, and Applications**
- **4.3 Data Governance and Privacy**
- **4.4 Risk Management, Business Continuity, and Disaster Recovery**
- **4.5 IT Governance, Organization, and Communications**

Each of these domains will be treated as a stand-alone policy area while contributing to the overall resilience, effectiveness, and accountability of ERERA's ICT environment.

4.1 Information Security

The objective of the Information Security domain is to ensure that all information and ICT assets within ERERA are protected from unauthorized access, disruption, alteration, and loss. This domain establishes a comprehensive framework for safeguarding ERERA's data and systems in accordance with international standards (ISO/IEC 27001) and ECOWAS directives.

Specifically, this domain aims to:

- Preserve the **confidentiality**, **integrity**, and **availability** of ERERA's digital and physical information assets;
- Ensure that only authorized individuals have access to sensitive systems and data;
- Minimize the risk of cyber threats, insider breaches, and unintentional data loss;
- Define protocols for incident detection, response, and recovery;
- Promote a security-aware culture among staff and stakeholders;
- Ensure compliance with legal, regulatory, and ECOWAS data protection standards.

This domain underpins all other ICT functions by establishing a trusted digital environment for operations, regulatory oversight, and stakeholder engagement.

4.1.1 Information Security Policy

4.1.1.1 Purpose

The purpose of this policy is to establish a comprehensive, organization-wide framework for managing information security at ERERA. It sets the strategic direction, governance expectations, and commitment of the Authority to protecting its information assets and technology infrastructure. This overarching policy is supported by a set of domain-specific sub-policies that address key control areas in detail.

Information security is critical to ERERA's ability to fulfill its regulatory mandate and maintain stakeholder trust. This policy affirms ERERA's alignment with international standards (ISO/IEC 27001), regional frameworks (ECOWAS), and global best practices in safeguarding confidentiality, integrity, and availability of information.

4.1.1.2 Scope

This policy applies to all:

- **Information types**: Including but not limited to emails, reports, regulatory data, personnel records, and system logs—whether stored physically or digitally.
- **Systems and infrastructure**: All hardware, software, databases, network components, and cloud services used by or connected to ERERA systems.
- **Users**: All ERERA employees, consultants, contractors, vendors, interns, and third parties with access to ERERA's ICT resources.

- **Locations**: All ERERA-managed facilities, remote work environments, and mobile or cloud-based systems.

This policy excludes non-official personal systems or assets not connected to the ERERA network. It serves as the foundational policy for all other information security directives and procedures.

4.1.1.3 Roles and responsibilities

Role	Responsibility
Regulatory Council	Approves the policy and ensures executive alignment with ERERA's strategic goals.
IT Steering Comittee	Reviews and endorses the ICT policy before submission to the Regulatory Council.
IT Officer	Owns this policy and ensures its application through subordinate policies.
System Administrators	Implement system-level controls as defined in supporting sub-policies.
Internal Audit	Monitors compliance and evaluates effectiveness of the security program.
All Users	Comply with all information security rules and participate in awareness programs.

Table 6 Roles and Responsabilties - Information Security Policy

4.1.1.4 Policy Statement

ERERA is committed to maintaining a secure and resilient information environment. All information assets must be protected from unauthorized access, alteration, loss, or destruction through appropriate governance, technology, and user behavior. This policy affirms that information security is a shared responsibility and must be embedded in all business processes.

To operationalize this commitment, ERERA has developed a suite of supporting policies that define control requirements, procedures, and roles across all major domains of information security.

4.1.1.5 Guiding Principles / Key Directives

The implementation of this policy shall be guided by the following principles:

- **Leadership Commitment**: Security governance will be driven by top management and aligned with ERERA's institutional priorities.
- **Risk-Based Approach**: Security measures shall be implemented based on criticality of assets, assessed threats, and business impact.
- **Layered Controls**: Security protections shall be implemented in layers (technical, administrative, physical).

- **Continuous Improvement**: Controls, policies, and awareness efforts shall be reviewed periodically and improved based on audit findings, incidents, and changing risks.
- **Integration with ICT Governance**: This policy is embedded in ERERA's broader ICT policy lifecycle (Section 3).

4.1.1.6 Supporting Policies

This umbrella policy is supported by the following sub-policies, which together form ERERA's full Information Security Framework:

Policy No.	Policy Title	Focus Area
4.1.2	**Access Control and User Management Policy**	Role-based access, account creation, and deactivation
4.1.3	**Password Management Policy**	Password strength, renewal, confidentiality
4.1.4	**Antivirus and Endpoint Protection Policy**	Device-level protection, antivirus software enforcement
4.1.5	**Patch Management Policy**	Timely software and firmware updates
4.1.6	**Physical and Environmental Security Policy**	Server room access, physical safeguards
4.1.7	**Wireless Network Security Policy**	Wireless segmentation, encryption, access control
4.1.8	**Vulnerability and Threat Management Policy**	Threat intelligence, scanning, mitigation
4.1.9	**Network Monitoring and Logging Policy**	Logging standards, retention, real-time monitoring
4.1.10	**Incident Response and Management Policy**	Incident reporting, containment, recovery
4.1.11	**Information Security Awareness and Training Policy**	Mandatory staff education and simulations

Table 7 Information Security policy's Supporting Policies

4.1.1.7 Compliance and Enforcement

Compliance with this policy and all supporting information security policies is mandatory for all users and systems. Monitoring is conducted through:

- Routine audits by Internal Audit and the ICT Department / Unit;

- Periodic vulnerability scans and system health checks;
- Security incident tracking and post-incident reviews.

Violations may result in disciplinary action, suspension of system privileges, contract termination (for third parties), or legal escalation in severe cases.

4.1.2 Access Control and User Management Policy

4.1.2.1 Purpose

The purpose of this policy is to ensure that access to ERERA's ICT systems, data, and applications is granted only to authorized users based on clearly defined business needs and roles. By controlling access to systems and information, ERERA can reduce the risk of unauthorized use, data breaches, service disruptions, and compliance violations.

This policy establishes the rules and responsibilities for managing user identities, access permissions, authentication methods, and access reviews throughout the user lifecycle.

4.1.2.2 Scope

This policy applies to:

- All ERERA staff, consultants, interns, contractors, and third-party vendors who require access to ERERA's ICT systems and data;
- All ICT assets, including user accounts, servers, workstations, applications (e.g., ECOLINK, Microsoft 365), databases, mobile devices, and cloud platforms;
- All environments—on-premises, remote, and cloud-based—where ERERA systems are accessed.

It covers both human users and service accounts used for system-to-system communication.

4.1.2.3 Roles and Responsibilities

Role	Responsibilities
IT Officer	Oversees implementation of access controls and approves high-privilege access.
System Administrators	Provision, modify, and revoke access; maintain account and privilege logs.
Departmental Heads	Initiate access requests based on job roles and confirm user responsibilities.
Human Resources	Provide onboarding and offboarding notifications to the ICT Unit.
Internal Audit	Periodically reviews user access controls and logs for compliance.
All Users	Maintain password security and report access anomalies or policy violations.

Table 8 Roles and Responsabilities - Access Control and User Management Policy

4.1.2.4 Policy Statement

ERERA shall maintain a secure and structured access control system to ensure that only authorized users are granted access to information systems, based on their specific roles and job functions. Access shall be:

- **Role-based**: Based on defined roles and least privilege principles;
- **Time-bound**: Access rights will be regularly reviewed and revoked when no longer required;
- **Auditable**: All access events and changes will be logged and periodically reviewed.

The ICT Unit is responsible for maintaining centralized control of user accounts, managing access rights, and conducting periodic access reviews in coordination with department heads and internal auditors.

4.1.2.5 Guiding Principles / Key Directives

4.1.2.5.1 User Access Authorization

- All user access must be formally requested using a standardized access request form and approved by the relevant department head and IT Officer.
- Temporary access must be time-limited and must include a documented expiration date.

4.1.2.5.2 Role-Based Access Control (RBAC)

- Access rights shall be based on predefined roles and job responsibilities.
- Users shall not receive administrative rights unless justified and approved by the IT Officer.

4.1.2.5.3 Authentication Controls

- All users must authenticate using secure login credentials.
- Multi-Factor Authentication (MFA) is required for remote access, system administrators, sensitive applications, and all users accessing Microsoft 365 (M365) services.

4.1.2.5.4 Account Lifecycle Management

- New accounts must be created only upon formal onboarding approval from HR.
- Accounts must be deactivated immediately upon termination, resignation, or role change.
    - Inactive accounts (over 60 days) must be automatically flagged for review and disabled unless approved for extension.

4.1.2.5.5 Access Reviews

- Access rights must be reviewed at least quarterly by the ICT Unit in collaboration with department heads.
- Access logs must be retained for at least 12 months for audit and investigation purposes.

4.1.2.5.6 Shared and Privileged Accounts

- Shared accounts are prohibited unless specifically approved for operational needs.
- Privileged accounts (e.g., admin/root) must be tightly controlled, monitored, and logged.

4.1.2.6 Compliance and Enforcement

4.1.2.6.1 Monitoring

- System and account activities are subject to continuous monitoring through audit logs and alerts.
- Any deviations from approved access configurations will be reported to the IT Officer and, where necessary, escalated to Internal Audit.

4.1.2.6.2 Disciplinary Action

- Unauthorized access, account misuse, or failure to follow access request procedures may result in:
    - Suspension or revocation of system access;
    - Internal disciplinary measures for staff;
    - Contractual penalties or termination for vendors.

4.1.2.6.3 Exception Handling

- Exceptions to this policy must be requested in writing and approved jointly by the IT Officer and Chairman, with documentation retained for audit purposes.

4.1.3 Password Management Policy

4.1.3.1 Purpose

The purpose of this Password Management Policy is to establish minimum standards for the creation, maintenance, and protection of passwords used to access ERERA's ICT systems and data. Passwords are a critical component of ERERA's access control framework and the first line of defense against unauthorized access.

This policy ensures that all users apply secure password practices in alignment with evolving cybersecurity threats, institutional risk levels, and compliance requirements..

4.1.3.2 Scope

This policy applies to:

- All ERERA employees, interns, consultants, vendors, and third parties accessing ERERA systems;
- All accounts used to access ERERA resources, including domain logins, email accounts, administrative systems (e.g., Active Directory, ECOLINK), cloud platforms (e.g., Microsoft 365), databases, mobile apps, and network equipment;
- Both user-level and privileged/system-level accounts.

It covers on-site, remote, and cloud-based access, and applies to internal systems and third-party solutions integrated with ERERA's infrastructure.

4.1.3.3 Roles and Responsibilities

Role	Responsibilities
IT Officer	Oversees implementation, enforcement, and review of password controls and related systems.
System Administrators	Configure password settings, enforce resets, and monitor compliance.
All Users	Create and protect strong passwords; report suspected compromise; comply with renewal cycles.
Internal Audit	Reviews compliance with password policies and tracks policy violations.
HR Department	Notifies ICT of staff onboarding and exits to trigger password creation or deactivation.

4.1.3.4 Policy Statement

Passwords must be managed securely to prevent unauthorized access to ERERA's systems and data. All users must use strong, unique passwords and follow established security practices to protect their credentials. The ICT Unit will enforce system-wide password policies through centralized administration, monitoring, and training.

This policy defines required password complexity, renewal frequency, handling, and response procedures in case of compromise.

4.1.3.5 Guiding Principles / Key Directives

4.1.3.5.1 Password Complexity Requirements

- Passwords must be at least **12 characters** long and include a mix of:
    - Uppercase letters (A–Z)
    - Lowercase letters (a–z)
    - Numbers (0–9)
    - Special characters (e.g., @, #, $, %, &)
- Dictionary words, personal information (e.g., name, ID number), or common patterns (e.g., "123456") are not allowed.

4.1.3.5.2 Password Expiry and Reuse

- User passwords must be changed every **180 days**.
- Privileged/admin passwords must be changed every **90 days**.
- The last **5 passwords** may not be reused.

4.1.3.5.3 Password Protection

- Passwords must **never be shared** or written down in an unsecured format.
- Passwords must **not be stored in plaintext** in any application or document.
- Password autofill/browser storage is discouraged and disabled where possible.

4.1.3.5.4 Account Lockout and Recovery

- After **5 failed login attempts**, accounts will be temporarily locked for 15 minutes.
- Password reset requests must follow a secure, verifiable process administered by the ICT Unit.

4.1.3.5.5 Multi-Factor Authentication (MFA)

- MFA is required for:
    - Remote access to ERERA systems;
    - Administrative and privileged accounts;
    - All access to email and cloud platforms (e.g., Microsoft 365).

4.1.3.5.6 Emergency and Temporary Access

- Temporary passwords must be random, expire after 24 hours, and be reset upon first login.
- System-generated passwords must meet complexity standards and be securely communicated.

4.1.3.6 Compliance and Enforcement

4.1.3.6.1 Monitoring and Logs

- The ICT Unit will enforce password policy settings using directory services and system controls.
- Logs of password changes, resets, and failed login attempts are retained for **12 months**.

4.1.3.6.2 Non-Compliance Consequences

- Failure to comply may result in:
    - Forced password resets;
    - Suspension of access privileges;
    - Disciplinary action for employees or termination of vendor access.

4.1.3.6.3 Exception Handling

- Exceptions (e.g., application limitations) must be approved by the IT Officer and documented with compensating controls.

4.1.4 Antivirus and Endpoint Protection Policy

4.1.4.1 Purpose

The purpose of this policy is to ensure that all endpoint devices connected to ERERA's ICT infrastructure are protected from viruses, malware, spyware, ransomware, and other malicious software. As endpoint devices serve as critical access points to ERERA systems and data, it is vital to secure them to prevent breaches, data loss, service disruptions, and reputational harm.

This policy outlines requirements for the deployment, configuration, and monitoring of antivirus and endpoint protection solutions across the organization.

4.1.4.2 Scope

This policy applies to:

- All ERERA-managed endpoint devices including desktops, laptops, tablets, smartphones, and servers;
- Personal (BYOD) devices granted conditional access to ERERA networks;
- All operating environments (on-site and remote) connected to ERERA's internal systems;
- Staff, contractors, consultants, and third-party providers using ERERA equipment or systems.

This includes systems within data centers, administrative offices, mobile setups, and cloud-connected services.

4.1.4.3 Roles and Responsibilities

Role	Responsibilities
IT Officer	Ensures enterprise-wide deployment and policy enforcement of antivirus tools.
System Administrators	Install and maintain antivirus software, respond to alerts, update virus definitions.
All Users	Avoid suspicious downloads; report malware signs; do not disable protection tools.
Internal Audit	Verifies adherence to antivirus deployment, alert response, and update schedules.
Third-Party Vendors	Ensure endpoint compliance with ERERA standards before device/network integration.

4.1.4.4 Policy Statement

ERERA shall protect all endpoint devices and servers from malware and malicious code by deploying centrally managed antivirus and endpoint protection software. The ICT Unit is responsible for implementing, monitoring, and enforcing this protection as part of the broader information security program.

No device may be connected to ERERA's internal or cloud environments without adequate malware protection and verification.

4.1.4.5 Guiding Principles / Key Directives

4.1.4.5.1 Mandatory Protection

- All endpoints (servers, workstations, laptops, and mobile devices) must run ERERA-approved antivirus and endpoint protection software.
- Devices must be enrolled in a **centralized endpoint management system** (e.g., Microsoft Defender for Endpoint, Sophos Central).

4.1.4.5.2 Automatic Updates and Real-Time Scanning

- Virus definitions and protection engines must update **daily** or as soon as new definitions are released.
- Real-time scanning must remain **enabled** at all times; users may not disable or bypass antivirus services.

4.1.4.5.3 Scheduled and On-Demand Scans

- Full system scans must be performed **weekly** and on-demand if threats are suspected.
- Scans must cover all drives, temporary files, and system areas.

4.1.4.5.4 Alerting and Logging

- Antivirus alerts and logs must be:
    - Monitored centrally by the ICT Unit;
    - Retained for **at least 6 months** for forensic and compliance purposes;
    - Escalated immediately if critical malware is detected.

4.1.4.5.5 Quarantine and Removal

- Infected files must be **quarantined automatically**.
- Manual intervention for malware removal must be logged and reviewed.

- Any endpoint requiring re-imaging or full recovery must be reported to the IT Officer.

4.1.4.5.6 USB and External Device Control

- Removable media must be automatically scanned upon insertion.
- The ICT Unit reserves the right to **disable USB ports** or enforce encryption for high-risk users.

4.1.4.5.7 Unauthorized Software and Exceptions

- Users must not install any third-party antivirus solutions or software that conflicts with ERERA protection policies.
- Exceptions require formal written approval and risk justification.

4.1.4.6 Compliance and Enforcement

4.1.4.6.1 Monitoring and Audits

- Antivirus status, update logs, and threat alerts will be monitored through the endpoint management platform.
- Non-compliant devices will be disconnected from the network until resolved.

4.1.4.6.2 Violations and Sanctions

- Disabling antivirus tools, ignoring threat alerts, or using unauthorized software may result in:
    - Access suspension;
    - Internal disciplinary measures;
    - Revocation of vendor privileges.

4.1.4.6.3 Exception Handling

- Where antivirus agents cannot be installed (e.g., on legacy systems), alternate security controls must be implemented and documented with ICT and Audit approval.

4.1.5 Patch Management Policy

4.1.5.1 Purpose

The purpose of this policy is to ensure that all ERERA systems, applications, and devices are kept up to date with the latest security and functionality patches. Timely and consistent patching mitigates vulnerabilities that could be exploited by cyber threats, enhances system performance, and maintains regulatory compliance.

Patch management is a foundational element of ERERA's overall information security posture and operational resilience.

4.1.5.2 Scope

This policy applies to:

- All operating systems, enterprise applications (e.g., ECOLINK, Microsoft 365), productivity tools, antivirus agents, firmware, and network devices (e.g., routers, firewalls) in use at ERERA;
- Physical and virtual servers, workstations, laptops, and mobile devices managed or used within ERERA's ICT environment;
- Third-party software and platforms integrated into ERERA's network;
- Cloud-based systems, including SaaS platforms, where ERERA retains administrative responsibility.

The policy applies to both production and test environments.

4.1.5.3 Roles and Responsibilities

Role	Responsibilities
IT Officer	Approves the patch management schedule, risk exceptions, and policy revisions.
System Administrators	Deploy, test, and validate patches. Maintain records of applied and pending patches.
Application Owners	Coordinate testing of business application patches before deployment.
End Users	Restart systems when prompted and report post-patch issues promptly.
Internal Audit	Verifies patch management documentation and controls during periodic audits.

4.1.5.4 Policy Statement

All systems within ERERA's infrastructure must be kept current with manufacturer-released patches and updates to address known security vulnerabilities and ensure functional reliability. The patch management process will follow a risk-based approach that prioritizes critical updates for essential systems and services.

Patch deployment shall be conducted in a controlled, documented, and traceable manner, with minimal disruption to business operations.

4.1.5.5 Guiding Principles / Key Directives

4.1.5.5.1 Patch Categorization and Prioritization

- Patches shall be categorized as:
    - **Critical** – addressing exploitable vulnerabilities or regulatory compliance;
    - **High** – affecting core functionality or performance;
    - **Routine** – general bug fixes and feature enhancements.
- **Critical patches** must be applied within **72 hours** of release or notification.

4.1.5.5.2 Patch Identification

- The ICT Unit shall subscribe to vendor security bulletins, ECOWAS alerts, and trusted vulnerability feeds.
- Weekly reviews of pending patches will be conducted using patch management tools (e.g., WSUS, Intune, SCCM, or other EDR systems).

4.1.5.5.3 Testing and Staging

- All patches must be tested in a **controlled staging environment** prior to production deployment, especially for mission-critical systems.
- Any compatibility issues must be documented and resolved with relevant system/application owners.

4.1.5.5.4 Deployment Schedule

- Patches will be deployed based on the following timeline:
    - **Critical**: within 3 days
    - **High**: within 7 days
    - **Routine**: within 30 days

- Patching shall be scheduled during off-peak hours to reduce business impact, with stakeholder notification at least 24 hours in advance.

4.1.5.5.5 Verification and Validation

- Post-patch validation checks shall be performed to confirm successful application and system integrity.
- Failed patches must be rolled back, and the issue escalated for analysis and correction.

4.1.5.5.6 Documentation and Reporting

- Patch logs shall be retained for at least **12 months**.
- A monthly **Patch Compliance Report** will be submitted to the IT Officer and summarized for management review.

4.1.5.5.7 Exceptions

- In cases where patches cannot be applied (e.g., legacy systems), compensating controls (e.g., network isolation, increased monitoring) must be implemented.
- Exceptions must be documented and approved by the IT Officer and reviewed quarterly.

4.1.5.6 Compliance and Enforcement

4.1.5.6.1 Monitoring and Audits

- Patch compliance will be monitored using automated tools and reviewed by Internal Audit.
- Systems failing to meet patch requirements may be disconnected or restricted until compliance is achieved.

4.1.5.6.2 Violations and Sanctions

- Repeated negligence in applying critical patches may lead to:
  - System quarantining;
  - Staff disciplinary actions;
  - Escalation to management for corrective decisions.

4.1.6 Physical and Environmental Security Policy

4.1.6.1 Purpose

The purpose of this policy is to establish and maintain secure physical and environmental controls for all ICT infrastructure and equipment used within ERERA. This includes protecting critical assets such as servers, networking equipment, power supplies, and backup systems from unauthorized physical access, damage, theft, or environmental hazards.

As ERERA expands its ICT capabilities, this updated policy reflects improved best practices in server room control, biometric access, environmental sensors, and facility zoning aligned with ISO/IEC 27001 Annex A.11 and ECOWAS data protection principles.

4.1.6.2 Scope

This policy applies to:

- All physical locations where ERERA's ICT equipment is stored or operated, including:
    - Server rooms, network cabinets, data storage units, communications hubs;
    - Disaster recovery (DR) sites, backup locations, and cloud-connected terminals;
- Physical infrastructure such as:
    - Air conditioning, fire suppression systems, Uninterruptible Power Supplies (UPS), biometric locks, security cameras, and raised flooring;
- All employees, vendors, service providers, and cleaning or maintenance staff who access secured ICT areas.

This policy applies to both permanent and temporary installations managed directly or through third-party contracts.

4.1.6.3 Roles and Responsibilities

Role	Responsibilities
IT Officer	Defines access levels, approves access requests, oversees environmental controls.
Facilities Management	Maintains physical security infrastructure (locks, CCTV, fire suppression, access logs).
System Administrators	Ensure physical servers, cables, and network racks are housed and labeled securely.

Internal Audit	Verifies enforcement of access restrictions and integrity of physical protections.
All Staff / Vendors	Must comply with facility access procedures and report abnormalities or unauthorized access.

4.1.6.4 Policy Statement

ERERA shall ensure that physical access to ICT systems and related infrastructure is restricted to authorized personnel, monitored continuously, and protected against environmental risks. Server rooms and communication infrastructure shall meet secure facility standards, including power, climate, and fire control safeguards.

This policy defines how physical and environmental controls shall be maintained, monitored, and enforced to protect operational integrity.

4.1.6.5 Guiding Principles / Key Directives

4.1.6.5.1 Access Restrictions

- Access to server rooms, network closets, and IT-controlled zones must be restricted to authorized personnel only.
- Entry must be controlled by physical locks, **biometric readers**, or **electronic access badges**.
- A visitor logbook or **electronic access log system** must be maintained and reviewed monthly.

4.1.6.5.2 Surveillance and Monitoring

- **CCTV cameras** must be installed at all data rooms and entry points, monitored 24/7 by security personnel or automated platforms.
- Video footage must be stored securely for **at least 30 days** for review and incident response.

4.1.6.5.3 Environmental Controls

- Server rooms must be equipped with:
    - **Air conditioning** or HVAC systems to maintain optimal temperature and humidity levels;
    - **Temperature and humidity sensors** with alert capabilities;
    - **Fire detection and suppression systems** (e.g., gas or dry chemical-based, not water-based);
    - Adequate **dust and moisture protection** for all racks and exposed devices.

4.1.6.5.4 Power Supply and Redundancy

- All critical systems must be protected by:
    - **Uninterruptible Power Supplies (UPS)** for short-term power continuity;
    - **Backup generators** where available for long-term supply during outages;
    - Clearly labeled power circuits with surge protection.

