REPUBLIC OF KENYA

Centre for Mathematics, Science and Technology Education in Africa (CEMASTEA)

Doc. Ref:CEM/GOP/ICT Circulation Approved by Management Representative

General Operating Procedures

ICT PROCEDURE MANUAL

Signature		**Date**
Prepared by: Head of Department		16/09/2026
Controlled by: Management Representative		16/09/2026
Approved by: CEO		16/09/2026

Revision No.06

Copy No…….

TABLE OF CONTENTS

1.0 Purpose....4
2.0 Scope....4
3.0 Reference....4
4.0 Definition of Terms, Acronyms and Abbreviations....5
4.1 Acronyms and Abbreviations....5
4.2 Terms....5
5.0 Principal Responsibility....6
6.0 Method....6
6.1 Website Management....7
6.1.1 Web Content and Update Procedure....7
6.1.2 Website Availability and Performance Monitoring....7
6.2 Data Backup and Security....7
6.3 User Support....8
6.3.1 ICT Equipment Installation and Technical Support....8
6.3.2 ICT Equipment and Infrastructure Maintenance....9
6.3.3 ICT Equipment and Asset Management....9
6.3.4 Lending of ICT Equipment....10
6.3.5 Request for ICT Staff Services....10
6.3.6 Request for ICT Equipment Specifications....10
6.4 ICT Incident Management....11
6.5 User Account and Access Management....12
6.6 Information Security....12
6.7 Digital Platforms, Applications and Cloud Services....13
7.0 Key Performance Indicators....13
8.0 Retained Documentation....14
9.0 Annexes....15
9.1 Process interaction matrix....15
9.2 ICT Processes Maps....16

9.2.1 Website Management....16
9.2.2 ICT Equipment and Infrastructure Maintenance 16
9.2.3 Data Backup and Security....17
9.2.4 ICT Equipment Installation and Technical Support 17
9.2.5 ICT Equipment and Asset Management....18
9.2.6 Lending of ICT Equipment....18
9.2.7 Request for ICT Staff Services 19
9.2.8 Request for ICT Equipment Specifications 19

GENERAL

1.0 Purpose

The purpose of this procedure is to ensure that ICT services, systems, infrastructure, information and support activities at CEMASTEA are planned, delivered, maintained and monitored in a secure, reliable, efficient and accountable manner to support ICT integration in STEM education, training and research, in accordance with the CEMASTEA Quality Manual, approved ICT Policy and applicable standards and requirements.

2.0 Scope

This procedure applies to ICT services and resources provided or administered by CEMASTEA, including website management and monitoring; data backup, security and restoration; ICT user support, equipment installation and maintenance; ICT equipment and asset management; lending of ICT equipment; ICT staff and event support; ICT procurement specifications and technical verification; ICT incident management; user account and access management; information security; and the management and support of digital platforms, applications and cloud services. Related matters, including data protection, change management, vulnerability management, disaster recovery, business continuity, and the use of AI and emerging technologies, shall be addressed in accordance with applicable CEMASTEA policies, procedures and requirements.

3.0 Reference

3.0.1 CEMASTEA Quality Manual

3.0.2 ISO 9001:2015 Standard

3.0.3 CEMASTEA Strategic Plan 2023-2027

3.0.4 CEMASTEA ICT Policy

3.0.5 CEMASTEA Communication Policy

3.0.6 ICT e-government standards

3.0.7 Data Protection ACT, 2019

3.0.8 CEMASTEA Data Protection Policy

3.0.9 Computer Misuse and Cybercrimes Act, 2018

3.0.10 National Cybersecurity Strategy 2022

3.0.11 Kenya AI Strategy 2025–2030

3.0.12 Kenya Cloud Policy (2025) Implementation Guidelines

4.0 Definition of Terms, Acronyms and Abbreviations

In addition to the relevant common definitions of terms given in ISO 9000, the following definitions shall apply:

4.1 Acronyms and Abbreviations

Acronym/Abbreviation	Definition
ICT	Information and Communication Technology
ICTO	Information and Communication Technology Officer
KPI	Key Performance Indicator
KENET	Kenya Education Network
PM	Preventive Maintenance
SOP	Standard Operating Procedure

4.2 Terms

4.2.1 Backup: A separate copy of data maintained for recovery following loss, corruption, accidental deletion or system failure.

4.2.2 Critical ICT Service: An ICT service whose prolonged unavailability may materially affect CEMASTEA's core operations, learning, training, communication or statutory functions.

4.2.3 ICT Asset: Hardware, software, licence, application, cloud resource, network component, digital service or other technology resource owned, leased or administered by CEMASTEA.

4.2.4 ICT Incident: An unplanned interruption, degradation, security event or failure affecting an ICT service, system, device, network or information resource.