4.1.6.5.5 Physical Asset Protection

- All servers, switches, and routers must be mounted in **locked cabinets or racks**.
- Cabling must be organized, secured, and tagged to reduce tampering and accidental disconnections.
- ICT assets must be included in ERERA's physical asset inventory and inspected quarterly.

4.1.6.5.6 Facility Zoning

- ERERA offices shall be divided into **controlled zones**, with sensitive ICT areas marked as "Restricted Access."
- Only staff with "ICT Access Clearance" may enter designated zones without escort.

4.1.6.5.7 Emergency Access and Incidents

- Emergency access may be granted only under supervision and must be logged.
- In case of physical breaches, the IT Officer and Head of Security must be notified immediately.
- Post-incident reviews must be conducted for any access violation or environmental event (e.g., overheating, water ingress).

4.1.6.6 Compliance and Enforcement

4.1.6.6.1 Monitoring

- ICT and Facilities teams shall conduct **monthly access reviews** and **quarterly inspections** of all secure areas.
- Environmental control systems must be tested semi-annually and documented.

4.1.6.6.2 Violations

- Unauthorized access attempts, disabling of surveillance, or bypassing physical security systems will result in:
    - Revocation of access rights;

- Disciplinary action;
- Contract termination for vendors or service providers.

4.1.6.6.3 Exception Handling

- Requests for temporary or emergency access must be logged and approved by both ICT and Facilities.

4.1.6.7 Supporting Procedures

Procedure Title	Description
Server Room Access Request Procedure	Formal process to request and approve ICT area access with clearance level.
Server Room Entry Log and Monitoring SOP	Describes how entries and exits are tracked and reviewed.
CCTV and Surveillance Footage Handling SOP	Covers retention, review, and privacy rules for video footage.
Environmental Monitoring and Alert SOP	Outlines how temperature, humidity, and fire systems are configured and monitored.
Physical Security Incident Response Procedure	Steps for reporting and investigating physical or environmental breaches.
Power Backup and UPS Testing Procedure	Periodic testing and load assessment of power continuity systems.

4.1.7 Wireless Network Security Policy

4.1.7.1 Purpose

The purpose of this policy is to ensure the secure configuration, use, and management of wireless network infrastructure at ERERA. Wireless technologies, while offering flexibility and mobility, also introduce significant security risks such as unauthorized access, eavesdropping, and service disruption.

This policy establishes technical and procedural controls to protect ERERA's wireless networks from internal and external threats, ensure segmentation of access, and maintain confidentiality and data integrity over Wi-Fi transmissions.

4.1.7.2 Scope

This policy applies to:

- All wireless networking devices (e.g., wireless access points, routers, wireless controllers) deployed within ERERA offices or facilities;
- All users connecting to ERERA's wireless networks, including employees, guests, consultants, and third-party vendors;
- All wireless networks operating in ERERA, including production, development, and guest networks;
- Wireless access to both internal enterprise systems and external internet services.

This policy includes ERERA-controlled wireless networks in headquarters, remote offices, meeting rooms, and outdoor coverage areas.

4.1.7.3 Roles and Responsibilities

Role	Responsibilities
IT Officer	Oversees design, approval, and monitoring of wireless network architecture.
Network Administrators	Configure, secure, monitor, and maintain all wireless devices and access controls.
System Users	Connect only to authorized wireless networks and comply with access terms.
Facilities / Security	Ensure physical access to wireless infrastructure is controlled.
Internal Audit	Reviews access logs, security settings, and segmentation compliance.

4.1.7.4 Policy Statement

ERERA shall secure its wireless networking environment using encryption, access controls, traffic segmentation, and continuous monitoring. Only authorized wireless devices and users may access designated networks, and different categories of users (e.g., staff vs. guests) must be logically separated using secure configurations.

All wireless deployments must align with organizational security objectives, protect against unauthorized intrusion, and support ICT governance standards.

4.1.7.5 Guiding Principles / Key Directives

4.1.7.5.1 Network Segmentation

- ERERA shall operate **at least two logically separated wireless networks**:
    - **Enterprise Wi-Fi (e.g., ERERA-Secure)**: For ERERA staff, encrypted and integrated with user credentials;
    - **Guest Wi-Fi (e.g., ERERA-Guest)**: Isolated from the internal network, with time-bound internet-only access.

4.1.7.5.2 Wireless Encryption Standards

- All wireless networks must use **WPA2-Enterprise or WPA3** encryption.
- Shared passwords (WPA2-PSK) are prohibited on production or enterprise systems.

4.1.7.5.3 Authentication and Access Control

- Enterprise users must authenticate using their **Active Directory credentials** or other enterprise SSO integration.
- Guest access credentials must be:
    - Provisioned temporarily via a request-based process;
    - Validated with expiration periods (e.g., 24 hours or per event).

4.1.7.5.4 Device Registration

- Only ERERA-approved devices may connect to internal Wi-Fi networks.
- All connected devices must be:
    - Registered in the asset inventory;
    - Monitored for compliance (e.g., antivirus, OS version).

4.1.7.5.5 Monitoring and Intrusion Detection

- Wireless activity must be monitored using Wireless Intrusion Detection Systems (WIDS) or access point logs.
- Alerts for rogue access points, unauthorized connections, or anomalies must be reviewed by the ICT Unit.

4.1.7.5.6 Physical and Logical Security

- Wireless access points (WAPs) must be physically secured (mounted, locked).
- SSIDs must not broadcast sensitive network identifiers and should use neutral naming (e.g., "ERERA-WiFi" not "ERERA-Internal").

4.1.7.5.7 Configuration and Firmware Management

- Default administrator credentials on all WAPs must be changed and managed centrally.
- Firmware must be regularly updated to address vulnerabilities and performance issues.

4.1.7.6 Compliance and Enforcement

4.1.7.6.1 Monitoring

- Logs of wireless sessions, MAC addresses, SSID usage, and access events must be retained for **6 months**.
- The ICT Unit will review usage monthly and audit guest access registration records.

4.1.7.6.2 Violations

- Use of unauthorized access points or bypassing enterprise authentication mechanisms may result in:
    - Network isolation of the device;
    - Disciplinary action for staff;
    - Revocation of vendor or guest access privileges.

4.1.7.6.3 Exception Handling

- Exceptions (e.g., use of legacy devices without WPA2 support) must be requested in writing with compensating controls, and reviewed by the IT Officer.

4.1.8 Vulnerability and Threat Management Policy

4.1.8.1 Purpose

The purpose of this policy is to establish a proactive and systematic approach to identifying, assessing, and mitigating security vulnerabilities and threats that may affect ERERA's information systems, networks, applications, and digital assets.

This policy ensures that ERERA maintains situational awareness of evolving risks and implements timely mitigation measures to prevent exploitation, data compromise, or operational disruption.

4.1.8.2 Scope

This policy applies to:

- All ERERA-managed ICT assets including servers, endpoints, network infrastructure, firewalls, web applications, mobile devices, and cloud services;
- Internal and external threats including zero-day vulnerabilities, ransomware, phishing, insider threats, and misconfigurations;
- All staff, third-party service providers, and contractors responsible for system administration, monitoring, and ICT risk oversight.

The policy includes systems hosted on-premises and in third-party or hybrid cloud environments.

4.1.8.3 Roles and Responsibilities

Role	Responsibilities
IT Officer	Oversees vulnerability and threat management programs and ensures risk reporting to leadership.
System/Network Administrators	Conduct vulnerability scans, threat monitoring, and mitigation activities.
Cybersecurity Focal Point (if assigned)	Liaises with national and ECOWAS cybersecurity agencies for intelligence sharing.
Internal Audit	Reviews vulnerability and threat records, verifies remediation and reporting practices.
All Users	Report suspicious activity or unusual system behavior; participate in awareness programs.

4.1.8.4 Policy Statement

ERERA shall implement continuous vulnerability and threat management processes to detect, assess, and remediate security weaknesses and potential cyber threats in a timely and structured manner. The ICT Unit shall lead efforts to integrate automated scanning tools, threat intelligence feeds, and risk-based prioritization into a cohesive framework.

All vulnerabilities must be addressed based on severity, asset criticality, and business impact, and all threat activity must be logged, reviewed, and responded to under ERERA's security response protocols.

4.1.8.5 Guiding Principles / Key Directives

4.1.8.5.1 Vulnerability Identification

- All critical systems must be scanned using approved **vulnerability assessment tools** at least **monthly**, and after significant changes.
- **Authenticated internal scans** are required for server infrastructure and enterprise applications.
- External vulnerability scans (e.g., on public-facing systems) must be conducted **quarterly**.
- **5.2 Risk-Based Prioritization**
- Vulnerabilities will be classified according to:
    - **CVSS (Common Vulnerability Scoring System)** scores;
    - **System sensitivity** (e.g., HR, financial, regulatory systems);
    - **Exploit availability** and threat intelligence.
- **Critical vulnerabilities** must be remediated within **72 hours**, and high risks within **7 days**.

4.1.8.5.2 Threat Intelligence Integration

- ERERA shall subscribe to:
    - Vendor security advisories (e.g., Microsoft, Cisco, Oracle);
    - Regional and global threat intelligence sources (e.g., ECOWAS Cybersecurity Unit, CERTs);
    - National security alert systems and global feeds (e.g., CVE, NIST, MITRE ATT&CK).
- Threat alerts must be evaluated daily, and relevant IOCs (Indicators of Compromise) documented and acted upon.

4.1.8.5.3 Remediation and Mitigation

- Identified vulnerabilities must be addressed through:

- Patching (see Policy 4.1.5);
- Configuration changes;
- Access restrictions;
- Compensating controls (e.g., segmentation, firewall rules).

- All remediation actions must be logged and validated.

4.1.8.5.4 Monitoring and Detection

- ERERA shall implement centralized **log correlation and threat detection tools**, such as:
  - Endpoint Detection and Response (EDR);
  - SIEM (Security Information and Event Management) solutions;
  - Firewall and access control logs;
  - DNS and traffic pattern anomaly detection.

4.1.8.5.5 Reporting and Documentation

- A **Vulnerability and Threat Management Register** must be maintained.
- Monthly summaries of unresolved vulnerabilities and active threats shall be presented to the IT Officer and reviewed by Internal Audit quarterly.

4.1.8.6 Compliance and Enforcement

4.1.8.6.1 Monitoring

- The ICT Unit must maintain logs of scans, remediation efforts, and incident responses.
- Any delay in responding to critical vulnerabilities must be documented and escalated.

4.1.8.6.2 Enforcement

- Failure to remediate critical vulnerabilities or respond to credible threats may result in:
  - Temporary disconnection of systems from the network;
  - Management escalation;
  - Disciplinary or contractual penalties for negligence or non-compliance.

4.1.8.6.3 Exception Handling

- If remediation is not feasible within the prescribed timeframe (e.g., due to operational dependencies), an Exception Request must be submitted with:

- Risk justification;
- Compensating controls;
- Approved remediation timeline.

4.1.9 Network Monitoring and Logging Policy

4.1.9.1 Purpose

The purpose of this policy is to define ERERA's approach to monitoring its ICT networks and systems and maintaining secure, accurate, and auditable logs. Effective monitoring and logging are essential for detecting threats, investigating incidents, ensuring regulatory compliance, and supporting operational continuity.

This policy ensures that all network and system activities are recorded, stored, and reviewed to provide transparency, accountability, and real-time insight into ERERA's digital environment.

4.1.9.2 Scope

This policy applies to:

- All network infrastructure and ICT systems, including servers, endpoints, routers, switches, firewalls, applications, and cloud services;
- Logs related to access control, system events, configuration changes, error reporting, and security alerts;
- All staff, administrators, contractors, and vendors involved in system administration or monitoring;
- Internal and external (internet-facing) environments where ERERA systems are hosted or accessed.

It covers real-time monitoring, log retention, access to logs, and audit trail requirements.

4.1.9.3 Roles and Responsibilities

Role	Responsibilities
IT Officer	Oversees the network and system monitoring strategy and ensures enforcement of logging policies.
System & Network Administrators	Configure logging tools, monitor events, and escalate alerts to the IT Officer.
Internal Audit	Reviews log records, log access practices, and retention compliance.
All Staff and Users	Must not tamper with monitoring systems or delete log records.
Security Vendors (if applicable)	Provide managed detection or alerting services based on ERERA configurations.

4.1.9.4 Policy Statement

ERERA shall monitor all critical ICT infrastructure and collect logs on user activity, network behavior, system operations, and security events to enable threat detection, forensic analysis, policy compliance, and performance evaluation.

Log generation, retention, access, and analysis will be implemented consistently across the organization and aligned with security and audit requirements.

4.1.9.5 Guiding Principles / Key Directives

4.1.9.5.1 Network and System Monitoring

- All network segments and ICT systems must be continuously monitored using approved tools.
- Real-time alerts must be configured for:
    - Unauthorized access attempts;
    - Malware detections;
    - System or service failures;
    - Traffic anomalies (e.g., spikes, external beacons).

4.1.9.5.2 Log Generation and Collection

- The following types of logs must be enabled:
    - Authentication and login logs;
    - Administrator activities;
    - Firewall and intrusion prevention events;
    - Network traffic flow summaries;
    - Application logs (e.g., email, financial, regulatory systems).
- Logs must be collected to a centralized **log management system** or **Security Information and Event Management (SIEM)** platform.

4.1.9.5.3 Log Integrity and Security

- Logs must be **read-only** and protected from tampering or unauthorized deletion.
- Administrator access to log configuration must be tightly restricted and logged.
- Logs must include **timestamps**, source IPs, user identifiers, and action/event details.

4.1.9.5.4 Log Review and Analysis

- Security logs must be reviewed:
    - **Daily** for critical systems;
    - **Weekly** for general operational systems.
- Alerts must be triaged within **24 hours** and documented in the incident register if actionable.

4.1.9.5.5 Retention and Archiving

- Logs must be retained for:
    - **12 months** for security and audit logs;
    - **6 months** for operational and application logs.
- Archived logs must be encrypted and backed up regularly in accordance with the Data Backup and Retention Policy.
- **5.6 Reporting and Escalation**
- Suspicious patterns must be escalated to the IT Officer for further investigation.
- Significant findings may require coordination with incident response (Policy 4.1.10).

4.1.9.6 Compliance and Enforcement

4.1.9.6.1 Oversight

- Internal Audit will conduct reviews of log completeness, access rights, and retention practices on an annual basis.
- Any gap in log availability or improper access will be documented with a corrective action plan.

4.1.9.6.2 Non-Compliance

- Disabling logging features, tampering with logs, or failing to respond to alerts may result in:
    - Disciplinary action for internal staff;
    - Contractual penalties for vendors or service providers.

4.1.9.6.3 Exception Handling

- Exceptions (e.g., for systems without built-in logging) must be formally documented with alternative controls and approved by the IT Officer.

4.1.10 Incident Response and Management Policy

4.1.10.1 Purpose

The purpose of this policy is to establish a structured, timely, and effective approach for responding to information security incidents at ERERA. The policy ensures incidents are identified quickly, contained efficiently, resolved appropriately, and documented thoroughly to prevent recurrence and support institutional resilience.

By defining procedures, responsibilities, and escalation paths, this policy minimizes the impact of cyberattacks, data breaches, malware infections, system disruptions, and unauthorized access on ERERA's operations and reputation.

4.1.10.2 Scope

This policy applies to:

- All information security incidents involving ERERA's ICT systems, networks, applications, users, or data;
- All employees, consultants, interns, contractors, and third parties with access to ERERA's digital assets;
- All types of incidents, including but not limited to:
    - Malware or ransomware outbreaks;
    - Unauthorized system access or data breaches;
    - Phishing and social engineering attacks;
    - Insider misuse of systems or data;
    - Denial of Service (DoS) or network intrusions;
    - Loss or theft of devices containing ERERA data.

It applies to on-premises, remote, and cloud environments.

4.1.10.3 Roles and Responsibilities

Role	Responsibilities
IT Officer (Incident Lead)	Coordinates all incident response activities and serves as escalation point.
Incident Response Team (IRT)	Cross-functional team (ICT, Legal, HR, etc.) responsible for containment and resolution.

System Administrators	Implement technical containment, log analysis, and remediation steps.
End Users	Report suspected incidents promptly and cooperate with response efforts.
Internal Audit	Conducts post-incident reviews and compliance assessments.
Legal Unit / Chairman	Engage in cases involving external communication, data protection, or breaches of confidentiality.

4.1.10.4 Policy Statement

ERERA shall maintain a proactive and coordinated incident response capability to protect its ICT environment and data assets. All users must promptly report suspected or actual security incidents, which will be investigated and resolved following a standardized incident lifecycle.

Incidents shall be classified based on severity, escalated when necessary, and documented in an incident register. Lessons learned will inform continuous improvement in policies, systems, and awareness programs.

4.1.10.5 Guiding Principles / Key Directives

4.1.10.5.1 Incident Detection and Reporting

- All users must report unusual system behavior, suspicious emails, or data access anomalies immediately via:
    - The **Incident Reporting Form**;
    - Email or hotline to the ICT Unit;
    - Automated alerts from antivirus, SIEM, or EDR systems.

4.1.10.5.2 Incident Classification

Incidents will be categorized by severity:

Level	Description	Response Time
High	Major breach, system compromise, data exfiltration	Immediate (within 1 hr)
Medium	Localized infection, attempted access, phishing	Within 4 hours
Low	Minor misuse, unsuccessful scanning, spam	Within 1 working day

4.1.10.5.3 Incident Response Lifecycle

ERERA shall follow these standardized stages for managing incidents:

1. **Identification** – Detect or report abnormal activity or breach;
2. **Containment** – Isolate affected systems to prevent further damage;
3. **Eradication** – Remove root cause (e.g., malware, compromised accounts);
4. **Recovery** – Restore systems and validate integrity before reintegration;
5. **Communication** – Notify stakeholders internally or externally if required;
6. **Post-Incident Review** – Document findings, lessons, and improvement actions.

4.1.10.5.4 Communication and Escalation

- Critical incidents must be escalated to the Chairman and Principal Legal Regulatory Officer.
- If a **personal data breach** occurs, ECOWAS or relevant data protection authorities must be notified within **72 hours**, in line with regional data protection laws.
- External communication (e.g., with regulators, media, affected third parties) must be approved and coordinated by executive management.

4.1.10.5.5 Documentation and Reporting

- All incidents must be logged in the **ERERA Security Incident Register**.
- For each incident, the IRT must record:
    - Incident description and scope;
    - Timeline of actions taken;
    - Individuals involved;
    - Evidence collected (e.g., logs, screenshots);
    - Lessons learned and preventive recommendations.

4.1.10.6 Compliance and Enforcement

4.1.10.6.1 Oversight

- Internal Audit will review incident records and response activities quarterly.
- Missed response times or failures to follow the response lifecycle must be documented and investigated.

4.1.10.6.2 Violations

- Failure to report incidents, unauthorized handling, or tampering with evidence may result in:
    - Disciplinary action for staff;
    - Termination of vendor contracts;
    - Regulatory sanctions if non-compliance with breach laws is established.

4.1.10.6.3 Exception Handling

- In exceptional situations where deviations from the standard process occur, the IT Officer must document justification and corrective steps within the incident report.

4.1.11 Information Security Awareness and Training Policy

4.1.11.1 Purpose

The purpose of this policy is to ensure that all ERERA personnel and stakeholders understand their information security responsibilities and are equipped to prevent, detect, and respond to potential cyber threats. By establishing a structured awareness and training program, ERERA aims to foster a culture of security, reduce human-related risks, and maintain compliance with regional and international information security standards.

4.1.11.2 Scope

This policy applies to:

- All ERERA employees (full-time, temporary, interns), contractors, consultants, vendors, and third parties with access to ERERA systems or information;
- All forms of information handled by ERERA, including regulated data, financial records, regulatory submissions, and internal documentation;
- All training and awareness formats, including orientation sessions, online modules, simulations, tabletop exercises, and posters or digital signage.

This policy is applicable at onboarding, during employment, and upon role changes or technology deployments that introduce new risks.

4.1.11.3 Roles and Responsibilities

Role	Responsibilities
IT Officer	Oversees the design, scheduling, and content of the awareness program.
Human Resources (HR)	Ensures all new hires receive security onboarding and tracks annual completion.
Department Heads	Ensure staff complete role-based training and participate in awareness initiatives.
All Users	Participate in assigned training and apply knowledge to daily work practices.
Internal Audit	Verifies training compliance and evaluates awareness effectiveness.

4.1.11.4 Policy Statement

ERERA shall implement and maintain an information security awareness and training program that is continuous, role-based, and responsive to emerging threats and organizational needs. All users must

understand the risks they face and the controls they are expected to apply to protect ERERA's digital assets.

Participation in annual security training is mandatory, and certain staff will receive targeted instruction based on access level, job role, or regulatory exposure.

4.1.11.5 Guiding Principles / Key Directives

4.1.11.5.1 Mandatory Security Training

- **All new users** must complete introductory information security training within **10 working days** of joining ERERA.
- **Annual refresher training** is mandatory for all personnel.
- Completion status shall be tracked and reported quarterly by HR.

4.1.11.5.2 Role-Based Training

- Specialized training must be delivered to:
    - System Administrators (e.g., secure configuration, logging);
    - Procurement and finance personnel (e.g., phishing, fraud awareness);
    - Senior management (e.g., risk ownership, regulatory reporting);
    - Helpdesk and ICT support (e.g., incident reporting protocols).

4.1.11.5.3 Awareness Campaigns

- ERERA shall conduct periodic awareness activities including:
    - **Phishing simulations** (at least once per year);
    - **Security tip emails**, intranet bulletins, posters;
    - **Cybersecurity Month campaigns**;
    - **Mini-quizzes** and scenario-based workshops.

4.1.11.5.4 Training Topics

Training and awareness content shall cover at a minimum:

- Password hygiene and MFA usage;
- Social engineering and phishing recognition;
- Safe internet and email practices;
- Secure file storage and data handling;

- Reporting incidents and suspicious activity;
- Privacy and confidentiality expectations;
- Remote work and mobile device security.

4.1.11.5.5 Evaluation and Improvement

- Anonymous post-training surveys shall be used to gather feedback.
- Test scores, completion rates, and phishing simulation outcomes will guide program enhancements.
- Training materials shall be reviewed annually to ensure alignment with the current threat landscape.

4.1.11.6 Compliance and Enforcement

4.1.11.6.1 Monitoring

- HR and ICT will maintain a **training compliance register**.
- Internal Audit will verify training participation during regular compliance reviews.

4.1.11.6.2 Enforcement

- Failure to complete required training may result in:
    - Temporary suspension of system access;
    - Formal performance warnings;
    - Delays in role-based access approvals (for high-risk systems).

4.1.11.6.3 Exceptions

- Exceptions due to leave, onboarding delays, or technical barriers must be documented and resolved within one month of return or access grant.

4.1.11.6.4 Warning List / Alert Mechanism

- ERERA shall maintain an internal “Security Awareness Warning List” to track individuals who:
    - Miss mandatory training deadlines;
    - Repeatedly underperform in simulations or quizzes;
    - Fail to respond to critical awareness updates.
- Individuals on the Warning List will receive:

- A formal alert from the ICT and HR departments;
- A one-week remedial training assignment;
- System access restrictions for critical applications until the deficiency is corrected.

- The list shall be reviewed monthly by HR and ICT, and repeat non-compliance may escalate to line management or disciplinary panels.

4.1.12 Supporting Procedures

This section serves as a reference to the detailed procedures that underpin the policies outlined in Domain 4.1. These procedures provide the granular, step-by-step instructions necessary to effectively implement the policy directives. They are maintained separately from the policies themselves to allow for agile updates without requiring a full policy review, while ensuring full traceability and alignment.

The following is a consolidated list of supporting procedures referenced across the above policies, designed to provide operational guidance:

Policy Name	Procedure ID	Supporting Procedure	Procedure Objective	Key Outcome/Benefit
4.1.2 Access Control and User Management	ERERA-ICT-PRO-4.1.2-001	User Access Request and Deactivation Procedure	Define the process for granting, modifying, and revoking access rights.	Ensures only authorized users access ICT systems; reduces insider threats.
4.1.4 Antivirus and Endpoint Protection	ERERA-ICT-PRO-4.1.4-001	Antivirus Deployment and Update SOP	Deploy and maintain antivirus software on all endpoints.	Continuous protection against known malware.
4.1.6 Physical and Environmental Security	ERERA-ICT-PRO-4.1.6-001	Server Room Access Request Procedure	Define how access to server rooms is requested and granted.	Enforces physical access controls to critical ICT zones.
4.1.7 Wireless Network Security	ERERA-ICT-PRO-4.1.7-001	Wireless Network Configuration SOP	Secure wireless networks with encryption and SSID controls.	Protects Wi-Fi against unauthorized access and sniffing.
4.1.10 Incident Response & Management	ERERA-ICT-PRO-4.1.10-001	Incident Reporting and Escalation Procedure	Guide users and IT staff in recognizing and reporting incidents.	Enables rapid containment and limits damage.
4.1.11 Information Security Awareness	ERERA-ICT-PRO-4.1.11-001	Security Training and Awareness Planning SOP	Design and schedule regular awareness programs and campaigns.	Improves staff vigilance and reduces human-related risks.

4.2 IT Operations, Infrastructure, and Applications

This section defines ERERA's strategic and operational approach to managing its ICT operations, infrastructure assets, platforms, and business-critical applications. Effective IT operations form the backbone of service delivery, regulatory execution, and internal efficiency at ERERA. As ICT usage increases and service expectations evolve, structured operational policies are required to guide asset control, service management, system changes, configuration, and application performance.

The policies within this domain aim to ensure high service availability, secure and optimized infrastructure, and alignment of ICT services with ERERA's strategic goals. They are structured to reflect best practices from **ITIL 4**, **ISO/IEC 20000-1 (IT Service Management)**, **COBIT 2019**, and ECOWAS ICT governance frameworks.

Each policy in this domain is designed to:

- Support seamless ICT service operations and delivery;
- Minimize disruptions through proactive problem, change, and configuration control;
- Ensure infrastructure performance, continuity, and compliance;
- Provide governance for enterprise platforms such as **ECOLINK (SAP)** and **Microsoft 365**;
- Establish clear roles, monitoring, and improvement plans for each technical function.

4.2.1 IT Asset Management Policy

4.2.1.1 Purpose

The purpose of this policy is to establish the principles and controls governing the lifecycle management of all ICT assets owned, leased, or used by ERERA. Proper IT asset management ensures accountability, enables strategic planning, supports inventory control, reduces risks related to asset misuse or loss, and facilitates cost-effective maintenance and disposal.

This policy aligns with best practices from **ISO/IEC 19770 (IT Asset Management)** and ECOWAS directives on institutional resource governance.

4.2.1.2 Scope

This policy applies to:

- All hardware and software assets procured, leased, or donated to ERERA;
- End-user devices (e.g., laptops, desktops, tablets, mobile phones), servers, printers, network equipment, storage media, licensed software, and cloud subscriptions;
- Personnel responsible for asset lifecycle stages: acquisition, tagging, use, transfer, maintenance, disposal, and retirement;

- All locations (headquarters, remote sites) where ERERA assets are used or stored.

4.2.1.3 Roles and Responsibilities

Role	Responsibilities
IT Officer	Overall responsibility for IT asset lifecycle governance and policy enforcement.
Asset Focal Point / IT Support Officer	Maintains the central asset register and coordinates tagging, tracking, and audits.
Finance Department	Coordinates with ICT for capital asset registration and depreciation.
Procurement Unit	Ensures asset acquisitions are compliant with procurement and ICT standards.
All Staff / Users	Accept and adhere to terms of use; protect issued assets from loss or misuse.

4.2.1.4 Policy Statement

ERERA shall manage all ICT assets in a controlled and transparent manner from acquisition to disposal. All assets must be identified, recorded, tagged, and tracked in a centralized register. Users must be formally assigned assets and accept responsibility for their care and usage.

Unauthorized movement, modification, or disposal of ICT assets is prohibited. Disposal shall follow security, environmental, and accountability guidelines.

4.2.1.5 Guiding Principles / Key Directives

4.2.1.5.1 Asset Identification and Inventory

- All ICT assets must be registered in the **ERERA ICT Asset Register**, including:
    - Asset tag number and serial number;
    - Type, model, and specifications;
    - Purchase date, location, and assigned user;
    - Warranty, replacement date, and depreciation value;
- The register must be updated regularly, and reconciled annually during asset verification exercises.

4.2.1.5.2 Acquisition and Assignment

- All asset acquisitions must follow ERERA procurement processes and be reviewed for technical compatibility.
- Upon delivery, assets are tagged by the Administration Unit. The ICT Unit records IT assets in its own inventory register and issues them with a Terms of Use Form signed by the recipient.
- Assignment details are recorded and linked to user profiles.

4.2.1.5.3 Movement and Transfer of Assets

- Any relocation (internal or external) must be approved using an **Asset Movement Authorization Form**.
- Temporary removals (e.g., home use, external servicing) require written authorization by the IT Officer and documented return deadlines. **This requirement does not apply to portable ICT equipment such as laptops or tablets officially assigned to users, unless the device is being taken out of the country or transferred to another individual.**.

4.2.1.5.4 Maintenance and Servicing

- Preventive maintenance schedules shall be defined for critical equipment.
- Equipment sent for repair must be logged out; returned items are inspected and logged back in.
- Maintenance logs shall include service provider details and actions taken.

4.2.1.5.5 Asset Disposal and Retirement

- Assets may be retired if they are obsolete, damaged, beyond economic repair, or no longer needed.
- Before disposal:
    - **Data must be securely wiped or destroyed**;
    - Approval must be obtained from ICT, Procurement, and Finance;
    - Disposal method may include internal redeployment, donation, resale, salvage, or recycling;
    - ECOWAS disposal procedures must be followed

4.2.1.5.6 Security and Accountability

- Users must:
    - Not install unauthorized software or reassign assets;

- Ensure physical protection of devices (e.g., avoid theft/loss during travel);
- Report lost/stolen assets immediately using the **General Incident and Loss Form**.

- Unauthorized removal of ICT equipment may result in disciplinary actions

4.2.1.6 Compliance and Enforcement

4.2.1.6.1 Monitoring

- ICT conducts bi-annual spot checks and full inventory audits annually.
- Any discrepancies or unauthorized movement will be investigated.

4.2.1.6.2 Enforcement

- Misuse, tampering, or unauthorized transfer of assets may result in:
  - Access revocation;
  - Disciplinary measures;
  - Reimbursement for loss/damage.

4.2.1.6.3 Exceptions

- Requests for exceptions must be submitted in writing, justified, and approved by the IT Officer with endorsement from Executive Management.

4.2.2 IT Service Management Policy (including SLAs)

4.2.2.1 Purpose

The purpose of this policy is to ensure that IT services provided by the ERERA ICT Department are reliable, consistent, measurable, and aligned with the business objectives of the organization. It establishes principles for delivering and supporting IT services through structured service management processes, including the use of **Service Level Agreements (SLAs)** to define performance expectations and accountability.

This policy aims to promote efficient service delivery, optimize resource use, and enhance user satisfaction through a structured IT service lifecycle.

4.2.2.2 Scope

This policy applies to:

- All ICT services provided by the ERERA ICT Department to internal stakeholders;
- All service types including user support, application management (e.g., Microsoft 365, ECOLINK), email, file sharing, printing, internet connectivity, server hosting, and network access;
- All ICT support processes including incident management, service request fulfillment, and escalation;
- All ERERA staff, departments, and units that consume or depend on ICT services;
- All outsourced services and third-party support providers.

It applies across headquarters and any remote or field-based operations where ERERA has ICT dependencies.

4.2.2.3 Roles and Responsibilities

Role	Responsibilities
IT Officer	Owns service management processes, monitors SLA compliance, and leads service reporting.
Service Desk / Help Desk	First-line support for all user-reported incidents and service requests.
Service Owners	Manage specific services (e.g., email, ERP) and ensure they meet agreed SLAs.
All Staff / End Users	Use services responsibly, report issues, and respect defined usage and support processes.

Vendors / Contractors	Comply with agreed service terms and availability commitments.

4.2.2.4 Policy Statement

ERERA shall establish and maintain a formal IT Service Management framework to ensure ICT services are delivered effectively, meet quality standards, and support ERERA's regulatory and operational needs. All services must be supported by clearly defined **Service Level Agreements (SLAs)** that outline expected performance, availability, support hours, escalation paths, and user responsibilities.

4.2.2.5 Guiding Principles / Key Directives

4.2.2.5.1 Service Catalog and Classification

- All IT services must be listed in a centralized **Service Catalog**, which categorizes services into:
    - Core services (e.g., email, ERP access);
    - Support services (e.g., printing, password resets);
    - Administrative services (e.g., hardware provisioning, software licensing).
- Each service entry must include:
    - Description, owner, dependencies, request channels, and SLA.

4.2.2.5.2 Incident and Request Management

- All user issues must be logged as:
    - **Incidents** (unexpected interruptions or degradation);
    - **Service Requests** (standard user needs such as account creation).
- The Help Desk will prioritize based on **impact and urgency** and follow SLA timeframes.

4.2.2.5.3 Service Level Agreements (SLAs)

Each service shall have an SLA defining:

- Service availability (e.g., 99.5% uptime);
- Response time and resolution time for incidents (e.g., respond within 1 hour for critical issues);
- Hours of support (e.g., 8:00–17:00, Monday to Friday);
- Escalation procedures;
- User and service provider responsibilities.

4.2.2.5.4 Performance Monitoring and Reporting

- Services must be monitored for uptime, responsiveness, and user satisfaction;
- SLA performance metrics will be reviewed **quarterly**, and exceptions documented;
- Monthly service reports must include key indicators such as:
    - Incident volume and resolution time;
    - SLA compliance rate;
    - Root causes of recurring problems.

4.2.2.5.5 Continuous Improvement

- Annual service reviews will be conducted with stakeholders;
- SLA terms may be adjusted based on service maturity, user demand, or risk changes;
- User feedback (e.g., surveys) will inform service improvements.

4.2.2.6 Compliance and Enforcement

4.2.2.6.1 Monitoring

- The IT Officer shall oversee automated service performance monitoring tools and Help Desk data.
- Repeated service failures must trigger a **Corrective Action Plan (CAP)**.

4.2.2.6.2 Non-Compliance

- Failure to meet SLAs consistently may lead to:
    - Internal performance reviews;
    - Penalties or contract review for third-party providers;
    - Service redesign if performance gaps are structural.

4.2.2.6.3 Exception Handling

- Temporary SLA exceptions may be granted for:
    - Major system upgrades;
    - Force majeure events (e.g., network outages, disasters);
- All exceptions must be documented and justified.

4.2.3 IT Change Management Policy

4.2.3.1 Purpose

The purpose of this policy is to ensure that all changes to ERERA's ICT systems are managed in a controlled and standardized manner to minimize the risk of service disruption, unauthorized modification, data loss, and operational errors. This policy promotes transparency, accountability, and continuous service availability by enforcing structured procedures for planning, testing, approving, implementing, and reviewing all changes.

4.2.3.2 Scope

This policy applies to:

- All changes affecting ICT systems, applications, infrastructure, and services, including:
    - Configuration changes;
    - Software updates and patches;
    - Hardware replacements;
    - New system deployments;
    - Security control modifications;
- All change initiators, reviewers, implementers, and approvers;
- Both internal and third-party (vendor-initiated) change requests;
- Routine, emergency, and project-related changes.

4.2.3.3 Roles and Responsibilities

Role	Responsibilities
Change Requestor	Submits Request for Change (RFC) with supporting justification and documentation.
Change Implementer	Prepares, tests, and executes the change in line with the approved plan.
Change Approver	Reviews the RFC, risk, and impact; escalates to CAB or ECAB as needed.
Change Advisory Board (CAB)	Reviews and approves major changes, provides risk recommendations, and prioritizes RFCs.

Emergency Change Advisory Board (ECAB)	Reviews and authorizes emergency changes during high-impact situations.
IT Officer	Chairs CAB meetings, maintains change logs, ensures compliance, and reports to management.

4.2.3.4 Policy Statement

ERERA shall ensure that all changes to its ICT environment are initiated, assessed, tested, approved, implemented, and reviewed in a structured and auditable manner. No change shall proceed without formal risk assessment and documented authorization in accordance with this policy.

All changes must be:

- Classified by type (Standard, Minor, Major, Emergency);
- Evaluated for technical, business, and security risks;
- Scheduled and communicated to stakeholders;
- Documented from request to post-implementation review.

4.2.3.5 Guiding Principles / Key Directives

4.2.3.5.1 Change Classification

Changes shall be classified as:

Type	Definition
Standard	Low-risk, routine changes following pre-approved procedures (e.g., password reset, software install).
Minor	Low-impact, well-understood changes requiring minimal testing and limited rollback plans.
Major	Complex or high-risk changes requiring full review, CAB approval, formal test and rollback plan.
Emergency	Urgent changes needed to resolve critical incidents or prevent major outages.

4.2.3.5.2 Change Lifecycle Stages

1. **Request Submission** – RFC created with risk, scope, timing, and impact assessment;
2. **Review and Classification** – Performed by Change Approver or routed to CAB/ECAB;
3. **Approval** – Authorization based on type and severity;

4. **Testing and Scheduling** – Conducted in staging or sandbox environments where possible;
5. **Implementation** – Carried out by assigned Implementer;
6. **Post-Implementation Review** – Evaluation of success, impact, and unresolved issues;
7. **Closure** – Final documentation and system log updates.

4.2.3.5.3 Emergency Changes

- Must be reviewed by ECAB before implementation;
- Post-change documentation is required within 1 business day;
- Retroactive testing and stakeholder notification must occur.

4.2.3.5.4 Documentation and Audit Trail

All RFCs must include:

- Risk assessment;
- Impact statement (technical and business);
- Implementation and back-out plan;
- Approvals and sign-offs;
- Post-implementation outcome.

RFCs must be logged and tracked in the official change management register or system.

4.2.3.6 Compliance and Enforcement

4.2.3.6.1 Monitoring and Review

- CAB meets monthly (or as needed) to review open RFCs, discuss trends, and assess control performance.
- Annual audit of the change management log is conducted by Internal Audit.

4.2.3.6.2 Non-Compliance

Unapproved or undocumented changes may result in:

- Incident investigation;
- Disciplinary action;
- Service rollback or system quarantine.

4.2.3.6.3 Exceptions

All exceptions must be:

- Approved by the IT Officer;
- Justified with an explanation and risk mitigation plan;
- Documented and retained for audit.

4.2.4 Configuration and Release Management Policy

4.2.4.1 Purpose

The purpose of this policy is to ensure that all configuration items (CIs) within ERERA's ICT infrastructure are identified, recorded, maintained, and protected through structured configuration and release management practices. The policy also ensures that new or updated services are released into the production environment in a controlled, predictable, and secure manner.

This dual-purpose policy supports the reduction of operational risk and enables service continuity, quality control, and governance over changes to infrastructure and applications.

4.2.4.2 Scope

This policy applies to:

- All physical and virtual configuration items (CIs), including hardware, software, applications, databases, network devices, system settings, and service dependencies;
- All environments: production, development, test, and staging;
- All IT personnel and third-party providers involved in infrastructure or application updates;
- All releases of new systems, feature enhancements, patches, and hotfixes deployed in ERERA's environment.

4.2.4.3 Roles and Responsibilities

Role	Responsibilities
IT Officer	Approves policy implementation, oversees release schedules, and monitors CMDB integrity.
Configuration Manager	Maintains and audits the Configuration Management Database (CMDB).
Release Manager	Coordinates release planning, validation, deployment, and rollback protocols.
System Administrators	Implement CI updates and report any unplanned configuration changes.
Application Owners	Validate application releases and ensure business requirements are met.
Change Advisory Board (CAB)	Reviews configuration changes as part of change management process.

4.2.4.4 Policy Statement

ERERA shall maintain an accurate record of its ICT assets and configurations through a central **Configuration Management Database (CMDB)** and manage the release of changes to systems and applications through a controlled and auditable process.

All releases must be:

- Planned and approved through change management channels;
- Tested and validated in staging environments;
- Accompanied by clear rollback plans and documentation;
- Linked to updated CI records in the CMDB.

4.2.4.5 Guiding Principles / Key Directives

4.2.4.5.1 Configuration Identification and Control

- Each Configuration Item (CI) must have a unique identifier, type, version, and owner recorded in the CMDB.
- The CMDB must document:
    - Hardware details (e.g., asset ID, location, assigned user);
    - Software versions and licenses;
    - Service dependencies and network configurations;
    - Status changes (active, in testing, deprecated).

4.2.4.5.2 Configuration Change Tracking

- Any change to a CI (e.g., IP address, OS version, installed application) must:
    - Be approved via the Change Management process;
    - Be updated in the CMDB within 24 hours of implementation;
    - Be linked to the related RFC and release documentation.

4.2.4.5.3 Release Planning and Coordination

- Releases must follow a structured lifecycle:
    1. **Planning** – Schedule coordinated with affected stakeholders;
    2. **Build and Testing** – Performed in sandbox or pre-production environment;
    3. **Approval** – Authorized by CAB for major releases;

4. **Deployment** – Includes backup creation and rollback plan;
5. **Validation** – Confirmed through post-deployment checks.

4.2.4.5.4 Emergency Releases

- In urgent cases, fast-tracked emergency releases are permitted with ECAB authorization and must be documented retroactively.

4.2.4.5.5 Audits and Reconciliation

- Monthly CMDB updates and quarterly audits must be performed to validate:
  - Accuracy of CI attributes;
  - Unauthorized changes or configuration drift;
  - License compliance for software and applications.

4.2.4.6 Compliance and Enforcement

4.2.4.6.1 Monitoring and Review

- Configuration and release events are logged and periodically reviewed by Internal Audit and ICT.
- Deviations from established release or configuration procedures must be documented and corrected.

4.2.4.6.2 Violations and Sanctions

- Unapproved releases or undocumented configuration changes may lead to:
  - Rollback of deployed changes;
  - Disciplinary measures for staff;
  - Termination of contractor access.

4.2.4.6.3 Exception Handling

- Exceptions to this policy (e.g., expedited patching in response to vulnerability) require:
  - IT Officer's approval;
  - Post-release documentation within 48 hours.

4.2.5 Network Architecture, Segmentation, and Availability Policy

4.2.5.1 Purpose

The purpose of this policy is to ensure that ERERA's ICT network infrastructure is designed, segmented, and managed in a secure, resilient, and scalable manner. This policy establishes technical and governance principles for building and maintaining a robust network that supports business continuity, controls access, mitigates risks, and ensures high availability of services.

4.2.5.2 Scope

This policy applies to:

- All network infrastructure managed or contracted by ERERA, including local area networks (LANs), wide area networks (WANs), wireless networks, and virtual networks (VPNs);
- All network components such as routers, switches, firewalls, access points, gateways, and load balancers;
- All sites where ERERA operates ICT infrastructure (headquarters, disaster recovery locations, remote offices);
- All users, administrators, and third parties with access to ERERA's network.

4.2.5.3 Roles and Responsibilities

Role	Responsibilities
IT Officer	Oversees network design decisions, ensures segmentation strategy, and reviews availability metrics.
Network Administrator	Implements network configuration and monitors availability, access, and performance.
System Administrators	Report network issues and manage dependent systems in accordance with segmentation rules.
Service Providers	Must comply with ERERA's network architecture and availability requirements.

4.2.5.4 Policy Statement

ERERA shall implement a secure, segmented, and high-availability network infrastructure to protect its information systems and ensure continuous access to ICT services. Network segmentation and redundancy shall be used to reduce attack surfaces, isolate critical systems, and ensure operational resilience during system failures or disruptions.

4.2.5.5 Guiding Principles / Key Directives

4.2.5.5.1 Network Architecture

- Network design must follow **layered architecture** with separation of responsibilities between core, distribution, and access layers;
- All traffic should pass through ERERA-approved security controls (e.g., firewall, intrusion detection systems);
- Redundant paths, links, and failover mechanisms must be used in core infrastructure.

4.2.5.5.2 Network Segmentation

- Networks shall be segmented into **security zones**, such as:
    - Internal corporate zone (e.g., ERP, HR);
    - Public access zone (e.g., website, guest Wi-Fi);
    - Management and admin zones;
    - Demilitarized Zone (DMZ) for external-facing services
- VLANs and access control lists (ACLs) shall be used to restrict inter-zone traffic.

4.2.5.5.3 Access Controls

- Device and user authentication must be enforced before network access is granted;
- Physical access to network ports, switches, and cabling must be protected, especially in public or shared areas;
- Unauthorized equipment (e.g., rogue wireless APs) must be scanned and removed promptly

4.2.5.5.4 Availability and Redundancy

- Mission-critical systems must be connected via redundant network links and power sources (e.g., dual ISP, UPS-backed switches);
- High-availability protocols (e.g., HSRP, VRRP, link aggregation) must be enabled where supported;
- Backup internet connectivity must be available for essential services (e.g., SAP, cloud systems).

4.2.5.5.5 Monitoring and Quality of Service (QoS)

- Network performance must be monitored for latency, packet loss, uptime, and throughput;
- Alerts should be configured for high-latency links or link failure;

- QoS configurations shall prioritize voice, video, and critical data traffic.

4.2.5.5.6 Wireless and Remote Access

- Wireless networks must use secure authentication (e.g., WPA2-Enterprise) and be logically segregated from internal LANs;
- VPN must be used for remote access, with encryption and endpoint controls enforced

4.2.5.6 Compliance and Enforcement

4.2.5.6.1 Monitoring and Audits

- The network shall be subject to periodic vulnerability scans and availability testing;
- Configuration baselines must be maintained and compared during quarterly audits;
- Logs of network events (e.g., link failures, unauthorized access attempts) must be reviewed regularly.

4.2.5.6.2 Non-Compliance

- Unauthorized reconfiguration, bypassing of segmentation controls, or poor cabling practices may result in:
    - Revocation of administrator privileges;
    - Disciplinary action or contract termination;
    - Root cause analysis and immediate remediation.

4.2.5.6.3 Exceptions

- Any temporary bypass of network segmentation or redundancy (e.g., during migration or disaster) must:
    - Be documented;
    - Approved by the IT Officer;
    - Reviewed within 7 days post-implementation.

4.2.6 Application Management Policy

4.2.6.1 Purpose

The purpose of this policy is to ensure the effective governance, availability, security, and user support of enterprise applications used at ERERA, including core platforms like **ECOLINK (SAP)** and **Microsoft 365**. It defines responsibilities for application lifecycle management, user access control, license compliance, updates, and continuity.

This policy supports operational efficiency, data integrity, and regulatory alignment across all application environments.

4.2.6.2 Scope

This policy applies to:

- All business-critical applications deployed, licensed, or maintained by ERERA including:
    - **ECOLINK (SAP)** – for procurement, finance, HR, and inventory;
    - **Microsoft 365** – for email, collaboration, document management;
    - **Technical and operational modeling tools** such as Siemens PSS®E, ETAP, or equivalent software used for grid simulation, regulatory planning, and operational analysis.
    - Any other business or regulatory software introduced into the environment;
- All users of ERERA enterprise applications;
- All application owners, administrators, and technical support personnel.

4.2.6.3 Roles and Responsibilities

Role	Responsibilities
IT Officer	Approves application policies, ensures license compliance, monitors critical updates.
Application Owners	Define functional needs, approve user access, and validate system changes.
System Administrators	Implement configurations, updates, and provide technical support.
Users	Use applications responsibly and report issues through official channels.
Finance & Procurement	Manage license renewal, vendor coordination, and application budgeting (e.g., ECOLINK).

Operational Tool Owners / Engineering Leads	Define usage requirements, validate analysis inputs/outputs, ensure software is used in line with licensing and regulatory models. Coordinate technical training and version control.

4.2.6.4 Policy Statement

ERERA shall implement a structured and controlled application management process that ensures business applications are secure, reliable, regularly updated, and aligned with institutional objectives. All software must be legally licensed and installed under the authority of the ICT Department. Application access must be based on user roles and responsibilities.

4.2.6.5 Guiding Principles / Key Directives

4.2.6.5.1 Application Lifecycle Management

- Applications shall be selected, tested, deployed, and retired based on documented business needs and approvals;
- Application changes (e.g., upgrades, new modules) must follow the **Change Management Policy (4.2.3)**;
- All applications must be assessed for compatibility, licensing, and user impact before procurement.

4.2.6.5.2 ECOLINK (SAP)

- All SAP-related access (e.g., procurement, HR modules) must be requested through the **Application Access Form** approved by the relevant department head
- SAP transactions and workflows must follow ECOWAS-approved processes;
- The SAP access matrix shall be reviewed quarterly.

4.2.6.5.3 Microsoft 365

- Users must authenticate using their official ERERA credentials with multi-factor authentication;
- Microsoft Teams, SharePoint, and OneDrive shall be used for collaboration within official scopes;
- Licensing and feature allocation must match user roles (e.g., Admin vs. Standard User).

4.2.6.5.4 Access Management

- Application access is granted based on need-to-know and least privilege principles;
- New user access must be provisioned only upon receiving a properly authorized request;
- Access for departing users must be deactivated within 24 hours of contract termination

4.2.6.5.5 Software Licensing and Audits

- Only software licensed to ERERA shall be installed;
- The ICT Unit must maintain a **software inventory and license register**;
- Unauthorized software installations shall be removed and reported.

4.2.6.5.6 Updates and Maintenance

- Application patches and upgrades must be planned and tested before deployment;
- Scheduled maintenance windows shall be communicated to stakeholders in advance;
- Critical security updates must be applied within 48 hours.

4.2.6.5.7 Monitoring and Backup

- Applications must be monitored for usage, errors, and performance;
- Backup procedures must protect application configurations and data;
- Recovery testing for business-critical applications must be conducted annually.

4.2.6.5.8 Operational Tool Governance

- All operational analysis tools such as Siemens PSS®E must be:
    - Procured with a valid license agreement and supported by vendor documentation;
    - Configured and maintained by qualified personnel in coordination with the ICT Department;
    - Used only for officially approved regulatory, modeling, or operational purposes.
- Output data from these tools must be treated in accordance with ERERA's Data Classification and Handling Policy (4.3.1) if it includes sensitive or restricted grid/market data.
- Updates and custom modules (scripts/macros) must be tested and reviewed prior to use in decision-making or reporting.
- ICT and Operational Teams shall jointly define backup schedules for models, datasets, and simulation results.
- Users must complete technical onboarding and periodic training before accessing these systems.

4.2.6.6 Compliance and Enforcement

4.2.6.6.1 Monitoring

- The ICT Department will audit application access logs and license usage regularly;
- Discrepancies must be resolved through formal review and corrective actions.

4.2.6.6.2 Enforcement

- Violations such as unauthorized installations, license misuse, or access abuse may result in:
    - Disciplinary action;
    - System access suspension;
    - Notification to the Regulatory Council.

4.2.6.6.3 Exception Handling

- Exceptions (e.g., temporary access for consultants) must be authorized in writing and time-bound.

4.2.7 Problem Management Policy

4.2.7.1 Purpose

The purpose of this policy is to establish a structured and proactive approach to identifying, documenting, analyzing, and resolving the root causes of ICT incidents and service interruptions within ERERA. The Problem Management Policy aims to reduce incident recurrence, minimize service downtime, and improve overall ICT reliability and performance.

This policy complements the Incident Management process by focusing on underlying causes rather than immediate incident resolution.

4.2.7.2 Scope

This policy applies to:

- All ICT systems, services, applications, and infrastructure used or managed by ERERA;
- All problems identified as recurring incidents, significant disruptions, system errors, or critical configuration failures;
- All permanent and contracted ICT personnel responsible for support, system management, and service operations;
- All problems triggered by incident trends, major incidents, change failures, and audits.

4.2.7.3 Roles and Responsibilities

Role	Responsibilities
IT Officer	Oversees the Problem Management process and reviews major problems with management.
Problem Coordinator	Leads root cause analysis (RCA), ensures problem documentation, and tracks resolutions.
Service Desk	Identifies recurring incidents and logs them as potential problems.
System Administrators	Investigate problems, perform diagnostics, and implement solutions.
Application Owners	Support root cause discovery and validate permanent fixes related to business systems.

4.2.7.4 Policy Statement

ERERA shall maintain a proactive and reactive problem management process to identify root causes of ICT incidents and implement permanent fixes or workarounds. The goal is to improve service quality, reduce operational costs, and prevent incident recurrence.

No critical issue shall be closed until its root cause has been identified, mitigated, or documented with an acceptable workaround.

4.2.7.5 Guiding Principles / Key Directives

4.2.7.5.1 Problem Identification and Logging

- A **Problem Record** must be created when:
    - An incident recurs more than twice within a defined period;
    - A major incident occurs;
    - There is an unresolved root cause after a high-severity incident;
    - A pattern of similar incidents is detected by the Service Desk.

4.2.7.5.2 Problem Categorization and Prioritization

- Problems must be assigned:
    - **Impact Level** (low, medium, high);
    - **Urgency** (based on disruption, recurrence, stakeholder impact);
- Prioritization determines assignment and expected timeframes for analysis and resolution.

4.2.7.5.3 Root Cause Analysis (RCA)

- For all high-priority problems, RCA must be conducted using a standard methodology (e.g., 5 Whys, Fishbone Diagram);
- The **Problem Coordinator** must lead RCA sessions and ensure findings are recorded;
- RCA must occur within 3–5 business days of a major incident.

4.2.7.5.4 Resolution and Workarounds

- When a full solution is not immediately possible, a documented **workaround** must be implemented and communicated;
- Permanent solutions should be reviewed and approved through the **Change Management Process (4.2.3)**;

- The Problem Record must be updated upon:
    - Root cause confirmation;
    - Change request creation;
    - Resolution implementation.

4.2.7.5.5 Problem Reviews and Reporting

- Problem logs shall be reviewed monthly by the ICT team;
- A **Problem Management Dashboard** shall track:
    - Number of new problems identified;
    - Root causes found;
    - Resolved vs. unresolved problems;
    - Top recurring issues.

4.2.7.6 Compliance and Enforcement

4.2.7.6.1 Monitoring

- Internal Audit will review the Problem Register semi-annually for completeness, timeliness, and traceability;
- Major problems must be discussed in quarterly ICT performance reviews.

4.2.7.6.2 Non-Compliance

- Repeated failure to analyze or document root causes may result in:
    - ICT staff performance reviews;
    - Escalation to executive oversight;
    - Delay in closing related incidents or change requests.

4.2.7.6.3 Exception Handling

- Low-impact, isolated incidents may be closed without formal RCA if justified and approved by the IT Officer.

4.2.8 Active Directory Management Policy

4.2.8.1 Purpose

The purpose of this policy is to ensure that the **Active Directory (AD)** environment is securely managed, consistently maintained, and properly governed to protect ERERA's network resources and support access control enforcement. AD is the core infrastructure for user identity management, system authentication, and role-based access to ICT services.

This policy ensures user lifecycle management, administrative delegation, and security controls over all domain-joined assets and user accounts.

4.2.8.2 Scope

This policy applies to:

- All user, administrator, service, and machine accounts managed in ERERA's Active Directory;
- All domain controllers, group policies, organizational units (OUs), and trust relationships;
- All authorized ICT personnel managing or accessing AD services;
- All systems integrated into ERERA's AD environment, including mail systems, file servers, printers, and applications like Microsoft 365 and ECOLINK.

4.2.8.3 Roles and Responsibilities

Role	Responsibilities
IT Officer	Approves policies, oversees AD health, audits privileged access, and authorizes structural changes.
Domain Administrators	Manage AD objects, enforce policies, maintain account integrity, and respond to incidents.
System Administrators	Apply group policies, implement access restrictions, and execute secure configuration baselines.
HR / Department Heads	Initiate user onboarding, transfers, and exits for access provisioning or revocation.

4.2.8.4 Policy Statement

ERERA shall maintain a secure, efficient, and auditable Active Directory environment as the central source of truth for digital identity and access control. All AD configurations, access privileges, and group policies must be defined based on the principle of least privilege, business need, and security best practices.

4.2.8.5 Guiding Principles / Key Directives

4.2.8.5.1 User Account Lifecycle

- **Account Creation**: Only authorized personnel may request accounts via the **Network/E-mail Account Form** approved by HR and department supervisors
- **Access Rights**: Assigned based on role and department-specific security groups.
- **Password Policies**: Must comply with ERERA's Password Management Policy.
- **Account Change**: Adjusted when user roles or responsibilities change, with written approval.
- **Account Deletion**: Deactivated on the last working day, deleted after grace period (2 weeks for staff, 1 month for management)

4.2.8.5.2 Administrative Access and Segregation of Duties

- **Domain Admin** privileges are granted only to authorized ICT personnel;
- **Delegated Admin** roles are defined for specific OUs (e.g., printer admin, HR app admin);
- Dual control mechanisms must be applied to high-risk accounts and system-level groups.

4.2.8.5.3 Group Policy Management

- GPOs (Group Policy Objects) must be versioned, documented, and linked by function;
- GPOs enforcing security (e.g., login scripts, password length, lockout policies) must be applied uniformly and reviewed quarterly.

4.2.8.5.4 Organizational Units (OUs)

- OUs must be created logically by department, location, or function;
- All systems and accounts must reside in appropriate OUs to support granular policy assignment.

4.2.8.5.5 Logging and Monitoring

- Logon/logoff attempts, account lockouts, and privilege changes must be logged;
- AD audit logs must be retained for at least **12 months** and reviewed monthly.

4.2.8.5.6 Integration and Synchronization

- AD must be the central identity source for email, Microsoft 365, VPN, and internal applications;
- Synchronization with cloud services must use secure protocols (e.g., ADFS, Azure AD Connect);
- External access must enforce MFA and conditional access policies.

4.2.8.6 Compliance and Enforcement

4.2.8.6.1 Monitoring

- ICT Unit must perform monthly AD audits for:
    - Inactive accounts;
    - Expired passwords;
    - Privilege escalations;
    - GPO drift or unauthorized changes.

4.2.8.6.2 Enforcement

- Violations such as unauthorized account creation or access abuse may result in:
    - Immediate access suspension;
    - Disciplinary measures;
    - Review by the Regulatory Council for persistent violations.

4.2.8.6.3 Exception Handling

- Any deviation from policy (e.g., legacy system integration) must be:
    - Documented;
    - Approved by the IT Officer;
    - Reviewed every 6 months.

4.2.9 IT Server Room and Environmental Controls Policy

4.2.9.1 Purpose

The purpose of this policy is to safeguard ERERA's server rooms and critical ICT infrastructure from physical and environmental threats. This policy ensures that all ICT facilities are adequately protected against unauthorized access, environmental hazards (temperature, humidity, fire, power failure), and operational risks that could compromise system availability and data integrity.

4.2.9.2 Scope

This policy applies to:

- All ERERA ICT rooms, server rooms, network closets, and telecom spaces across headquarters and any remote or backup sites;
- All equipment hosted within these environments, including servers, storage, routers, UPS units, and backup systems;
- ICT personnel, vendors, contractors, and any third parties requiring access to restricted ICT infrastructure;
- All supporting environmental systems: air conditioning, fire suppression, CCTV, UPS, surge protectors, smoke detectors, and intrusion detection systems.

4.2.9.3 Roles and Responsibilities

Role	Responsibilities
IT Officer	Oversees server room access control, monitors facility conditions, and ensures policy compliance.
Facilities/Security	Ensures physical barriers, lighting, CCTV, and emergency systems are maintained.
System Administrators	Ensure hosted systems are powered, cooled, and secured appropriately.
Visitors/Contractors	Must be authorized and escorted; must comply with physical and environmental protocols.

4.2.9.4 Policy Statement

ERERA's server rooms and ICT facilities shall be treated as restricted, mission-critical areas requiring controlled access and regulated environmental conditions. All systems hosted within shall be protected against unauthorized access, physical tampering, environmental degradation, and accidental damage.

ICT rooms must remain operational under defined temperature, humidity, and power standards at all times.

4.2.9.5 Guiding Principles / Key Directives

4.2.9.5.1 Physical Access Control

- Server rooms shall be classified as **Restricted Areas** and protected using:
    - Biometric readers, access cards, or combination locks;
    - CCTV coverage, intrusion detection, and alarm systems;
- Only authorized ICT staff may enter unescorted;
- All visitors must be escorted and logged;
- Sharing of access credentials is strictly prohibited

4.2.9.5.2 Access Records and Revocation

- All access must be logged (entry/exit timestamps);
- Access rights must be removed when roles change or staff exit;
- Lost or stolen access cards/devices must be reported immediately.

4.2.9.5.3 Environmental Controls

- Temperature must be maintained between **18°C and 25°C**; humidity between **40% and 60%**
- **Air conditioning** systems with air filtration must operate 24/7 with alerts for malfunction;
- **Smoke detectors** and **fire suppression systems** (non-water-based) must be installed, regularly tested, and operable;
- No food, drink, or flammable items are allowed in ICT rooms.

4.2.9.5.4 Electrical Power and Surge Protection

- All critical systems must be connected to:
    - **Uninterruptible Power Supply (UPS)** systems;
    - **Surge protectors** for voltage spikes;
    - **Backup generators** where applicable;
- Electrical sockets must not be overloaded;
- Water sensors must be installed under raised floors to detect leaks or flooding

4.2.9.5.5 Video Surveillance and Intrusion Detection

- Server rooms must be continuously monitored by **CCTV** with:
    - 30-day video retention;
    - Motion-detection capabilities;
    - Regular maintenance and tamper detection;
- Intrusion Detection Systems (IDS) must be tested regularly to verify responsiveness.

4.2.9.5.6 Safety and Fire Prevention

- Fire extinguishers must be accessible and clearly marked;
- All ICT and security staff must be trained in fire response procedures;
- Emergency lighting and signage must be tested quarterly.

4.2.9.6 Compliance and Enforcement

4.2.9.6.1 Monitoring and Reviews

- Access logs and CCTV footage must be reviewed monthly;
- Temperature, humidity, and power supply logs must be archived for 12 months;
- Internal audit shall verify compliance annually.

4.2.9.6.2 Enforcement

- Unauthorized access, tampering with controls, or breach of safety standards may result in:
    - Access suspension;
    - Disciplinary or legal action;
    - Reporting to the ERERA Regulatory Council if necessary.

4.2.9.6.3 Exception Handling

- Exceptions (e.g., emergency equipment relocation or vendor access) require written authorization and supervised access.

4.2.10 Supporting Procedures

This section serves as a reference to the detailed procedures that underpin the policies outlined in Domain 4.2. These procedures provide the granular, step-by-step instructions necessary to effectively implement the policy directives. They are maintained separately from the policies themselves to allow for agile updates without requiring a full policy review, while ensuring full traceability and alignment.

The following is a consolidated list of supporting procedures referenced across the above policies, designed to provide operational guidance:

Policy	Procedure ID	Supporting Procedure	Objective	Key Outcome/Benefit
4.2.1 IT Asset Management Policy	**ERERA-ICT-PRO-4.2.1-001**	Asset Registration and Tagging Procedure	Ensure consistent tagging and registration of new ICT assets.	Enables traceability and audit readiness.
	ERERA-ICT-PRO-4.2.1-002	Asset Assignment and Return Procedure	Standardize asset handover and return processes.	Ensures user accountability and prevents asset loss.
	ERERA-ICT-PRO-4.2.1-003	Asset Movement and Authorization SOP	Regulate internal and external asset movements.	Maintains visibility and control over asset locations.
	ERERA-ICT-PRO-4.2.1-004	Asset Disposal and Retirement Procedure	Guide secure and policy-compliant asset decommissioning.	Prevents data leakage and aligns with environmental/legal obligations.
	ERERA-ICT-PRO-4.2.1-005	Asset Verification and Audit Procedure	Define periodic inventory check process.	Enhances integrity of asset records and supports financial reporting.

Policy	Procedure ID	Supporting Procedure	Objective	Key Outcome/Benefit
4.2.2 IT Service Management Policy (including SLAs)	**ERERA-ICT-PRO-4.2.2-001**	Incident and Request Handling SOP	Outline steps for triaging and resolving support tickets.	Ensures fast, standardized support response across ERERA.
4.2.3 IT Change Management Policy	**ERERA-ICT-PRO-4.2.3-001**	Change Request Submission and Approval Workflow	Guide users through submission, classification, and approval routing.	Ensures traceable and risk-aware change decision-making.
4.2.4 Configuration and Release Management Policy	**ERERA-ICT-PRO-4.2.4-001**	Configuration Item Identification and Registration SOP	Define how new CIs are identified and logged into the CMDB.	Ensures traceability and accurate system modeling.
4.2.6 Application Management Policy	**ERERA-ICT-PRO-4.2.6-001**	Application Access Request and Approval Procedure	Define how users request and receive application permissions.	Controls and audits user access based on job roles.
4.2.9 IT Server Room and Environmental Controls Policy	**ERERA-ICT-PRO-4.2.9-001**	Server Room Access Request and Logging Procedure	Define steps for applying, granting, and revoking access.	Ensures controlled, documented entry to secure environments.

4.3 Data Governance and Privacy

As a regional regulatory institution responsible for cross-border electricity regulation, ERERA processes and safeguards large volumes of sensitive data—ranging from regulatory submissions and internal operations to partner communications and cloud-based content. This section defines the principles, policies, and controls that govern how ERERA manages, protects, and ensures the quality of its data assets.

Data Governance and Privacy encompasses the full data lifecycle: from classification and ownership to access, storage, sharing, retention, and secure disposal. It also includes policies that ensure compliance with ECOWAS legal frameworks, ISO/IEC 27001, ISO/IEC 27701, data protection laws, and internal accountability standards.

The objectives of the policies in this domain are to:

- Assign clear ownership and stewardship over data assets;
- Safeguard personal and sensitive data in accordance with privacy principles;
- Ensure the confidentiality, integrity, and availability (CIA) of institutional data;
- Comply with applicable legal, regulatory, and contractual obligations;
- Support trustworthy analytics, reporting, and knowledge management;
- Enable consistent, accurate, and secure decision-making.

4.3.1 Data Classification and Handling Policy

4.3.1.1 Purpose

The purpose of this policy is to establish a structured classification scheme for ERERA's information assets and to define appropriate handling procedures for each classification level. This policy ensures that data is protected based on its sensitivity, criticality, and applicable regulatory or contractual obligations.

By classifying data and applying consistent handling measures, ERERA aims to reduce the risk of unauthorized access, data breaches, and regulatory non-compliance.

4.3.1.2 Scope

This policy applies to:

- All forms of data created, accessed, transmitted, processed, or stored by ERERA (e.g., electronic, paper, audio, visual);
- All staff, contractors, consultants, interns, and external parties with authorized access to ERERA information;
- All systems, applications, platforms, and devices (owned or leased) through which ERERA data is stored or transmitted.

4.3.1.3 Roles and Responsibilities

Role	Responsibilities
Data Owners	Assign classification levels, approve access, and monitor handling of data under their domain.
Data Stewards	Ensure labels are applied, protection standards are enforced, and users are trained.
ICT Department	Enforce classification in system design, transmission, and storage protocols.
All Users	Apply labels correctly and follow handling instructions appropriate to classification.

4.3.1.4 Policy Statement

All ERERA information must be classified based on its sensitivity, legal requirements, business value, and potential impact of unauthorized disclosure. The classification must dictate how data is handled, transmitted, stored, accessed, and destroyed.

Classified data must retain its label and be handled in accordance with procedures aligned to its classification level throughout its lifecycle.

4.3.1.5 Guiding Principles / Key Directives

4.3.1.5.1 Data Classification Levels

ERERA adopts a four-tier classification scheme:

Level	Definition	Examples
Public	Approved for unrestricted distribution; no impact from disclosure.	Press releases, published reports.
Internal Use Only	Intended for ERERA internal operations; minimal impact if disclosed.	Meeting schedules, internal memos.
Confidential	Sensitive data restricted to specific users; unauthorized disclosure could cause significant harm.	Financial reports, contracts.
Highly Restricted	Critical or sensitive data; unauthorized disclosure could cause severe legal, reputational, or financial harm.	Personnel records, regulatory data.

If data is not explicitly classified, it defaults to **Internal Use Only**

4.3.1.5.2 Data Handling Standards by Classification

Each classification level has distinct handling requirements:

Handling Category	Public	Internal Use Only	Confidential	Highly Restricted
Labeling	Optional	Optional	Mandatory – digital and physical	Mandatory and prominent
Storage	Open directories	Internal drives, controlled access	Encrypted storage, access controls, and protection against malware, unauthorized access, and cyber threats using endpoint security tools.	Encrypted and isolated storage on hardened systems, with continuous monitoring for intrusion and cyber-attack resilience.
Transmission	Unrestricted	Internal email or LAN	Encrypted email, VPN	Encrypted channels, dual authentication
Destruction	Shred if physical	Shred/delete securely	Shred, DOD-wipe digital	Certified destruction/logging

4.3.1.5.3 Labeling and Collection Rules

- Labels must appear on digital files (metadata or filenames) and printed documents;
- When combining datasets, the resulting collection must carry the label of the most sensitive data it contains;
- Physical media (USBs, CDs) containing mixed classification data must reflect the highest sensitivity label.

4.3.1.5.4 Handling in Shared or Remote Environments

- Sensitive data may not be shared via unsecured cloud services or unauthorized removable media;
- Remote access to classified data must enforce encryption, MFA, and policy-aligned VPN controls;
- Third-party access must be covered by NDAs and formal agreements.
- Users must complete privacy and data handling awareness training, which includes secure remote access, labeling responsibility, and incident reporting protocols.

4.3.1.5.5 Data Classification Awareness and Training

All ERERA users must complete periodic training on:

- Identifying classification levels and applying appropriate labels;

- Secure handling procedures for digital and physical information;
- Recognizing and preventing data mishandling or leakage;
- Good privacy practices and the importance of protecting sensitive data;

Department Heads and Data Stewards must coordinate hands-on sessions for roles dealing with highly sensitive or classified information.

4.3.1.6 Compliance and Enforcement

4.3.1.6.1 Monitoring

- ICT and Internal Audit will monitor compliance through access reviews, file scans, and audit trail analysis;
- Violations, such as mislabeling or improper sharing, must be logged and investigated.

4.3.1.6.2 Sanctions

- Non-compliance may result in:
    - Access revocation;
    - Disciplinary measures;
    - Legal escalation in case of data breaches.

4.3.1.6.3 Exception Handling

- Any exceptions must be:
    - Formally requested in writing;
    - Approved by the Data Owner and IT Officer;
    - Reviewed after 90 days.

4.3.2 Data Ownership and Stewardship Policy

4.3.2.1 Purpose

The purpose of this policy is to define the roles, responsibilities, and expectations for the ownership and stewardship of ERERA's data. This ensures that each data element or dataset has a formally designated authority accountable for its protection, quality, access, and usage. Effective data ownership promotes governance, accountability, regulatory compliance, and informed decision-making.

4.3.2.2 Scope

This policy applies to:

- All structured and unstructured data generated, acquired, processed, stored, or transmitted by ERERA;
- All data systems, repositories, and platforms under ERERA control (e.g., databases, file shares, SharePoint, ECOLINK);
- All personnel with designated data management responsibilities: Data Owners, Data Stewards, and Data Custodians;
- All business units and departments involved in the lifecycle of critical data.

4.3.2.3 Roles and Responsibilities

Role	Responsibilities
Data Owner	A department head or designated official responsible for approving access, defining rules, and ensuring data quality.
Data Steward	Staff responsible for operational oversight of data, enforcing policies, and coordinating updates.
Data Custodian	ICT personnel who provide technical infrastructure and secure access to systems housing the data.
All Users	Handle data per classification and policy; report inaccuracies or violations.

Note: Data Owners must be full-time ERERA staff; ownership cannot be delegated to vendors or external consultants

4.3.2.4 Policy Statement

ERERA shall assign ownership and stewardship responsibilities to ensure that all institutional data is managed in a structured, compliant, and secure manner. Data Owners must define quality thresholds, access rules, classification, and retention policies, while Data Stewards and Custodians shall implement and maintain data integrity, protection, and compliance.

4.3.2.5 Guiding Principles / Key Directives

4.3.2.5.1 Designation of Data Owners

- Every dataset or system must have a clearly designated Data Owner, **formally approved by the Chairman or the Regulatory Council**, with advice from the IT Officer where appropriate.
- Data Owners must maintain up-to-date documentation on:
    - Data classification (see Policy 4.3.1);
    - Data access privileges;
    - Systems of record (i.e., authoritative sources).

4.3.2.5.2 Duties of Data Owners

- Approve access for job roles or exceptions not covered by job profiles;
- Set the data retention period (with input from Legal);
- Define acceptable data quality limits (accuracy, timeliness, completeness);
- Review reports on system usage, breaches, or anomalies affecting their data;
- Validate system enhancement requests that affect the structure or flow of their data;
- Designate a backup owner during absences.

4.3.2.5.3 Duties of Data Stewards

- Monitor compliance with data quality, labeling, access, and update policies;
- Assist with audits, cleansing, and validation of critical datasets;
- Communicate with end users and ensure proper documentation and reporting.

4.3.2.5.4 Duties of Data Custodians

- Maintain the infrastructure (databases, storage, backups) supporting the data;
- Enforce access control systems;
- Support Data Owners in identifying vulnerabilities and operational risks;
- Maintain audit logs and provide usage reports upon request

4.3.2.5.5 Shared and Cross-Functional Data

- For datasets used across departments, the originating unit will serve as the **Primary Data Owner**;
- A **Data Stewardship Council** may be convened to resolve conflicts or define shared standards.

4.3.2.6 Compliance and Enforcement

4.3.2.6.1 Monitoring

- The ICT Unit and Internal Audit shall maintain a register of designated Data Owners and validate updates annually;
- Random checks will be performed to verify proper ownership attribution and accountability.

4.3.2.6.2 Enforcement

- If no owner is designated, the Principal Manager or Department Head shall be assigned by default;
- Persistent neglect of ownership responsibilities may result in:
    - Escalation to the Chairman;
    - Suspension of system change approvals.

4.3.2.6.3 Exception Handling

- Exceptions to ownership or stewardship arrangements must be approved in writing by the Executive Office and reviewed semi-annually.

4.3.3 Data Access Control and Security Policy

4.3.3.1 Purpose

The purpose of this policy is to establish consistent controls for regulating access to ERERA's data assets, ensuring that only authorized individuals have access to appropriate data based on their roles, responsibilities, and business needs. This policy supports confidentiality, integrity, and availability (CIA) of ERERA's data through role-based, risk-informed access control mechanisms.

4.3.3.2 Scope

This policy applies to:

- All data systems and repositories (applications, databases, storage platforms) used by ERERA;
- All personnel, consultants, vendors, and third-party users accessing ERERA information assets;
- All forms of access (on-site, remote, mobile, read/write privileges) to physical and digital data environments;
- All access to sensitive data (classified as Confidential or Highly Restricted in Policy 4.3.1).

4.3.3.3 Roles and Responsibilities

Role	Responsibilities
IT Officer	Approves access rights architecture and enforces access control policies across systems.
System Administrators	Implement access changes, maintain logs, monitor activity, and report violations.
Data Owners	Approve user access requests to datasets under their jurisdiction.
All Users	Use access credentials securely and report anomalies.

4.3.3.4 Policy Statement

ERERA shall implement role-based access control (RBAC) principles to ensure that access to data is strictly limited to those with authorized, documented business needs. All access shall be:

- Based on "least privilege" and "need-to-know" principles;
- Assigned and approved using formal workflows;
- Logged, monitored, and reviewed periodically;
- Revoked immediately upon role change, contract termination, or inactivity.

4.3.3.5 Guiding Principles / Key Directives

4.3.3.5.1 Access Levels and Privileges

Access to ERERA data shall be divided into:

- **Read-Only Access** – Viewing data only;
- **Read/Write Access** – Creating or editing data;
- **Privileged Access** – Administrative/system-level authority;
- **Restricted Access** – Access to specific applications or datasets with clearance.

Access levels must correspond to a user's official job role and be reviewed regularly.

4.3.3.5.2 User Registration and Deregistration

- All users must complete an **Access Request Form** signed by their supervisor and the Data Owner;
- Users shall be assigned to appropriate **security groups** based on job functions;
- When a user leaves or changes roles, the account shall be:
    - **Disabled** within 24 hours;
    - **Deleted** after a review period;
    - **Access logs** archived as part of the exit checklist

4.3.3.5.3 Privileged Access Management

- Privileged accounts must be:
    - Assigned to named individuals;
    - Protected by strong authentication (e.g., MFA);
    - Logged and monitored for use patterns and anomalies;
- Shared or generic admin accounts are prohibited unless technically justified and tightly controlled.

4.3.3.5.4 Access Review and Audit

- All access rights must be:
    - Reviewed **quarterly** by System Admins in coordination with Data Owners;
    - Adjusted immediately upon detection of anomalies;
    - Logged for auditing for at least **12 months**.

4.3.3.5.5 Access to Sensitive and Confidential Data

- Access to data classified as **Confidential or Highly Restricted** requires:
    - Approval from the Data Owner and IT Officer;
    - Monitoring of all access logs;
    - Use of encrypted communication and storage mechanisms;
- Users accessing such data must have signed Non-Disclosure Agreements (NDAs).

4.3.3.5.6 Remote and Third-Party Access

- Remote access must be:
    - Approved in writing and time-bound;
    - Enforced via VPN, endpoint compliance checks, and MFA;
- Third-party access must be contractually governed and revoked upon completion of service delivery

4.3.3.6 Compliance and Enforcement

4.3.3.6.1 Monitoring

- System activity and access logs will be reviewed weekly;
- Suspicious access (e.g., after hours, cross-departmental) must be flagged and investigated.

4.3.3.6.2 Violations

- Any unauthorized access, privilege abuse, or failure to follow access workflows may result in:
    - Suspension or revocation of access;
    - Disciplinary action;
    - Legal or regulatory escalation in case of data breach.

4.3.3.6.3 Exceptions

- Access exceptions must be:
    - Requested formally and justified;
    - Approved by the IT Officer and Chairman;
    - Reviewed and revoked after 30 days unless renewed.

4.3.4 Data Privacy and Protection Policy

4.3.4.1 Purpose

The purpose of this policy is to ensure that personal data collected, processed, stored, or shared by ERERA is handled responsibly, lawfully, and in accordance with international and regional data protection standards. This policy sets out ERERA's approach to protecting the privacy of individuals whose data it manages, including employees, partners, regulatory stakeholders, and service recipients.

It ensures that ERERA meets obligations under applicable data protection regulations such as the **ECOWAS Supplementary Act on Personal Data Protection**, the **African Union Convention on Cybersecurity and Personal Data Protection**, and international frameworks including **GDPR**.

4.3.4.2 Scope

This policy applies to:

- All personal data and sensitive personal data held or processed by ERERA;
- All staff, interns, consultants, contractors, and third-party service providers with access to personal data;
- All information systems, manual files, cloud platforms, and communication tools used to manage personal information.

Personal data includes any information relating to an identified or identifiable natural person (e.g., name, ID number, contact details, employment records).

4.3.4.3 Roles and Responsibilities

Role	Responsibilities
Data Protection Officer (DPO)	Ensures compliance with privacy laws, oversees privacy program implementation, and manages data subject requests.
Data Owners / Department Heads	Define legal basis for collection and approve data processing activities.
ICT Department	Ensures security of personal data systems and supports breach response.
All Users / Employees	Comply with data protection procedures and report potential breaches.

4.3.4.4 Policy Statement

ERERA commits to safeguarding personal data through lawful, fair, and transparent practices. Personal data shall be:

- Collected for specific, legitimate purposes;

- Limited to what is necessary (data minimization);
- Accurate and up to date;
- Stored securely and retained only as long as needed;
- Processed with adequate technical and organizational safeguards;
- Subject to data subject rights (e.g., access, correction, erasure, objection).

4.3.4.5 Guiding Principles / Key Directives

4.3.4.5.1 Lawful Basis for Data Processing

- All personal data collection must be based on:
  - Consent;
  - Legal obligation;
  - Contractual necessity;
  - Public interest or legitimate organizational function.

4.3.4.5.2 Data Subject Rights

ERERA shall uphold the following rights of individuals:

- Right to be informed;
- Right to access their personal data;
- Right to rectification or erasure;
- Right to object to processing;
- Right to restrict or withdraw consent;
- Right to lodge complaints with supervisory authorities.

Requests must be responded to within 30 days.

4.3.4.5.3 Consent Management

- Consent must be freely given, specific, informed, and unambiguous;
- Records of consent must be retained for auditability;
- Individuals may withdraw consent at any time.
- All individuals whose personal data is collected shall be required to sign a **Consent and Confidentiality Agreement** documenting their understanding and approval of how their data will be used, stored, and protected.

4.3.4.5.4 Data Security Measures

- Access to personal data must be restricted using role-based controls;
- Encryption, masking, or pseudonymization must be applied to sensitive data;
- Systems housing personal data must be hardened and monitored;
- Personal data in transit (e.g., email) must be encrypted.

4.3.4.5.5 Cross-Border Data Transfers

- Personal data shall not be transferred outside of ECOWAS or the host jurisdiction without appropriate safeguards and compliance with trans-border data flow laws

4.3.4.5.6 Third-Party Processors

- All third-party service providers must sign a **Consent and Confidentiality Agreement** before accessing any personal data, to affirm their responsibility for data privacy and restricted use.
- Their access shall be limited, time-bound, and monitored;
- Vendors must meet ERERA's minimum technical and organizational safeguards.

4.3.4.5.7 Data Breach Response

- A **Data Breach Notification Procedure** shall be in place;
- High-risk breaches must be reported to the DPO and authorities within 72 hours;
- Affected individuals must be informed without undue delay when rights are impacted.

4.3.4.6 Compliance and Enforcement

4.3.4.6.1 Monitoring

- The DPO and Internal Audit shall:
    - Conduct privacy impact assessments (PIAs);
    - Monitor policy compliance and system configurations;
    - Track responses to data subject requests.

4.3.4.6.2 Non-Compliance

- Violations may result in:
    - Internal disciplinary measures;
    - Termination of contracts;

- Regulatory fines or public sanctions depending on severity.

4.3.4.6.3 Exception Handling

- Justified exceptions must be:
  - Documented by the DPO;
  - Approved by Executive Management;
  - Reviewed quarterly.

4.3.5 Data Compliance and Regulatory Alignment Policy

4.3.5.1 Purpose

The purpose of this policy is to ensure that ERERA's handling of data complies with all applicable legal, regulatory, institutional, and contractual requirements. This includes regional obligations under **ECOWAS**, national data protection laws, and international frameworks such as **ISO/IEC 27001**, **ISO/IEC 27701**, and, where applicable, the **General Data Protection Regulation (GDPR)**.

This policy provides a framework to identify data-related compliance requirements, monitor adherence, and ensure that ERERA's data practices reflect legal and ethical standards.

4.3.5.2 Scope

This policy applies to:

- All ERERA employees, contractors, partners, and stakeholders involved in data processing, storage, reporting, or sharing;
- All data types managed by ERERA, especially personal, financial, regulatory, and operational data;
- All systems and platforms where ERERA data is processed (on-premises or in the cloud);
- All external regulatory, funding, or oversight entities with jurisdiction over ERERA operations.

4.3.5.3 Roles and Responsibilities

Role	Responsibilities
Compliance Officer / Legal Advisor	Interprets data regulations and guides alignment with applicable frameworks.
Data Protection Officer (DPO)	Monitors data processing activities and facilitates compliance documentation.
IT Officer	Ensures systems, backups, and platforms comply with technical data standards.
Data Owners / Managers	Implement rules for record-keeping, retention, reporting, and audit readiness.
Internal Audit	Conducts periodic reviews of ERERA's data compliance practices.

4.3.5.4 Policy Statement

ERERA shall comply with all relevant regulatory and legal requirements regarding the processing, protection, reporting, and retention of data. All users of ERERA data must understand and adhere to

compliance obligations, which may include mandatory documentation, audits, training, and reporting to supervisory authorities.

ERERA's data environment shall be auditable, transparent, and aligned with risk-based data governance controls.

4.3.5.5 Guiding Principles / Key Directives

4.3.5.5.1 Regulatory Mapping and Register

- The Compliance Officer and DPO must maintain a **Data Regulatory Compliance Register**, detailing:
    - Applicable data laws (e.g., ECOWAS, host country data law);
    - Audit requirements (e.g., financial or donor reporting);
    - Data subject rights and obligations;
    - Licensing or sector-specific data mandates.

4.3.5.5.2 Recordkeeping and Audit Trails

- All critical data transactions and modifications must be traceable;
- Metadata and logs (who, when, what) must be retained for a minimum of **12 months**;
- Documented justification must exist for data collection and sharing practices.

4.3.5.5.3 Mandatory Policies and Controls

- All policies under Section 4.3 (e.g., access, classification, retention, backup) are mandatory compliance instruments;
- Any data-sharing agreements (with donors, partners, or national regulators) must be reviewed by Legal and documented.

4.3.5.5.4 Training and Awareness

- All ERERA employees must complete **annual data compliance training**;
- New employees must be inducted within **30 working days** of onboarding;
- ICT systems used for compliance reporting (e.g., SAP, SharePoint, monitoring portals) must **maintain records of user training**, but **training should be conducted in a dedicated test or training environment, not in the production system**.

4.3.5.5.5 Risk-Based Approach

- ERERA shall adopt a **risk-based framework** to prioritize regulatory controls where data loss, breach, or misuse may:
    - Trigger legal sanctions;
    - Disrupt regulatory activities;
    - Impact cross-border reporting or funding mechanisms.

4.3.5.5.6 Incident Reporting and External Coordination

- All suspected data violations or breaches must be escalated to the DPO and Executive Office within **24 hours**;
- Where applicable, regulatory bodies (e.g., ECOWAS Data Protection Authority) must be notified within **72 hours**.

4.3.5.6 Compliance and Enforcement

4.3.5.6.1 Monitoring and Audits

- The Internal Audit Unit shall:
    - Review compliance logs and register updates quarterly;
    - Audit system permissions and documentation practices annually;
    - Provide remediation timelines and verify corrective actions.

4.3.5.6.2 Enforcement

- Non-compliance may result in:
    - Suspension of system privileges;
    - Disciplinary action;
    - Legal escalation if institutional risks or data subject rights are breached.

4.3.5.6.3 Exception Handling

- All exceptions must be:
    - Formally requested and documented;
    - Reviewed by Legal and the Compliance Officer;
    - Approved by the Chairman and reviewed annually.

4.3.6 Data Retention and Disposal Policy

4.3.6.1 Purpose

The purpose of this policy is to define ERERA's requirements for the retention, archival, and secure disposal of data. It ensures that information is preserved for operational, legal, and historical needs and is securely discarded when it is no longer required, minimizing data-related risks and ensuring compliance with applicable laws.

4.3.6.2 Scope

This policy applies to:

- All electronic and physical data stored or processed by ERERA;
- All employees, consultants, and third parties who handle ERERA data;
- All data systems including servers, laptops, cloud storage, backup media, and removable devices;
- All forms of records including regulatory documents, emails, databases, reports, HR files, and system logs.

4.3.6.3 Roles and Responsibilities

Role	Responsibilities
Data Owners	Define retention timelines and approve disposal schedules for their data domains.
ICT Department	Ensure secure storage, backup, erasure, and destruction processes are implemented.
Records Management Officer	Oversees physical archiving and supports data retention audits.
All Users	Handle data in accordance with retention policies and report obsolete or excess records.

4.3.6.4 Policy Statement

ERERA shall retain information only for as long as it is legally, operationally, or historically required. When data exceeds its retention period or becomes obsolete, it shall be securely archived or disposed of in a manner that prevents unauthorized recovery or misuse.

Data destruction shall be carried out using methods appropriate to its sensitivity and medium.

4.3.6.5 Guiding Principles / Key Directives

4.3.6.5.1 Retention Schedules

- Data retention periods shall be documented in a **Data Retention Schedule**, which classifies records into the following categories:

Data Type	Retention Period	Retention Authority
Financial Records (SAP)	10 years	ECOWAS Finance Rules
HR and Employment Records	7 years post-employment	Labor and tax laws
Regulatory and Market Data	10 years or as mandated	ECOWAS Energy Market Regulations
Emails (Official Correspondence)	3 years	ERERA internal policy
Logs and System Activity Files	12 months	ISO/IEC 27001, forensic audit needs
Project Documents	Until project closure + 5 yrs	ERERA Project Management Framework

4.3.6.5.2 Archiving Criteria

- Data considered inactive but still valuable for reference or compliance shall be transferred to secure archival systems with access restrictions;
- Archived data must be labeled, catalogued, and accessible for authorized audit or retrieval.

4.3.6.5.3 Disposal Methods

- **Digital Data**:
    - Deletion using certified data erasure software;
    - Cryptographic erasure (for encrypted volumes);
    - Degaussing or physical destruction of storage devices (e.g., shredding, incineration);
- **Physical Documents**:
    - Shredding, pulping, or incineration for Confidential and Highly Restricted documents;
    - Secure recycling for Internal Use documents.

All disposal events must be recorded in a **Disposal Log**

4.3.6.5.4 Removable and Backup Media

- Backup tapes and removable drives must be tracked and stored securely;

- Media that has reached its retention limit must be erased or destroyed under supervision;
- Sensitive data on mobile media must be encrypted and protected by access controls.

4.3.6.5.5 Use of Third Parties for Disposal

- When using external providers for data destruction, ERERA must ensure:
    - Providers are certified (e.g., ISO 14001, ISO 27001);
    - Disposal is logged and witnessed;
- A certificate of destruction is issued and archived

4.3.6.6 Compliance and Enforcement

4.3.6.6.1 Monitoring

- The ICT Department and Internal Audit must:
    - Conduct annual audits of retention compliance;
    - Randomly inspect backup archives and disposal logs;
    - Review the Data Retention Schedule every two years.

4.3.6.6.2 Violations

- Failure to apply retention or disposal procedures may result in:
    - Regulatory penalties;
    - Loss of critical data or exposure of sensitive information;
    - Disciplinary actions for staff or termination of vendor contracts.

4.3.6.6.3 Exception Handling

- Data exempted from standard retention timelines (e.g., legal holds, investigations) must be documented by Legal or Executive Management;
- A justification note must accompany such exemptions and reviewed annually.

4.3.7 Data Quality and Integrity Policy

4.3.7.1 Purpose

The purpose of this policy is to establish governance controls that ensure the accuracy, completeness, consistency, reliability, and timeliness of ERERA's data across its systems and processes. Data quality is fundamental to effective regulatory decision-making, compliance, operational efficiency, and stakeholder trust.

This policy promotes standardized procedures for data validation, cleansing, and lifecycle management to safeguard data integrity at all times.

4.3.7.2 Scope

This policy applies to:

- All structured and unstructured data used by ERERA in digital and physical formats;
- All business systems that capture, process, or report data (e.g., SAP/ECOLINK, Microsoft 365, monitoring databases);
- All departments and personnel responsible for creating, managing, using, or reporting data;
- All regulatory, operational, administrative, and project-related data.

4.3.7.3 Roles and Responsibilities

Role	Responsibilities
Data Owners	Define and monitor data quality standards; validate compliance with use-case needs.
Data Stewards	Perform quality checks, ensure consistency, and implement corrective actions.
ICT Department	Enforce integrity rules in applications, ensure secure data movement and backups.
All Users	Enter, process, and verify data accurately; report anomalies or errors.

4.3.7.4 Policy Statement

ERERA shall maintain data integrity and quality through proactive validation, standardized input processes, and regular audits. All institutional data must be managed using defined quality standards tailored to its purpose, lifecycle, and sensitivity.

Information shall not be used in critical decision-making unless verified as accurate, complete, and timely by authorized personnel.

4.3.7.5 Guiding Principles / Key Directives

4.3.7.5.1 Data Quality Dimensions

All data assets must adhere to the following quality attributes:

- **Accuracy** – Data must reflect the real-world object or event correctly;
- **Completeness** – No required values or fields should be missing;
- **Consistency** – Data must be coherent across formats, systems, and time;
- **Timeliness** – Data should be current and available within acceptable timeframes;
- **Validity** – Data must conform to business rules and allowed value ranges;
- **Uniqueness** – No redundant or duplicate entries unless justified.

4.3.7.5.2 Quality Assurance Responsibilities

- Each Data Owner shall:
    - Define **acceptable quality thresholds** for their datasets;
    - Approve key controls for input validation;
    - Ensure regular cleansing and deduplication.
- Data Stewards must:
    - Use validation scripts, reports, or dashboards to identify and correct errors;
    - Escalate recurring quality issues;
    - Document remediation steps and outcomes

4.3.7.5.3 Validation and Cleansing

- Data inputs must be verified at the point of entry using:
    - Drop-down lists, validation rules, field constraints;
    - Auto-population and logic checks (e.g., date vs. age inconsistencies);
- Periodic batch validations shall be scheduled for master datasets (e.g., vendor lists, employee records);
- Duplicate records must be flagged and resolved using master data management rules.

4.3.7.5.4 Change Control and Auditability

- Any structural change to data models (e.g., new fields, changed formats) must be reviewed and approved via the Change Management Process;
- All data corrections must be traceable, with **before/after values** and change justifications logged.

4.3.7.5.5 Monitoring and Reporting

- A **Data Quality Dashboard** shall be developed to track key metrics:
    - Error rates;
    - Correction turnaround time;
    - User-driven data submissions;
    - Number of unresolved quality alerts per department.

4.3.7.6 Compliance and Enforcement

4.3.7.6.1 Monitoring

- Internal Audit and ICT will:
    - Conduct quarterly data quality reviews;
    - Validate audit logs of corrections;
    - Review master data management effectiveness.

4.3.7.6.2 Non-Compliance

- Repeated failure to maintain or correct data quality may result in:
    - Notification to management and possible reassignment of responsibilities;
    - Escalation to the Executive Office for disciplinary review;
    - Temporary data use suspension (e.g., for unreliable dashboards or reports).

4.3.7.6.3 Exception Handling

- In rare cases, data inconsistencies may be tolerated temporarily under:
    - A documented waiver with reasons;
    - Clear rectification timeline approved by the Data Owner.

4.3.8 Data Backup and Recovery Policy

4.3.8.1 Purpose

The purpose of this policy is to ensure the timely, secure, and complete backup of ERERA's critical data and the effective recovery of business services in the event of accidental deletion, hardware failure, natural disasters, cyber incidents, or system corruption. The policy supports operational continuity, protects institutional data assets, and aligns with regulatory obligations on data resilience.

4.3.8.2 Scope

This policy applies to:

- All data stored or processed on ERERA-managed systems, servers, applications, and endpoint devices;
- Data hosted in cloud applications (e.g., Microsoft 365, SAP/ECOLINK), physical servers, or virtual environments;
- Backup infrastructure (media, software, offsite storage);
- All staff, ICT personnel, and vendors involved in backup scheduling, execution, and recovery.

4.3.8.3 Roles and Responsibilities

Role	Responsibilities
IT Officer	Approves backup strategy, ensures compliance, and validates restoration capabilities.
System Administrators	Perform and monitor backups, manage storage devices, and execute recovery procedures.
Users	Store official files in designated backup folders; report data loss or corruption.
Audit/Compliance	Review logs and verify consistency with backup and DR policies.

4.3.8.4 Policy Statement

ERERA shall establish and maintain secure, verifiable backup systems and recovery procedures for all critical data and ICT services. Backup frequency and storage retention must reflect the classification, operational value, and recovery objectives of the data.

Recovery procedures shall be tested regularly to ensure integrity, speed, and compliance with ERERA's business continuity and disaster recovery plans.

4.3.8.5 Guiding Principles / Key Directives

4.3.8.5.1 Backup Strategy

- All users are assigned a **central backup folder**, accessible only over the ERERA LAN. They must **regularly copy official documents** to this location.
- Personal or unofficial files (e.g., videos, music) are not to be backed up to ERERA systems;
- Outlook email files (.PST) are backed up **quarterly**, or more frequently for high-volume users;
- Official documents deemed **Highly Confidential** may be backed up separately to encrypted removable drives, under user custody or fireproof storage.

4.3.8.5.2 Backup Frequency and Scope

Data Type	Backup Frequency	Storage Duration
File servers & shared drives	Daily (incremental), Weekly (full)	30–90 days
Email archives (Outlook PST)	Quarterly or upon request	12 months
System configurations	Weekly and before system changes	6 months
Cloud platforms (M365, SAP)	Aligned with vendor SLAs	Varies (must be auditable)

Backups must be encrypted and, where applicable, compressed for efficient storage.

4.3.8.5.3 Backup Storage and Protection

- All backups must be stored in **secure, access-controlled locations**, including:
  - **Onsite servers and appliances** (short-term);
  - **Fireproof safes or lockable cabinets** for external drives
  - **Offsite storage or secure cloud repositories** for long-term or disaster resilience.
- Backup media must be rotated and labeled clearly with timestamps and dataset identifiers.

4.3.8.5.4 Recovery Procedures

- Recovery must be conducted within defined **Recovery Time Objectives (RTO)** and **Recovery Point Objectives (RPO)** from ERERA's DR framework;
- All recovery efforts must:
  - Follow documented steps;

- Be authorized by the IT Officer;
- Include **post-restoration validation** (checksums, file integrity);

- Test recoveries shall be conducted **quarterly** for core systems.

4.3.8.5.5 Monitoring and Logs

- All backup operations must be:
  - Logged automatically where possible;
  - Reviewed **weekly** for failures or incomplete jobs;
  - Documented in a **Backup and Recovery Register** for audit readiness.

4.3.8.6 Compliance and Enforcement

4.3.8.6.1 Monitoring

- Internal Audit will review:
  - Backup job success/failure trends;
  - Retention compliance;
  - Recovery drills and outcomes.

4.3.8.6.2 Non-Compliance

- Failure to comply with this policy may result in:
  - Data loss and operational disruption;
  - Disciplinary action for negligence;
  - Liability for breach of institutional data obligations.

4.3.8.6.3 Exception Handling

- Exceptions (e.g., for legacy systems or during upgrades) must be:
  - Documented with justification;
  - Approved by the IT Officer;
  - Reviewed within one month.

4.3.9 Supporting Procedures

This section serves as a reference to the detailed procedures that underpin the policies outlined in Domain 4.3. These procedures provide the granular, step-by-step instructions necessary to effectively implement the policy directives. They are maintained separately from the policies themselves to allow for agile updates without requiring a full policy review, while ensuring full traceability and alignment.

The following is a consolidated list of supporting procedures referenced across the above policies, designed to provide operational guidance:

Policy	Procedure ID	Supporting Procedure	Objective	Key Outcome/Benefit
4.3.6 Data Retention and Disposal Policy	**ERERA-ICT-PRO-4.3.6-001**	Data Retention Schedule Management SOP	Define how to create, update, and review retention timelines.	Ensures policy-aligned and legally valid retention across all systems.
4.3.8 Data Backup and Recovery Policy	**ERERA-ICT-PRO-4.3.8-001**	User Data Backup Responsibility and Folder Use SOP	Guide staff on what data to back up and how to use backup folders.	Improves user contribution to data resilience.

4.4 Risk Management, Business Continuity, and Disaster Recovery

As a regional regulatory authority, ERERA relies on resilient, secure, and continuously available ICT services to fulfill its mission. This section defines the framework by which ERERA anticipates, assesses, mitigates, and recovers from disruptions—whether technical, operational, cyber-related, or environmental. The policies in this domain ensure that ERERA's ICT ecosystem remains dependable and prepared to respond to both anticipated and unforeseen events.

Grounded in ISO/IEC 27005 (Information Security Risk Management), ISO 22301 (Business Continuity Management), and ECOWAS crisis response directives, this section establishes integrated controls for:

- ICT risk identification and treatment;
- Business impact analysis and critical function mapping;
- Disaster recovery and continuity planning;
- Crisis communication protocols;
- Testing, exercising, and improvement of preparedness plans.

The objective is not only to ensure survival during disruptions but to enable rapid recovery and continuity of critical services with minimal loss or operational impact.

4.4.1 IT Risk Assessment and Mitigation Policy

4.4.1.1 Purpose

This policy establishes ERERA's framework for identifying, assessing, evaluating, and mitigating risks to its Information and Communication Technology (ICT) assets and services. Its purpose is to protect ERERA's information assets, ensure the confidentiality, integrity, and availability of information, and maintain operational resilience in alignment with strategic objectives.

4.4.1.2 Scope

This policy applies to all ERERA ICT assets, information systems, applications, data, infrastructure, and services, including those managed by third-party vendors or cloud service providers. It covers all personnel, contractors, and third parties who access, process, or manage ERERA's ICT resources.

4.4.1.3 Roles and Responsibilities

Role	Responsibility
ERERA Management	Provides overall direction and resources for IT risk management and approves the risk management framework and risk appetite.

IT Department / CISO	Responsible for developing, implementing, and overseeing the IT risk management process, maintaining the risk register, and coordinating risk assessments.
Risk Management Committee	Reviews and advises on significant IT risks, mitigation strategies, and risk treatment plans.
Asset Owners (Business Process Owners & IT System Owners)	Identify risks related to their specific assets, participate in risk assessments, and approve risk treatment plans for their areas.
Internal Audit	Provides independent assurance on the effectiveness of the IT risk management process.
All Staff	Responsible for reporting identified vulnerabilities and potential risks to the IT Department.

4.4.1.4 Policy Statement

ERERA is committed to systematically identifying, assessing, and treating IT-related risks to ensure the security, continuity, and compliance of its information systems and services. A structured, proactive, and continuous IT risk management process will be maintained, aligning with ERERA's overall enterprise risk management framework and relevant international and regional standards.

4.4.1.5 Guiding Principles/Key Directives

- **Risk Identification:** Regular and systematic identification of potential threats and vulnerabilities to ERERA's ICT assets and services.
- **Risk Assessment:** Conduct comprehensive risk assessments (qualitative and/or quantitative) to evaluate the likelihood and impact of identified risks, considering confidentiality, integrity, and availability criteria.
- **Risk Evaluation:** Compare assessed risk levels against ERERA's defined risk appetite and criteria for risk acceptance.
- **Risk Treatment:** Develop and implement appropriate risk treatment plans to mitigate, transfer, avoid, or accept identified risks, prioritizing those exceeding the risk appetite.
- **Continuous Monitoring:** Establish a process for ongoing monitoring and review of identified risks and the effectiveness of implemented controls.
- **Reporting & Communication:** Regularly report on the status of IT risks to relevant stakeholders, including management and the Risk Management Committee.
- **Compliance Integration:** Ensure IT risk management considers and addresses regulatory and legal requirements, including ECOWAS Cybersecurity Guidelines and data protection directives.
- **Integration with BC/DR:** IT risk assessment findings shall inform and support Business Impact Analysis (BIA) and Business Continuity/Disaster Recovery (BC/DR) planning. (ITIL 4: Service Continuity Management)

4.4.1.6 Compliance and Enforcement

Compliance with this policy will be monitored through regular internal audits, management reviews, and performance metrics related to risk management. Non-compliance may result in disciplinary action up to and including termination of employment or contract, and may lead to legal consequences as per ERERA's policies and applicable laws (including ECOWAS Cybersecurity Guidelines on cybercrime).

4.4.2 Business Impact Analysis (BIA) Policy

4.4.2.1 Purpose

This policy defines ERERA's approach to conducting Business Impact Analyses (BIAs). The purpose of the BIA is to identify and prioritize critical business functions and processes, determine the potential impact of disruptions to these functions, and establish recovery requirements such as Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). This forms a foundational element for ERERA's Business Continuity and Disaster Recovery planning.

4.4.2.2 Scope

This policy applies to all business units, departments, functions, and processes within ERERA that are critical to its operations, mission, and regulatory compliance. It covers all information systems, applications, data, infrastructure, and personnel that support these critical functions.

4.4.2.3 Roles and Responsibilities

Role	Responsibility
ERERA Management	Provides strategic oversight and approves the BIA methodology and prioritization of critical functions.
Business Process Owners (Department Heads)	Primarily responsible for identifying their critical business functions, assessing potential impacts of disruptions, and defining recovery requirements (RTO, RPO, MTD) for their respective processes.
IT Department / BC/DR Coordinator	Facilitates the BIA process, provides technical input on system dependencies, and translates business recovery requirements into IT recovery strategies.
Risk Management Committee	Reviews and validates the BIA findings and critical function prioritization.
Internal Audit	May review the BIA process and outcomes for completeness and accuracy.

4.4.2.4 Policy Statement

ERERA shall conduct regular and systematic Business Impact Analyses to understand the criticality of its business functions and the potential consequences of their disruption. The BIA will serve as the basis for establishing appropriate recovery objectives (RTOs, RPOs) and developing effective business continuity and disaster recovery strategies.

4.4.2.5 Guiding Principles/Key Directives

- **Regularity:** BIAs shall be conducted periodically (annually) and whenever there are significant changes to business processes, organizational structure, or IT systems.

- **Stakeholder Engagement:** Active participation of Business Process Owners and relevant stakeholders is crucial to accurately identify critical functions, dependencies, and potential impacts.
- **Impact Assessment:** The BIA will assess the impact of disruptions across various dimensions, including financial, reputational, operational, legal, regulatory (e.g., ECOWAS Cybersecurity Guidelines), and safety.
- **Dependency Mapping:** Identify and document dependencies between business processes, supporting IT systems, infrastructure, external services, and key personnel.
- **Recovery Requirements:** Clearly define and document Recovery Time Objectives (RTO), Recovery Point Objectives (RPO), and Maximum Tolerable Downtime (MTD) for each critical business function and its supporting IT assets. (ITIL 4: Service Continuity Management)
- **Data-Driven Decisions:** The BIA results will be quantitative and qualitative data to drive decisions regarding business continuity strategies, resource allocation, and investment in resilience.
- **Documentation:** All BIA findings, including critical functions, impact assessments, dependencies, RTOs, and RPOs, shall be formally documented and maintained.

4.4.2.6 Compliance and Enforcement

Adherence to this policy will be verified through audits of BIA documentation and integration of BIA findings into BC/DR plans. Failure to participate in or adequately complete BIA activities may result in the prioritization of other functions during a crisis, potentially leading to significant business disruption.

4.4.3 Business Continuity and Disaster Recovery (BC/DR) Policy

4.4.3.1 Purpose

This policy outlines ERERA's commitment to establishing, implementing, and maintaining robust Business Continuity (BC) and Disaster Recovery (DR) capabilities. Its purpose is to ensure the continued availability of critical business functions and information systems in the face of disruptive events, minimizing downtime, data loss, and impact on ERERA's operations and mission.

4.4.3.2 Scope

This policy applies to all ERERA business units, departments, IT systems, infrastructure, data, facilities, and personnel involved in critical business operations. It covers all stages of a disruptive event, from preparation and response to recovery and restoration.

4.4.3.3 Roles and Responsibilities

Role	Responsibility
ERERA Management	Provides overall strategic direction, approves BC/DR strategies and resource allocation, and champions the BC/DR program.
BC/DR Steering Committee / Crisis Management Team	Oversees the BC/DR program, approves plans, activates plans during incidents, and makes strategic decisions during a crisis.
IT Department / BC/DR Coordinator	Develops, implements, maintains, and tests IT Disaster Recovery plans, coordinates IT recovery efforts, and provides technical expertise during a disruption.
Business Process Owners (Department Heads)	Develop, maintain, and test departmental Business Continuity Plans, ensure their personnel are trained, and manage the recovery of their respective functions during an incident.
All Employees	Understand their assigned roles and responsibilities within BC/DR plans and strictly follow established procedures during a disruptive event to support overall recovery efforts.
Internal Audit	Provides independent assurance on the effectiveness, adequacy, and ongoing implementation of the BC/DR program and its associated plans.

4.4.3.4 Policy Statement

ERERA shall implement and maintain comprehensive Business Continuity and Disaster Recovery plans derived from Business Impact Analysis (BIA) and risk assessments. These plans will enable ERERA to respond effectively to disruptive incidents, recover critical operations and IT systems, and minimize the impact on its stakeholders and regulatory obligations.

4.4.3.5 Guiding Principles/Key Directives

- **Risk-Based Approach:**
  - BC/DR planning will be informed by the outcomes of IT Risk Assessments (4.4.1) and Business Impact Analyses (4.4.2), prioritizing critical functions and systems based on their defined RTOs and RPOs.
  - Local redundancy will support scenarios identified in risk assessments and BIAs where cloud dependency presents a high risk.
- **Plan Development:** Comprehensive, documented BC/DR plans shall be developed for all critical business functions and supporting IT infrastructure, detailing response, recovery, and restoration procedures.
- **Recovery Strategies:**
  - Appropriate recovery strategies (e.g., hot site, warm site, cold site, cloud-based recovery, redundancy, data backup) will be selected based on RTO/RPO requirements and cost-effectiveness.
  - Desktop-based methods will act as cost-effective alternatives when cloud recovery (e.g., from a hot or warm site) is not immediately viable.
- **Desktop-Based Continuity Fallback:** In the event that cloud services are unavailable, staff shall continue operations using pre-approved desktop procedures, which include local data entry, offline documentation, and secure storage protocols. These procedures shall be documented and integrated with recovery workflows.
- **Incident Response Integration:** BC/DR plans will integrate with ERERA's overall incident management framework (ITIL 4: Incident Management) to ensure a coordinated and effective response to disruptions. It will also nclude offline work procedures in the incident management framework to maintain operations during cloud outages.
- **Regular Testing & Exercising:**
  - BC/DR plans will be regularly tested and exercised to validate their effectiveness, identify gaps, and ensure personnel proficiency. (Refer to 4.4.7 DR Testing and Exercising Procedures Policy).
  - Desktop continuity procedures will be periodically tested alongside regular BC/DR drills.
  - Desktop recovery processes will be inclued in the Post-Recovery Review to identify and correct usability or security issues.
- **Continuous Improvement:** Lessons learned from tests, exercises, and actual incidents will drive continuous improvement of BC/DR plans and capabilities.
- **Documentation & Review:** All BC/DR plans, procedures, and related documentation will be formally maintained, version-controlled, and reviewed periodically (at least annually) or after significant changes.
- **Legal & Regulatory Compliance:** BC/DR planning will consider all relevant legal and regulatory requirements, including those specified in the ECOWAS Cybersecurity Guidelines for critical information infrastructure protection.

4.4.3.6 Compliance and Enforcement

Compliance with this policy will be ensured through mandatory participation in BC/DR training and exercises, regular audits of plan documentation, and verification of recovery capabilities. Non-compliance may lead to significant operational disruptions and potential disciplinary action.

4.4.4 Communication and Crisis Management Policy

4.4.4.1 Purpose

This policy establishes a clear framework for managing communications and coordinating responses during and after disruptive incidents, crises, or disasters affecting ERERA's operations, reputation, or stakeholders. Its purpose is to ensure timely, accurate, and consistent communication to internal and external audiences, facilitate effective decision-making, and maintain public trust during challenging times.

4.4.4.2 Scope

This policy applies to all personnel, contractors, and third parties involved in ERERA's operations during a crisis or disruptive event. It covers all internal communications (e.g., staff, management) and external communications (e.g., media, regulators, partners, the public) related to the incident.

4.4.4.3 Roles and Responsibilities

Role	Responsibility
ERERA Management / Crisis Management Team (CMT)	Holds ultimate authority for crisis management and strategic communication decisions; approves key messages and overarching communication strategies.
Crisis Communications Lead (e.g., Head of PR/Communications)	Develops and implements the crisis communication plan, drafts official messages, manages media relations, and serves as the primary spokesperson or designates one.
IT Department	Provides timely updates on the status of IT systems, recovery progress, and relevant technical information to the CMT and Communication Lead.
Department Heads	Provide accurate information on the impact of the crisis on their respective business functions and coordinate internal communications within their departments.
Legal Counsel	Reviews all internal and external communications for legal implications, ensuring compliance with relevant laws and regulations before dissemination.
All Staff	Are responsible for understanding and adhering to established communication protocols, refraining from unauthorized or informal communication during a crisis to maintain message consistency.

4.4.4.4 Policy Statement

ERERA shall maintain a structured and proactive approach to crisis communication and management to ensure effective coordination, transparent information dissemination, and timely response during any

disruptive event. All communications will be coordinated, accurate, and consistent to minimize panic, mitigate reputational damage, and facilitate recovery efforts.

4.4.4.5 Guiding Principles/Key Directives

- **Centralized Coordination:** All crisis communications will be coordinated through the designated Crisis Management Team and Crisis Communications Lead to ensure consistency and control.
- **Timeliness & Accuracy:** Communications will be issued promptly, providing accurate and verified information, updated regularly as the situation evolves.
- **Transparency (Appropriate):** Information will be shared transparently where appropriate, without compromising sensitive data or ongoing investigations.
- **Stakeholder Identification:** Clearly identify all internal and external stakeholders requiring communication (e.g., employees, board, regulators, partners, media, customers, public).
- **Pre-approved Messages:** Develop pre-approved message templates and communication channels for various crisis scenarios.
- **Designated Spokespersons:** Only authorized and trained individuals will act as spokespersons for ERERA during a crisis.
- **Media Management:** Establish clear protocols for engaging with media, including press releases, interviews, and social media responses.
- **Regulatory Reporting:** Ensure timely reporting to relevant regulatory bodies as required, particularly for cybersecurity incidents as per ECOWAS Cybersecurity Guidelines.
- **Post-Crisis Review:** Conduct a post-crisis review to evaluate the effectiveness of communication and crisis management strategies and identify areas for improvement.

4.4.4.6 Compliance and Enforcement

Adherence to this policy is mandatory for all personnel. Unauthorized or inaccurate communication during a crisis may result in disciplinary action. The effectiveness of communication protocols will be evaluated during BC/DR exercises and post-incident reviews.

4.4.5 Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) Policy

4.4.5.1 Purpose

This policy establishes the framework for defining, documenting, and periodically reviewing Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for ERERA's critical business functions and supporting IT systems. The purpose is to ensure that recovery capabilities align with business needs and risk appetite, providing clear targets for Business Continuity and Disaster Recovery planning.

4.4.5.2 Scope

This policy applies to all ERERA business functions, processes, and the IT systems and data that support them. RTOs and RPOs will be defined for all identified critical assets and services derived from the Business Impact Analysis (BIA).

4.4.5.3 Roles and Responsibilities

Role	Responsibility
ERERA Management	Approves the methodology for RTO/RPO determination and endorses the final RTO/RPO targets as aligned with ERERA's risk appetite.
Business Process Owners (Department Heads)	Primarily responsible for determining and articulating the RTO and RPO for their critical business processes, based on the acceptable impact of downtime and data loss.
IT Department / BC/DR Coordinator	Translates business RTO/RPO requirements into technical recovery strategies and ensures IT systems and infrastructure can meet these objectives.
Risk Management Committee	Reviews the proposed RTOs and RPOs in the context of overall organizational risk tolerance.
Internal Audit	Verifies that established RTOs and RPOs are realistic, supported by BIA findings, and adequately addressed in recovery plans.

4.4.5.4 Policy Statement

ERERA shall define, document, and review Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for all critical business functions and supporting IT systems. These objectives will be derived from a comprehensive Business Impact Analysis (BIA) and will guide the selection and implementation of appropriate recovery strategies, ensuring that recovery efforts meet the organization's tolerance for disruption and data loss.

4.4.5.5 Guiding Principles/Key Directives

- **Business-Driven:** RTOs and RPOs will be primarily determined by business needs and the acceptable impact of disruption and data loss, as identified through the Business Impact Analysis (BIA).
- **Quantifiable:** RTOs will specify the maximum tolerable time to restore business functions to operational status after an incident, and RPOs will specify the maximum tolerable amount of data loss measured from the point of disruption.
- **Cost-Benefit Analysis:** The definition of RTOs and RPOs will consider the cost-effectiveness of achieving these objectives versus the potential cost of disruption.
- **Alignment with Risk Appetite:** RTOs and RPOs must be consistent with ERERA's overall risk appetite for business disruption and data loss.
- **Regular Review:** RTOs and RPOs will be formally reviewed at least annually, or whenever there are significant changes to business processes, IT systems, or the threat landscape.
- **Documentation:** All defined RTOs and RPOs, along with their justifications from the BIA, will be formally documented and readily accessible to relevant stakeholders.
- **Feasibility and Testability:** Recovery strategies and plans must be designed to realistically achieve the defined RTOs and RPOs, and their achievement will be validated through regular testing.

4.4.5.6 Compliance and Enforcement

Adherence to this policy will be verified through the BIA process, internal audits, and the outcomes of DR testing. Discrepancies between established RTO/RPO and actual recovery capabilities must be reported to management, and corrective actions taken.

4.4.6 Single Point of Failure Mitigation Policy

4.4.6.1 Purpose

This policy establishes ERERA's commitment to identifying, analyzing, and mitigating Single Points of Failure (SPOFs) within its critical IT infrastructure, systems, and processes. The purpose is to enhance the resilience, availability, and reliability of ERERA's essential services by reducing reliance on single components whose failure could lead to widespread disruption.

4.4.6.2 Scope

This policy applies to all critical IT infrastructure components (hardware, software, network devices, power supply, environmental controls), applications, data pathways, and key personnel involved in supporting ERERA's critical business functions. It encompasses both on-premises and cloud-based services.

4.4.6.3 Roles and Responsibilities

Mitigating Single Points of Failure is crucial for maintaining operational continuity. This section details the key **roles** and their **responsibilities** in proactively identifying, assessing, and implementing solutions to eliminate or reduce SPOFs across ERERA's IT environment.

Role	Responsibility
ERERA Management	Provides strategic direction and approves resource allocation for SPOF mitigation initiatives.
IT Operations and Infrastructure Teams	Primarily responsible for identifying, documenting, and implementing technical solutions to mitigate SPOFs.
Solution Architects/Engineers	Design systems and architectures with redundancy and fault tolerance to avoid SPOFs.
Business Process Owners	Highlight critical services and processes whose underlying IT components should be free of SPOFs.
Risk Management Committee	Reviews significant SPOFs and their associated risks, advises on mitigation strategies.
Internal Audit	Provides independent assurance on the effectiveness of SPOF identification and mitigation efforts.

4.4.6.4 Policy Statement

ERERA is committed to systematically identifying and mitigating single points of failure across its critical IT infrastructure and services. Through architectural design, redundancy, fault tolerance, and strategic planning, ERERA will strive to eliminate or reduce dependencies on individual components whose failure could cause unacceptable disruption to business operations.

4.4.6.5 Guiding Principles/Key Directives

- **Proactive Identification:** Conduct regular assessments to identify potential SPOFs within critical IT systems, networks, data storage, power, and environmental controls.
- **Criticality-Based Prioritization:** Prioritize SPOF mitigation efforts based on the criticality of the business functions they support, as determined by the Business Impact Analysis (BIA) and risk assessments.
- **Mitigation Strategies:** Implement appropriate mitigation strategies, including but not limited to:
    - **Redundancy:** Duplication of critical components (e.g., redundant power supplies, network links, servers).
    - **Fault Tolerance:** Designing systems to continue operating despite the failure of individual components (e.g., clustering, load balancing).
    - **Diversification:** Using multiple vendors or technologies to avoid a single point of failure at the supplier level.
    - **Geographic Dispersion:** Distributing critical resources across multiple physical locations to protect against regional disasters.
    - **Backup & Recovery:** Ensuring robust backup and recovery mechanisms are in place, even if components are not fully redundant.
- **Architectural Design:** Incorporate SPOF mitigation principles into the design and acquisition of new IT systems and infrastructure.
- **Regular Review & Testing:** Periodically review and test the effectiveness of implemented SPOF mitigation strategies, especially after significant changes to the IT environment.
- **Documentation:** Maintain comprehensive documentation of identified SPOFs, their associated risks, and implemented mitigation strategies.

4.4.6.6 Compliance and Enforcement

Failure to mitigate critical SPOFs may result in unacceptable downtime, financial loss, and reputational damage. Compliance will be monitored through periodic reviews and risk assessments. Persistent non-compliance may result in management escalation or disciplinary action

4.4.7 DR Testing and Exercising Procedures Policy

4.4.7.1 Purpose

This policy mandates and defines ERERA's approach to regularly testing and exercising its Disaster Recovery (DR) and Business Continuity (BC) plans. Its purpose is to validate the effectiveness and viability of these plans, identify gaps or deficiencies, ensure personnel proficiency, and build confidence in ERERA's ability to recover from disruptive events.

4.4.7.2 Scope

This policy applies to all documented Disaster Recovery and Business Continuity plans, critical IT systems and infrastructure, recovery sites, communication channels, and all personnel involved in plan execution. It covers various types of tests and exercises designed to simulate disruptive events.

4.4.7.3 Roles and Responsibilities

Role	Responsibility
ERERA Management / BC/DR Steering Committee	Approves the DR testing program, reviews test results, and ensures that resources are allocated for necessary improvements.
BC/DR Coordinator / Program Manager	Develops, schedules, and oversees the overall DR testing and exercising program. Coordinates test activities.
IT Department	Designs and executes technical DR tests, validates recovery objectives (RTO/RPO), and manages IT infrastructure for testing.
Business Process Owners (Department Heads)	Participate in and lead business continuity exercises for their respective departments, validating their roles and procedures.
Internal Audit	May observe tests and review test results to provide independent assurance on the testing program's effectiveness and compliance.
All Participants	Actively participate in assigned test roles and provide accurate feedback on the test outcomes.

4.4.7.4 Policy Statement

ERERA shall conduct regular, comprehensive, and documented tests and exercises of its DR and BC plans. The testing program is designed to validate recovery capabilities, assess system readiness, identify areas for improvement, ensure personnel competence, and drive continuous enhancement of ERERA’s resilience posture.

4.4.7.5 Guiding Principles / Key Directives

- **Regular Testing**: Conduct DR and BC tests at predefined intervals (e.g., annually or bi-annually) and after significant system or organizational changes.
- **Risk-Based Prioritization**: Testing priorities will be based on risk exposure, system criticality, and BIA results.
- **Variety of Test Scenarios**: Include a broad range of realistic, plausible scenarios (e.g., cyber-attack, hardware failure, natural disaster) in alignment with ECOWAS Cybersecurity Guidelines.
- **Diverse Test Types** :
    - ***Tabletop Exercises*:** Walkthroughs to discuss response plans and identify gaps.
    - ***Simulation Exercises***: Operational role-play under simulated disaster conditions.
    - ***Component/System Tests***: Validate recovery of specific IT systems.
    - ***Full-Scale / End-to-End Tests***: Simulate an organization-wide disaster event and recovery.
- **Defined Objectives & Metrics**: Each test must have clearly defined scope, objectives, and success metrics (e.g., RTO/RPO achievement).
- **Inclusion of External Dependencies**: Where applicable, include critical third-party systems and services in tests.
- **Comprehensive Documentation**: Maintain records of test plans, execution steps, outcomes, and variances.
- **Post-Test Review**: Perform formal debriefings to identify lessons learned and improvement opportunities.
- **Corrective Action & Improvement**: Deficiencies identified during tests must lead to documented corrective actions, plan updates, and continual improvement.
- **Minimal Impact to Production**: DR tests must be planned to minimize operational disruption, ideally using isolated environments or maintenance windows.

4.4.7.6 Compliance and Enforcement

All designated personnel must participate in scheduled DR and BC tests. Non-compliance with testing requirements or failure to act on findings may result in disciplinary actions. The effectiveness and completeness of the DR testing program will be subject to periodic audits and management reviews.

4.4.8 Training and Awareness for Continuity

4.4.8.1 Purpose

This policy outlines ERERA's commitment to providing ongoing training and awareness programs related to Business Continuity (BC) and Disaster Recovery (DR). Its purpose is to ensure that all relevant personnel understand their roles and responsibilities during disruptive events, are proficient in executing BC/DR procedures, and are aware of the importance of business continuity to ERERA's mission.

4.4.8.2 Scope

This policy applies to all ERERA employees, contractors, and third parties who have roles or responsibilities within Business Continuity Plans, Disaster Recovery Plans, Crisis Management Teams, or those whose actions could impact the continuity of ERERA's operations.

4.4.8.3 Roles and Responsibilities

Role	Responsibilities
ERERA Management	Champions the BC/DR training and awareness program, allocates necessary resources, and ensures senior management participation.
HR Department	Collaborates with the BC/DR Coordinator to integrate BC/DR training into employee onboarding and ongoing professional development programs.
BC/DR Coordinator / Program Manager	Develops the BC/DR training curriculum, identifies target audiences, coordinates training delivery, and maintains training records.
Department Heads / Business Process Owners	Ensure their teams participate in relevant BC/DR training and exercises, and reinforce the importance of continuity within their departments.
IT Department	Provides technical training related to IT Disaster Recovery procedures and tools.
Crisis Communications Lead	Provides training on crisis communication protocols.
All Staff	Participate in assigned training and awareness activities and understand their individual roles in continuity plans.

4.4.8.4 Policy Statement

ERERA shall establish and maintain a comprehensive and continuous training and awareness program for Business Continuity and Disaster Recovery. This program will equip all relevant personnel with the

knowledge, skills, and understanding necessary to effectively contribute to ERERA's resilience and recovery efforts during and after disruptive incidents.

4.4.8.5 Guiding Principles/Key Directives

- **Role-Based Training:** Training programs will be tailored to specific roles and responsibilities within BC/DR plans (e.g., Crisis Management Team members, IT recovery personnel, department-specific BC leads).
- **Mandatory Participation:** Participation in designated BC/DR training and awareness activities will be mandatory for all assigned personnel.
- **Regular Refreshers:** Training will not be a one-time event; regular refreshers and updates will be provided to ensure ongoing proficiency and adaptation to plan changes.
- **Awareness Campaigns:** Implement organization-wide awareness campaigns (e.g., posters, emails, intranet articles) to promote a culture of continuity and highlight the importance of BC/DR.
- **Integration with Onboarding:** New employees will receive an introduction to ERERA's BC/DR policies and their general responsibilities during the onboarding process.
- **Practical Application:** Training will incorporate practical exercises and simulations to reinforce learning and build confidence in executing procedures.
- **Documentation and Tracking:** Maintain records of all training activities, attendance, and assessment results to demonstrate compliance and identify training gaps.
- **Feedback and Improvement:** Collect feedback on training effectiveness and continuously improve the program based on participant input, test results, and actual incident reviews.
- **Compliance with Guidelines:** Ensure training content addresses awareness requirements stemming from regional guidelines, such as general cybersecurity awareness elements from ECOWAS Cybersecurity Guidelines.

4.4.8.6 Compliance and Enforcement

Compliance with this policy will be monitored through training attendance records, effectiveness evaluations, and observations during DR tests and BC exercises. Failure to complete mandatory training may result in limitations on an employee's responsibilities or disciplinary action.

4.4.9 Supporting Procedures

This section serves as a reference to the detailed procedures that underpin the policies outlined in Domain 4.4. These procedures provide the granular, step-by-step instructions necessary to effectively implement the policy directives. They are maintained separately from the policies themselves to allow for agile updates without requiring a full policy review, while ensuring full traceability and alignment.

The following is a consolidated list of supporting procedures referenced across the above policies, designed to provide operational guidance:

Policy Name	Procedure ID	Supporting Procedure	Procedure Objective	Key Outcome/Benefit
4.4.1 IT Risk Assessment and Mitigation Policy	**ERERA-ICT-PRO-4.4.1-001**	IT Risk Assessment	Systematically identify, analyze, and evaluate potential threats and vulnerabilities to ERERA's ICT assets and services.	Clear understanding of ERERA's IT risk landscape; Prioritized risks for treatment.
	ERERA-ICT-PRO-4.4.1-002	Risk Register Management	Maintain a centralized, up-to-date repository of all identified IT risks, their assessment details, treatment plans, and current status.	Centralized risk oversight; Facilitates risk reporting and decision-making.
4.4.3 Business Continuity and Disaster Recovery (BC/DR) Policy	**ERERA-ICT-PRO-4.4.3-001**	BC/DR Plan Development	Create detailed plans for responding to disruptive events, covering emergency procedures, recovery steps for critical business functions, and IT systems.	Comprehensive, actionable recovery plans; Organized approach to disaster response.

4.4.4 Communication and Crisis Management Policy	**ERERA-ICT-PRO-4.4.4-001**	Crisis Management Team Activation	Define the roles, responsibilities, and triggers for assembling and activating the Crisis Management Team (CMT) during an incident.	Centralized crisis leadership; Ensures rapid, coordinated response.
4.4.5 Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) Policy	**ERERA-ICT-PRO-4.4.5-001**	RTO/RPO Definition	Define the maximum acceptable downtime (RTO) and maximum tolerable data loss (RPO) for each critical business function and supporting IT system, based on BIA findings.	Quantifiable recovery targets; Guides effective resource allocation for BC/DR.
4.4.6 Single Point of Failure Mitigation Policy	**ERERA-ICT-PRO-4.4.6-001**	SPOF Identification and Mapping Procedure	Systematically identify and document all single points of failure (SPOFs) within critical IT infrastructure, applications, and processes.	Comprehensive inventory of vulnerabilities; Highlights critical dependencies.
4.4.7 DR Testing and Exercising Procedures Policy	**ERERA-ICT-PRO-4.4.7-001**	DR Test Execution Procedure	Conduct technical disaster recovery tests according to plan, simulating failures and validating the recovery of IT systems and data to meet RTO/RPO.	Validated IT recovery capabilities; Technical readiness confirmed.
4.4.8 Training and Awareness for Continuity	**ERERA-ICT-PRO-4.4.8-001**	Training Curriculum Development	Design and develop comprehensive training modules, materials, and exercises that cover ERERA's BC/DR policies, plans, procedures, and individual roles.	Standardized and effective training content; Enhances understanding and proficiency.

4.5 IT Governance, Organization, and Communications

Effective ICT governance ensures that ERERA's technology investments and operations are aligned with its regulatory mission, strategic goals, and stakeholder expectations. This section outlines the principles and practices that guide the organizational structure, decision-making, vendor engagement, and communication standards within ERERA's ICT function.

Grounded in COBIT 2019, ISO/IEC 38500 (Corporate Governance of IT), and ECOWAS procurement and oversight regulations, this section supports strategic ICT alignment through clear policies on:

- Resource usage and acceptable ICT behavior;
- Internal and external communication governance;
- Website and social media controls;
- ICT procurement lifecycle;
- Cloud and vendor risk management;
- ICT organizational structure and responsibilities.

Together, these policies promote transparency, accountability, value delivery, and security, ensuring that ICT is not only a support function but a well-managed, strategic enabler.

4.5.1 Acceptable Use Policy

4.5.1.1 Purpose

This policy defines the acceptable and unacceptable use of ERERA's Information and Communication Technology (ICT) resources. Its purpose is to protect ERERA's information assets, ensure the security and integrity of its ICT systems, promote a productive work environment, and ensure compliance with legal and ethical standards.

4.5.1.2 Scope

This policy applies to all ERERA employees, contractors, consultants, temporary staff, volunteers, and any other individuals who access or use ERERA's ICT resources, regardless of their location or the device used (ERERA-owned or personal). ICT resources include, but are not limited to, computers, networks, software, hardware, internet access, email, mobile devices, and data storage systems.

4.5.1.3 Roles and Responsibilities

Role	Responsibilities
ERERA Management	Provides overall strategic direction for ICT policies, endorses the Acceptable Use and Security Policy, and ensures enforcement across the organization.

IT Department	Implements and maintains technical controls, monitors ICT resource usage, investigates policy violations, and ensures compliance with security standards.
Human Resources Department	Coordinates with IT and management on disciplinary measures related to policy breaches; integrates policy awareness into onboarding and training.
Legal Counsel	Advises on compliance with applicable legal and regulatory requirements, including data protection and ECOWAS Cybersecurity Guidelines.
All Users	Must understand, accept, and adhere to the policy; responsible for ethical and secure use of ERERA's ICT resources.

4.5.1.4 Policy Statement

ERERA's ICT resources are provided primarily for conducting ERERA's business. All users are expected to utilize these resources responsibly, securely, ethically, and in compliance with all applicable laws, regulations (including ECOWAS Cybersecurity Guidelines), and ERERA policies. Limited and reasonable personal use is permitted, provided it does not interfere with job performance, consume excessive resources, or violate any other policy.

4.5.1.5 Guiding Principles/Key Directives

- **Business Use Primary:** All ICT resources are primarily for ERERA business operations.
- **Security & Confidentiality:** Users must take all reasonable steps to protect ERERA's information and systems from unauthorized access, disclosure, modification, or destruction. This includes protecting passwords, not sharing credentials, and reporting security incidents immediately.
- **Legal and Ethical Conduct:** Users must not engage in any activity that is illegal, unethical, or violates ERERA's code of conduct. This includes activities prohibited by ECOWAS Cybersecurity Guidelines (e.g., cybercrime, unauthorized access, data misuse).
- **Intellectual Property:** Respect intellectual property rights, including copyrights, trademarks, and patents, when using ERERA's ICT resources.
- **Privacy:** Users should have no expectation of privacy when using ERERA's ICT resources, as ERERA reserves the right to monitor usage for security, operational, and compliance purposes. Any monitoring will be conducted in accordance with applicable laws.
- **Resource Conservation:** Users should use ICT resources efficiently and avoid excessive consumption of bandwidth, storage, or processing power for non-business purposes.
- **Prohibited Activities:** Prohibited activities include, but are not limited to:
    - Accessing, creating, or distributing offensive, discriminatory, or harassing content.
    - Unauthorized access to systems or data (hacking).
    - Introduction of malware (viruses, worms, ransomware).
    - Sending unsolicited bulk emails (spam).
    - Gambling, illegal downloads, or unauthorized streaming.

- Engaging in political lobbying or partisan activities.
- Operating a personal business.
- Any activity that compromises ERERA's reputation or legal standing.

- **Software Usage:** Only authorized and licensed software may be installed and used on ERERA's ICT resources.

4.5.1.6 Compliance and Enforcement

Violations of this policy may result in disciplinary action, up to and including termination of employment or contract, and may also lead to civil or criminal legal proceedings in accordance with applicable laws (e.g., ECOWAS Cybersecurity Guidelines on cybercrime). ERERA reserves the right to monitor and audit ICT resource usage to ensure compliance with this policy.

4.5.2 Electronic Communication and Email Policy

4.5.2.1 Purpose

This policy governs the appropriate, secure, and professional use of ERERA's electronic communication systems, including email, instant messaging, collaboration platforms, and any future digital communication tools. The purpose is to:

- Ensure effective and efficient business communication;
- Safeguard ERERA's data, reputation, and legal standing;
- Promote responsible digital communication behavior; and
- Align with legal, regulatory, and cybersecurity requirements (including ECOWAS Cybersecurity Guidelines).

These measures support ERERA's mission by reducing the risk of data breaches, reputational damage, and legal non-compliance through misuse or compromise of electronic communication channels.

4.5.2.2 Scope

This policy applies to all ERERA employees, contractors, consultants, interns, and third-party service providers who use ERERA's electronic communication systems, whether via ERERA-owned or personally owned devices, and whether on-site or remote.

It includes but is not limited to:

- Email services
- Instant messaging (IM)
- Video conferencing and chat tools
- Internal and external collaboration platforms (e.g., Teams, SharePoint)
- Future electronic communication technologies approved by ERERA

Personal device use must comply with ERERA's **Bring Your Own Device (BYOD)** Policy and security standards.

4.5.2.3 Roles and Responsibilities

Role	Responsibilities
ERERA Management	Provides oversight, approves communication standards, and ensures organization-wide policy adoption.
IT Department	Manages communication systems, ensures technical controls, implements security measures, and enforces configurations and access controls.

Legal Counsel	Advises on privacy, intellectual property, data retention, and legal discovery obligations in accordance with relevant regional laws and ECOWAS Cybersecurity Guidelines.
All Users	Must use ERERA's communication tools responsibly, securely, and in compliance with this policy and associated procedures.

4.5.2.4 Policy Statement

ERERA's electronic communication systems are provided primarily for official business use. Users must ensure that all communications:

- Are professional, respectful, and business-appropriate.
- Protect confidential and sensitive information.
- Comply with ERERA's policies and applicable legal/regulatory requirements.
- Support ERERA's public image, values, and communication standards.

ERERA reserves the right to monitor and audit communications for business, security, or legal purposes while maintaining data privacy and ethical oversight.

4.5.2.5 Guiding Principles / Key Directives

- **Professional Conduct:** Communications must be courteous, respectful, and aligned with ERERA's ethical standards. Hate speech, harassment, or offensive content is strictly prohibited.
- **Confidentiality and Security:** Sensitive information must only be sent to authorized recipients. Use encryption for confidential emails or attachments where required.
- **Data Protection Compliance:** Personal data should be handled according to applicable data protection laws and ERERA's Data Handling and Classification Policy.
- **Appropriate Use:** Communications must not include illegal, obscene, defamatory, or unauthorized copyrighted content.
- **Email Signatures:** All external emails must include a standardized ERERA signature block with job title, contact information, and disclaimer.
- **Mass Messaging Controls:** Unsolicited mass emails, spam, or chain messages unrelated to ERERA business are prohibited.
- **Use of Distribution Lists:** Use mailing groups only for their intended purpose. Avoid unnecessary "Reply All" communications.
- **Email Retention:** Email is an official record. Communications should follow ERERA's Records Management and Retention Policies.
- **Monitoring and No Expectation of Privacy:** ERERA may monitor electronic communications with proper justification. All such actions will be logged and reviewed to ensure transparency and compliance with applicable laws.

- **Out-of-Office Messaging:** All users must enable an automatic out-of-office reply during extended absence, including contact information for backup personnel.
- **Cybersecurity Vigilance:** All users must be alert to phishing, spam, and malware threats. Suspicious communications must be reported immediately.

4.5.2.6 Compliance and Enforcement

Non-compliance may result in disciplinary actions including suspension of ICT privileges, formal reprimands, contract termination, or legal prosecution under applicable laws. ERERA's internal audit, HR, and compliance teams may conduct reviews to ensure adherence.

Users must report any misuse, security incidents, or suspected violations to the IT Service Desk or the Compliance Officer.

4.5.3 Website and Social Media Management Policy

4.5.3.1 Purpose

This policy establishes comprehensive guidelines and controls for the creation, content management, security, and usage of ERERA's official websites and social media channels. Its purpose is to ensure that ERERA's digital presence accurately reflects its mission, values, and professional image, facilitates effective stakeholder communication, protects ERERA's reputation, and complies with all applicable legal and regulatory requirements.

4.5.3.2 Scope

This policy applies to all digital platforms officially owned, managed, or affiliated with ERERA, including websites, subdomains, microsites, and verified social media accounts across various platforms (e.g., Facebook, Twitter, LinkedIn, YouTube). It covers all ERERA employees, contractors, consultants, and authorized third parties involved in the creation, publication, moderation, or management of content on these platforms.

4.5.3.3 Roles and Responsibilities

Role	Responsibilities
ERERA Management	Approves overall digital strategy and ensures allocation of resources for implementation.
Communications / Public Relations Department	Manages content, tone, and public engagement for official websites and social media, ensuring alignment with ERERA's messaging, branding, and values.
IT Department	Maintains technical infrastructure, security, hosting, access control, and data integrity; conducts security audits and vulnerability assessments.
Legal Counsel	Reviews content and activities for legal compliance, copyright, intellectual property, data protection (ECOWAS Cybersecurity Guidelines), and defamation risks.
Content Owners/Contributors (Departments)	Provide accurate, verified, and approved content for their respective website sections or social media themes.
Designated Social Media Managers	Authorized personnel to post and moderate official social media accounts on behalf of ERERA.

4.5.3.4 Policy Statement

ERERA's official websites and social media channels are vital communication and engagement tools. ERERA commits to maintaining a digital presence that is accurate, secure, professional, compliant with all applicable laws and regulations (including ECOWAS Cybersecurity Guidelines), and consistently reflective of ERERA's mission, values, and reputation.

Guiding Principles / Key Directives

- **Accuracy and Quality:** All published content must be accurate, up-to-date, relevant, grammatically correct, fact-checked, and verified before publication.
- **Branding and Image:** Content must strictly adhere to ERERA's branding guidelines, maintaining a consistent, professional corporate image.
- **Security:** Robust security measures must be implemented and maintained to prevent unauthorized access, data breaches, defacement, or service disruption. Regular security audits and vulnerability assessments are mandatory.
- **Authorization and Access Control:** Access to website backend systems and social media accounts is restricted to authorized personnel only, with access rights granted on a least-privilege basis and reviewed periodically.
- **Data Protection and Privacy:** Personal data collected through digital platforms must be processed in compliance with ERERA's Data Protection Policy and ECOWAS Cybersecurity Guidelines. Clear, accessible privacy notices and cookie consent must be provided where applicable.
- **Legal Compliance:** All content and activities must comply with applicable national and international laws, including but not limited to copyright, intellectual property, defamation, data protection, accessibility, and cybersecurity regulations.
- **Content Approval Process:** A formal workflow for content creation, review, and approval must be strictly followed before publishing on any official digital platform.
- **Monitoring and Engagement:** Websites and social media channels will be actively monitored for user comments, inquiries, and potential issues. Engagement must be respectful and professional, and crisis communication plans must be in place to address negative feedback or reputational threats.
- **Accessibility:** Websites and digital content should conform to recognized accessibility standards to ensure usability for individuals with disabilities.
- **Record Keeping:** Significant interactions, content, and changes are subject to ERERA's records retention policies and applicable legal requirements.
- **Training and Awareness:** All personnel responsible for content publishing, moderation, or platform management must receive training on digital communication standards, cybersecurity risks, and ERERA's policies.

- **Personal Use vs. Official Representation :** ERERA employees are reminded to exercise discretion on personal social media platforms and ensure that personal opinions are not misrepresented as official ERERA statements.

4.5.3.5 Compliance and Enforcement

Violations of this policy, especially those that jeopardize ERERA's reputation, security, or legal compliance, may result in disciplinary action up to and including termination of employment or contract, and may incur legal consequences. Regular audits and reviews of website and social media content, security configurations, and management practices will be conducted to ensure ongoing compliance.

4.5.4 ICT Procurement and Vendor Management Policy

4.5.4.1 Purpose

This policy establishes a standardized and transparent framework for the acquisition and lifecycle management of Information and Communication Technology (ICT) hardware, software, services, and related goods by ERERA. Its purpose is to ensure that all ICT procurements are cost-effective, strategically aligned, secure, legally compliant, and efficiently managed throughout their lifecycle.

4.5.4.2 Scope

This policy applies to all ERERA departments and personnel involved in the initiation, planning, approval, sourcing, contracting, and management of any ICT-related acquisition, regardless of value or procurement method (e.g., direct purchase, licensing, cloud services, consultancy). Procurement thresholds and approval levels shall be governed by ERERA's Procurement Policy and ECOWAS procurement regulations.

4.5.4.3 Roles and Responsibilities

Role	Responsibility
ERERA Management	Provides strategic direction for ICT investments and approves major ICT procurements.
Procurement Department	Leads procurement processes, manages vendor relationships, ensures regulatory compliance, and negotiates contracts.
IT Department	Defines technical specifications, evaluates solutions, assesses security and integration needs, and manages ICT assets.
Legal Counsel	Reviews and approves all ICT contracts to ensure compliance with legal, cybersecurity, and data protection standards.
Finance Department	Verifies budget availability and authorizes financial aspects of ICT procurements.
Risk Management Committee	Reviews and advises on significant risks associated with ICT procurements, particularly those involving critical services or data.

4.5.4.4 Policy Statement

ERERA shall implement a systematic, secure, and controlled approach to ICT procurement and vendor management to ensure all acquisitions support strategic objectives, deliver optimal value, comply with relevant legal, regulatory, and cybersecurity requirements, and are managed throughout their lifecycle.

4.5.4.5 Guiding Principles / Key Directives

- **Strategic Alignment**: All ICT procurements must align with ERERA's ICT strategy, enterprise architecture, and business objectives.
- **Needs-Based Procurement**: All acquisitions must be based on documented business needs, functional requirements, and technical specifications. Avoid overprovisioning or unnecessary procurement.
- **Due Diligence and Vendor Assessment**: Vendors must be assessed for financial viability, technical capacity, legal compliance, and cybersecurity posture.
- **Ongoing Vendor Governance**: High-risk or critical vendors must undergo regular performance reviews, compliance monitoring, and, where applicable, third-party assurance (e.g., ISO 27001 or SOC 2).
- **Competitive Sourcing**: Transparent and competitive sourcing methods should be used whenever feasible to ensure fairness, cost-effectiveness, and best value.
- **Security by Design**: Security requirements including confidentiality, integrity, resilience, and compliance with ECOWAS Cybersecurity Guidelines must be integrated into all procurement stages.
- **Contractual Rigor**: All procurements must be governed by contracts detailing scope, SLAs, security requirements, data ownership, Intellectual Property (IP) rights, and exit/termination clauses.
- **Lifecycle Management**: Procurement must consider the full lifecycle of ICT assets from acquisition to retirement including cost, maintenance, support, upgrades, and secure disposal.
- **Risk Management Integration**: Risks related to vendors and ICT acquisitions must be identified and mitigated throughout the procurement lifecycle. *(Refer to 4.5.5 Vendor and Cloud Services Risk Management Policy)*
- **Transparency and Auditability**: Procurement activities must be documented to support transparency, traceability, and internal or external audits.
- **Ethical Conduct and Conflict of Interest**: Staff involved in ICT procurement must adhere to ERERA's Code of Conduct and disclose any real or perceived conflicts of interest.

4.5.4.6 Compliance and Enforcement

Failure to comply with this policy may result in disciplinary action, rejection of procurement requests, financial penalties, or legal consequences. Internal audits, contract reviews, and vendor performance evaluations will be conducted regularly to ensure compliance.

4.5.5 Vendor and Cloud Services Risk Management Policy

4.5.5.1 Purpose

This policy establishes ERERA's framework for identifying, assessing, mitigating, and monitoring risks associated with third-party Information and Communication Technology (ICT) vendors and cloud service providers. Its purpose is to protect ERERA's information assets, ensure service continuity, maintain regulatory compliance, and safeguard ERERA's reputation when relying on external parties for ICT services.

4.5.5.2 Scope

This policy applies to all existing and prospective third-party ICT vendors and cloud service providers that process, store, transmit ERERA's data, provide ICT infrastructure, software, platforms, or deliver services critical to ERERA's operations. This includes, but is not limited to, software-as-a-service (SaaS), platform-as-a-service (PaaS), infrastructure-as-a-service (IaaS), managed service providers (MSPs), and IT consultants.

4.5.5.3 Roles and Responsibilities

Role	Responsibility
ERERA Management / Risk Management Committee	Provides oversight for third-party risk management, defines the organization's vendor risk appetite, and approves significant vendor relationships.
IT Department / Chief Information Security Officer (CISO)	Leads technical and security assessments of vendors, monitors compliance, manages vendor-related security incidents, and ensures alignment with ERERA's security requirements.
Procurement Department	Manages the contractual process, ensuring that appropriate risk clauses, security obligations, and service level agreements (SLAs) are included in contracts.
Legal Counsel	Reviews vendor contracts for legal compliance, incorporating data protection clauses in line with ECOWAS Cybersecurity Guidelines, and ensuring proper liability and dispute resolution mechanisms.
Business Process Owners	Define the criticality of vendor-provided services and identify associated business and operational risks.
Internal Audit	Provides independent assurance on the effectiveness, adequacy, and implementation of the vendor risk management framework.

4.5.5.4 Policy Statement

ERERA is committed to systematically identifying, assessing, and managing risks associated with its ICT vendors and cloud service providers throughout their lifecycle. A robust vendor risk management program will be maintained to ensure that third-party services align with ERERA's security, compliance, operational, and business continuity requirements, particularly those concerning data protection and cybersecurity as per ECOWAS Cybersecurity Guidelines.

4.5.5.5 Guiding Principles/Key Directives

- **Due Diligence:** Conduct comprehensive due diligence on all prospective ICT vendors and cloud service providers before engagement, including assessment of their information security controls, compliance with relevant standards (e.g., ISO/IEC 27001), financial stability, and operational capabilities.
- **Risk Assessment:** Perform a formal risk assessment for each vendor, considering the criticality of the service, the type of data processed, the vendor's security posture, and potential impact of disruption or compromise.
- **Contractual Obligations:** Ensure all contracts with ICT vendors and cloud service providers clearly define:
    - Information security requirements and responsibilities.
    - Data protection and privacy obligations (including adherence to ECOWAS Cybersecurity Guidelines for data localization, cross-border data transfer, and breach notification).
    - Service Level Agreements (SLAs) including RTO/RPO expectations.
    - Audit and right-to-audit clauses.
    - Incident management and reporting procedures.
    - Business continuity and disaster recovery capabilities.
    - Termination clauses and exit strategies.
- **Continuous Monitoring:** Establish a program for ongoing monitoring of vendor performance, security posture, and compliance with contractual obligations throughout the contract lifecycle.
- **Incident Management:** Define clear procedures for managing and reporting security incidents and service disruptions involving third-party vendors. (ITIL 4: Incident Management)
- **Data Protection & Jurisdiction:** Special attention will be given to vendors handling personal or sensitive ERERA data, ensuring compliance with data protection laws and considering data residency and cross-border transfer implications as per ECOWAS Cybersecurity Guidelines.
- **Exit Strategy:** Develop and maintain exit strategies for critical vendor relationships to ensure a smooth transition of services and data in case of contract termination or vendor failure. (ITIL 4: Supplier Management)
- **Review and Audit:** Conduct periodic reviews and audits of vendor compliance with security and contractual requirements.

4.5.5.6 Compliance and Enforcement

Failure to comply with this policy may result in the non-engagement or termination of vendor contracts, and disciplinary action for ERERA personnel. Compliance will be verified through vendor risk assessments, contract audits, performance reviews, and incident management procedures.

4.5.6 IT Organizational Structure and Role Mapping Policy

4.5.6.1 Purpose

This policy defines ERERA's approach to establishing, documenting, and maintaining its Information Technology (IT) organizational structure and the clear mapping of roles, responsibilities, and reporting lines within the IT department. Its purpose is to ensure effective IT governance, operational efficiency, clear accountability, and appropriate segregation of duties to support ERERA's mission.

4.5.6.2 Scope

This policy applies to the entire ERERA IT department, including all full-time employees, part-time staff, contractors, and consultants performing IT functions. It also extends to any cross-functional roles or committees that have significant IT responsibilities or decision-making authority.

4.5.6.3 Roles and Responsibilities

Entity/Role	Responsibilities
ERERA Management	Approves the overall IT organizational structure and ensures its alignment with ERERA's strategic objectives and risk posture.
Head of IT (CIO/IT Director)	Designs, implements, and maintains the IT structure; defines IT roles and responsibilities; ensures adequate staffing and alignment with strategic direction.
Chief Information Security Officer (CISO) ***(if designated)***	Defines and manages information security roles, ensuring alignment with ERERA's security framework and SoD principles.
Enterprise Architect / IT Planner ***(if designated)***	Aligns IT structure with enterprise architecture and digital transformation strategies.
Human Resources Department	Collaborates on role definitions, job descriptions, recruitment, training, and performance evaluation for IT personnel.
Internal Audit	Reviews IT structure and role mapping for effectiveness, SoD enforcement, and compliance with internal controls.
All IT Personnel	Understand and adhere to their defined roles, responsibilities, and reporting lines; comply with governance and security expectations.

4.5.6.4 Policy Statement

ERERA shall maintain a clearly defined and documented IT organizational structure with explicit roles, responsibilities, reporting lines, and accountability for all IT functions and services. This structure will be designed to optimize operational efficiency, ensure proper governance, facilitate decision-making, and uphold security principles, including the segregation of duties.

4.5.6.5 Guiding Principles/Key Directives

- **Clarity and Accountability:** Every IT function and task will have clearly defined ownership and accountability assigned to specific roles or teams.
- **Segregation of Duties (SoD):** Critical IT responsibilities, especially those related to development, operations, and security, will be segregated to prevent conflicts of interest, reduce the risk of fraud, and enhance control effectiveness.
- **Operational Efficiency:** The IT organizational structure will be designed to support efficient delivery of IT services and effective management of IT processes.
- **Scalability and Flexibility:** The structure should be adaptable to accommodate growth, technological changes, and evolving business needs.
- **Documentation:** The IT organizational structure, including organizational charts, job descriptions, and reporting lines, will be formally documented and kept up-to-date.
- **Communication:** Changes to the IT organizational structure or significant role mappings will be communicated effectively to all affected personnel and relevant stakeholders.
- **Competence and Training:** All roles shall be defined with required skills and qualifications; training and development plans shall be maintained to ensure role effectiveness.
- **Access Role Alignment:** Job roles shall align with access privileges; system and data access must reflect defined responsibilities.
- **Governance Integration:** The IT organizational structure will support ERERA's overall IT governance framework, facilitating decision-making and oversight.

4.5.6.6 Compliance and Enforcement

Adherence to this policy will be verified through regular reviews of IT organizational charts, job descriptions, and internal audits. Non-compliance, such as unapproved changes to roles or reporting lines, may lead to corrective actions or disciplinary measures.

4.5.7 Supporting Procedures

This section serves as a consolidated reference to the detailed procedures that provide operational guidance for implementing the policies outlined in Domain 4.5. These procedures will offer step-by-step instructions and practical methodologies to ensure effective compliance and management of ERERA's IT Governance, Organization, and Communications.

Policy Name	Procedure ID	Supporting Procedure	Procedure Objective
4.5.1 Acceptable Use Policy	**ERERA-ICT-PRO-4.5.1-001**	User Account Management Procedure	To define the systematic processes for the creation, modification, and termination of user accounts, ensuring authorized and appropriate access to ERERA's ICT resources.
	ERERA-ICT-PRO-4.5.1-002	Security Incident Reporting Procedure	To outline the necessary steps for all users and staff to report suspected or actual security incidents related to ICT resources, ensuring timely detection, initial response, and appropriate escalation.
4.5.2 Electronic Communication and Email Policy	**ERERA-ICT-PRO-4.5.2-001**	Electronic Communication Acceptable Use Procedure	Defines permitted vs. prohibited behaviors in using communication tools.
	ERERA-ICT-PRO-4.5.2-002	Phishing and Spam Reporting Procedure	Instructions for identifying and reporting suspicious communications.

Policy Name	Procedure ID	Supporting Procedure	Procedure Objective
4.5.3 Website and Social Media Management Policy	**ERERA-ICT-PRO-4.5.3-001**	Website and Social Media Security Configuration Procedure	Guidelines for securing platforms, managing access credentials, and implementing technical safeguards.
4.5.4 ICT Procurement and Vendor Management Policy	**ERERA-ICT-PRO-4.5.4-001**	ICT Asset Registration and Lifecycle Management Procedure	To ensure all acquired ICT assets are recorded, tracked, maintained, and securely disposed of at end-of-life.
4.5.5 Vendor and Cloud Services Risk Management Policy	**ERERA-ICT-PRO-4.5.5-001**	Third-Party Risk Assessment Procedure	Steps for performing initial and recurring risk assessments for ICT vendors and service providers.
4.5.6 IT Organizational Structure and Role Mapping Policy	**ERERA-ICT-PRO-4.5.6-001**	Segregation of Duties (SoD) Matrix and Review Procedure	Identifies incompatible roles and defines periodic review mechanisms to maintain SoD integrity.

5 POLICY IMPLEMENTATION AND ENFORCEMENT

The implementation and enforcement of ICT policies are vital to ensuring that ERERA's governance framework is not merely documented, but fully integrated into daily practice. While policies provide the foundation for decision-making and risk mitigation, their true effectiveness depends on clear communication, robust training, consistent enforcement, and performance monitoring.

This section outlines how ERERA will institutionalize its ICT policies across departments and personnel, supported by structured awareness plans, measurable KPIs, and accountability mechanisms.

5.1 Communication and Awareness Plan

To promote a shared understanding of ICT responsibilities, ERERA shall implement a formal communication strategy that ensures all stakeholders are informed, engaged, and able to access relevant policy documents.

Key Communication Channels

Channel	Description
Intranet Portal	A centralized repository where all current ICT policies and procedures are hosted.
Executive Announcements	Memos and launch messages from the Chairman or IT Officer to reinforce importance.
Email Campaigns	Periodic summaries and "Did You Know?" tips to reinforce compliance expectations.
Posters & Visual Aids	Awareness materials displayed in offices to highlight core policy messages.

Target Audiences

All ERERA staff, consultants, vendors, and new hires must be included in communication efforts. Periodic reminders shall target high-risk or high-privilege users (e.g., administrators, finance staff).

5.2 Staff Training and Onboarding Strategy

Training is a cornerstone of effective policy implementation. ERERA will institutionalize ICT policy awareness through a two-tiered approach: **onboarding** for new staff and **ongoing training** for existing personnel.

Onboarding Plan

Component	Timeframe	Responsible Unit
ICT Orientation Session	Within first 10 working days	ICT Department & HR
Policy Acknowledgment Form	Before system access	HR / ICT
Basic Security Awareness Briefing	At induction	DPO / ICT Security Officer

All onboarding materials shall include summaries of critical policies (e.g., Acceptable Use, Data Privacy, Access Control).

Ongoing Training

Audience	Frequency	Focus Areas
All Staff	Annually	Passwords, phishing, device security, acceptable use
Managers & Directors	Annually	Risk ownership, compliance KPIs, audit readiness
System Administrators	Semi-annually	Backup procedures, change control, access management
Data Owners & Stewards	As Needed	Classification, retention, and data integrity

Training outcomes will be tracked in ERERA's HR Learning Management System and subject to annual audit.

5.3 Policy Enforcement and Disciplinary Measures

ERERA adopts a **tiered enforcement approach** based on severity, risk impact, and recurrence of non-compliance. This ensures that accountability is enforced fairly while promoting a culture of learning and compliance.

Enforcement Model

Violation Level	Examples	Corrective Measures
Minor	Non-compliance with email etiquette, weak password use	Verbal/written warning; re-training
Moderate	Unauthorized use of external storage, ignoring update alerts	Temporary access revocation; departmental report
Major	Unauthorized data sharing, bypassing access controls	Suspension; ICT investigation; Executive notification

Critical / Severe	Data breach, sabotage, insider threat, fraud	Termination; legal referral; mandatory reporting to authorities

All incidents must be documented in the **ICT Violation Register**, including actions taken and lessons learned.

5.4 Monitoring, KPIs, and Performance Metrics

To ensure that ICT policies are effectively implemented and regularly improved, ERERA will monitor policy enforcement through a set of quantitative and qualitative performance indicators.

Sample Monitoring Activities

Activity	Frequency	Conducted By
ICT Policy Compliance Dashboard	Quarterly	IT Officer & Internal Audit
Access Review & Reconciliation	Quarterly	System Administrators
Incident Trend Analysis	Monthly	ICT Security Officer
Training Compliance Report	Annually	HR / ICT
Policy Review Compliance Audit	Every 2 years (or as needed)	Internal Audit

Key Performance Indicators (KPIs)

KPI	Target
% of new staff completing onboarding ICT training	100% within 10 days
% of staff completing annual policy refresher	≥ 95%
% of critical systems with defined RTOs and RPOs	100%
% of quarterly access rights reviewed	100%
Number of unresolved policy violations after 30 days	0
Number of critical audit findings related to policy gaps	0

These KPIs will feed into the Executive ICT Governance Report presented to senior management each year.

6 REVIEW AND MAINTENANCE

This section defines the mechanisms by which ERERA ensures its ICT Policies and Procedures remain current, effective, and relevant in a continuously evolving technological and threat landscape. Regular review and controlled updates are critical for maintaining the integrity, security, and compliance of ERERA's information and communication technology environment.

6.1 Review and Update Schedule

6.1.1 Purpose

To establish a systematic process for the periodic review and necessary updating of all ERERA ICT policies and procedures, ensuring their continued relevance, effectiveness, and alignment with organizational objectives, technological advancements, and regulatory requirements.

6.1.2 Key Components

Component	Description
Scheduled Reviews	**Annual Review:** • Formal review of all ICT policies and procedures at least once every 12 months. • Evaluate effectiveness, clarity, compliance, and alignment with ERERA's strategic goals. **Bi-annual Management Review:** • Conducted every six (6) months by ERERA Management or a designated steering committee. • Focus on the overall ICT policy framework and performance indicators.
Triggers for Ad-hoc Reviews	Policies and procedures must be reviewed outside of scheduled intervals when triggered by: • Significant changes in ERERA's organizational structure, mission, or business processes. • Introduction of new technologies, systems, or services (e.g., cloud platforms). • Discovery of new or emerging threats, vulnerabilities, or major incidents. • Changes in laws, regulations, or regional guidelines (e.g., ECOWAS Cybersecurity Guidelines). • Findings from audits, risk assessments, or penetration tests.

	• Lessons learned from DR/BC tests or real incidents.
Review Scope	Each review must assess the following: • Whether the policy's objectives remain valid and are being met. • Clarity and conciseness of the policy language. • Practicality and enforceability of directives. • Compliance with internal standards and external regulations. • Integration with other related policies and procedures.

6.1.3 Roles and Responsibilities for Review:

Role	Responsibility
Policy Owners	Initiating, coordinating, and leading the review of policies under their purview.
IT Department / Security Team	Providing technical input and assessing policy alignment with current security practices and infrastructure.
Legal Counsel / Compliance Officer	Ensuring compliance with legal and regulatory obligations.
Business Process Owners	Providing input on the policy's impact on their operations.
ERERA Management / Steering Committee	Approving the outcomes of major reviews and any proposed significant changes.

6.2 Policy Change Request Process

6.2.1 Purpose

To establish a structured and controlled process for the initiation, assessment, approval, implementation, and communication of any proposed changes to ERERA's ICT policies and procedures. This process ensures that changes are justified, risks are evaluated, and impacts are understood before implementation, maintaining policy integrity and stability.

6.2.2 Key Components:

Component	Description
Change Request Submission	• Any ERERA personnel may initiate a policy change by submitting a formal **Policy Change Request Form** to the designated **Policy Administrator** or **ICT Governance Body**. • The form must include: o A clear description of the proposed change o The rationale for the change o Expected benefits or identified necessity
Initial Triage and Assignment	• The Policy Administrator or ICT Governance Body conducts an initial completeness check. • Valid requests are assigned to the relevant **Policy Owner** for detailed assessment and follow-up.
Impact Assessment and Risk Analysis	• The Policy Owner leads the assessment in consultation with relevant stakeholders (e.g., IT, Security, Legal, HR, and affected departments). • The analysis considers: o Technical implications and required system changes o Operational impacts on workflows and personnel o Compliance considerations (e.g., ECOWAS Cybersecurity Guidelines) o Potential security risks or benefits o Resource implications (e.g., time, budget, training needs)

Component	Description

Review and Recommendation	• The proposed change and impact findings are reviewed by a designated review panel (e.g., **ICT Governance Committee**, **Security Committee**).
	• The panel issues a formal recommendation:
	  ○ Approve
	  ○ Reject
	  ○ Request additional information or clarification

Approval Authority	• Final approval depends on the **criticality and scope** of the change. • Minor changes may be approved by the Policy Owner; major revisions require approval from senior management or the ICT Steering Committee.

Implementation and Communication	• Upon approval, the updated policy or procedure is implemented following ERERA's established **change management protocols**.
	• All affected personnel and stakeholders are formally notified.
	• Communication includes:
	  ○ Summary of updates
	  ○ Effective date
	  ○ Any training or awareness requirements

Validation and Post-Implementation Review	• Post-implementation monitoring ensures the policy change delivers the intended outcomes.
	• A review is conducted to:
	  ○ Validate policy effectiveness
	  ○ Identify any unintended impacts
	  ○ Inform potential follow-up actions

6.2.3 Policy Change Approval Tiers:

Change Type	Description	Approval Authority
Minor Changes	Grammatical corrections, minor clarifications, formatting updates.	Policy Owner
Moderate Changes	Procedural updates, non-critical technical adjustments.	IT Director or relevant Department Head
Major Changes	New policy introduction, significant scope alteration, high impact on operations/security/compliance.	ERERA Management or BC/DR Steering Committee

6.3 Document Control, Versioning, and Archiving

6.3.1 Purpose

To ensure the integrity, authenticity, accessibility, and traceability of all ERERA's ICT policies and procedures throughout their lifecycle. This includes systematic version control, secure storage, and orderly archiving of obsolete documents.

6.3.2 Key Components:

Component	Description
Centralized Document Repository	• All official ICT policies and procedures shall be stored in a secure, centralized electronic **Document Management System (DMS)** or a controlled **network drive**. • Access is **role-based** and governed by **access control policies**.
Document Naming Convention	• A consistent and structured **naming convention** must be used for all documents. • This ensures easy identification, searchability, and uniformity across policy and procedure files.

Versioning Control	• Use a standardized versioning format: **Major.Minor.Revision** (e.g., V1.0.0, V1.1.0, V2.0.0).
	• Each version must include:
	  ○ Date of publication
	  ○ Author or responsible party
	  ○ Summary of changes from the previous version
	• Only the **most current approved version** should be actively published and accessible for operational use.

Ownership and Review Dates	Each document must clearly identify: • The **owner** (responsible individual/department) • The **next scheduled review date** to ensure ongoing accuracy and relevance.

Access and Modification Controls	• Access to create, modify, approve, or publish documents must be restricted to **authorized personnel**.
	• A comprehensive **audit trail** must be maintained, capturing:
	  ○ Who made each change
	  ○ What was changed
	  ○ When the change occurred

Archiving of Obsolete Documents	• Superseded versions of policies and procedures must be securely **archived**, not deleted.
	• Archived documents must retain:
	  ○ Their original version numbers
	  ○ Full change and review history
	• Define **retention periods** in alignment with ERERA's **data retention policy** and applicable legal or regulatory requirements.

Recovery and Backup	• The DMS or document repository must be included in ERERA's **regular backup** and **disaster recovery** plans. • This ensures the **availability and integrity** of all policy and procedure documentation during incidents or system failures.

7 APPENDIX

7.1 Appendix 1 - Implementation Plan

See Attached Document "Appendix 1 – Implementation Plan"

7.2 Appendix 2 – Templates and Forms

This appendix provides standardized templates and forms referenced across ERERA's ICT Policies and Procedures Manual. These tools are essential for ensuring policy compliance, operational consistency, and auditable documentation across key ICT functions such as access control, change management, incident response, risk assessment, and continuity planning.

All forms and templates shall be:

- Maintained by the ICT Department in editable and printable formats;
- Version-controlled and reviewed biennially (or as policies change);
- Stored in a centralized, access-controlled folder accessible to authorized users.

7.2.1 List of Standardized Templates and Forms

Form ID	Template Name	Purpose	Linked Policy Domain
ERERA-TPL-01	Risk Assessment Template	Used to identify, score, and document ICT risks and vulnerabilities	4.4.1 IT Risk Assessment
ERERA-TPL-02	User Access Request Form	For requesting creation, modification, or deletion of user accounts	4.1.2 Access Control / 4.2.8 AD
ERERA-TPL-03	Policy Acknowledgment Form	Signed confirmation of staff awareness and acceptance of ICT policies	5.2 Staff Training and Enforcement
ERERA-TPL-04	Change Request Form (RFC)	To formally propose a change to any ICT system or service	4.2.3 Change Management
ERERA-TPL-05	Incident Reporting Form	For documenting ICT security incidents or disruptions	4.1.10 Incident Response

ERERA-TPL-06	Data Breach Notification Form	For notifying the DPO and authorities of personal data breaches	4.3.4 Data Privacy & Protection
ERERA-TPL-07	Backup and Restore Log Sheet	To log details of backup completion, storage location, and recovery results	4.3.8 Backup and Recovery
ERERA-TPL-08	Asset Inventory Template	Tracks hardware, software, ownership, location, and status	4.2.1 Asset Management
ERERA-TPL-09	Data Classification Labeling Template	Standardizes how sensitivity levels are tagged on digital/physical data	4.3.1 Data Classification
ERERA-TPL-10	Access Review Checklist	Used during periodic access and privilege reviews	4.1.2 Access Control
ERERA-TPL-11	Vendor Risk Assessment Questionnaire	Screens third-party vendors before service engagement	4.5.5 Vendor Risk Management
ERERA-TPL-12	BIA Data Collection Template	Gathers input for Business Impact Analysis (critical systems, RTOs, etc.)	4.4.2 Business Impact Analysis
ERERA-TPL-13	DR Test Evaluation Form	Documents the outcomes of DR exercises and tabletop simulations	4.4.7 DR Testing & Exercises
ERERA-TPL-14	ICT Policy Change Request Form	For suggesting updates to existing policies and procedures	6.2 Change Management

See Attached Document "Appendix 2 – Templates and Forms"

7.3 Appendix 3 – ICT Procedures (Supporting Procedures)

See Attached Document "Appendix 3 – ICT Procedures (Supporting Procedures)"