4.2.5 Process Owner: The officer responsible for the business content, data or service for which ICT provides technical support.

4.2.6 Restoration: The process of recovering data or ICT services from a backup or other recovery source.

4.2.7 Service Request: A request by an authorised user for an ICT service, installation, access, configuration, information or assistance.

5.0 Principal Responsibility

The Coordinator ICT shall ensure that this procedure remains adequate for its intended purpose, is effectively implemented, and is periodically reviewed. ICT Officers shall implement assigned ICT activities and controls and maintain the required records. Process owners and users shall provide the information and support required for ICT service delivery and comply with approved ICT procedures, information security requirements and reporting obligations. Management shall provide the necessary oversight, resources and approvals to support effective implementation of this procedure.

6.0 Method

ICT activities shall be performed in accordance with the procedures and process controls provided in this manual. Where a detailed Standard Operating Procedure (SOP), checklist or form exists, the relevant document shall be used. ICT shall maintain evidence of activities performed and monitor implementation using the approved Key Performance Indicators (KPIs).

6.1 Website Management

6.1.1 Web Content and Update Procedure

6.1.1.1 The Communication Office shall provide website content to ICT for upload. Where website content is submitted directly by a process owner, the process owner shall ensure that the content has been appropriately verified and approved before submitting it to ICT for publication.

6.1.1.2 ICT shall publish approved website content within two working days of receipt from the Communication Office or process owner.

6.1.1.3 ICT shall unpublish or archive website content within two working days upon receipt of an authorised request from the Communication Office or process owner.

6.1.2 Website Availability and Performance Monitoring

6.1.2.1 The ICT Department shall monitor the availability and functionality of the CEMASTEA website to ensure that it remains accessible.

6.1.2.2 ICT shall periodically check the website for availability, functionality, page loading issues, broken links, missing or incorrectly displayed content, and other technical issues that may affect users.

6.1.2.3 ICT shall record website availability and performance issues and actions taken for resolution and review the records quarterly.

6.2 Data Backup and Security

6.2.1 ICT shall maintain an approved backup schedule that specifies the data and ICT services to be backed up, the backup frequency and the applicable backup method based on their criticality.

6.2.2 ICT shall protect backup data against unauthorised access, alteration, loss and deletion through approved access controls and secure storage, including encryption where required.

6.2.3 ICT shall maintain documented restoration procedures and prioritise the recovery of critical ICT services in accordance with approved recovery requirements. Restoration activities shall be recorded.

6.2.4 Backup retention periods shall be defined in accordance with applicable business, legal and operational requirements. Where technically practicable, backup copies shall be maintained separately from the primary data environment to reduce the risk of simultaneous loss.

6.2.5 ICT shall test restoration of selected backups in accordance with an approved testing schedule and retain records of the restoration tests and any corrective actions arising.

6.2.6 ICT shall monitor scheduled backups, investigate failed or incomplete backups and take appropriate corrective action.

6.3 User Support

6.3.1 ICT Equipment Installation and Technical Support

6.3.1.1 ICT support requests shall be submitted through an authorised communication channel to the Coordinator ICT or directly to an ICT Officer.

6.3.1.2 Where the Coordinator ICT receives a request, the request shall be assigned to an appropriate ICT Officer for action. Where a request is received directly by an ICT Officer, the ICT Officer shall record the request in the approved job card.

6.3.1.3 The ICT Officer shall assess the request, undertake the required technical support and record the diagnosis, action taken, equipment or system affected, date and outcome in the job card.

6.3.1.4 For installation of new ICT equipment, the ICT Officer shall configure the equipment using the approved installation/configuration checklist, including required software, security settings and updates, within two working days where all required resources are available.

6.3.1.5 Where the required technical support is beyond available ICT expertise or capability, the ICT Officer shall escalate the matter to the Coordinator ICT for

appropriate action, including referral to an authorised service provider where necessary.

6.3.2 ICT Equipment and Infrastructure Maintenance

6.3.2.1 The ICT Officer shall prepare an annual preventive maintenance schedule covering CEMASTEA ICT equipment and infrastructure and submit it to the Coordinator ICT for approval.

6.3.2.2 The Coordinator ICT shall approve the preventive maintenance schedule and issue a notification memo together with the schedule to staff at least three working days before commencement of the scheduled maintenance.

6.3.2.3 The ICT Officer shall carry out preventive maintenance in accordance with the approved schedule over the scheduled five-day maintenance period.

6.3.2.4 The ICT Officer shall record the equipment or infrastructure serviced, maintenance performed and observations in the approved Preventive Maintenance (PM) Form.

6.3.2.5 Where corrective maintenance is identified during preventive maintenance, the ICT Officer shall record the required action and follow up through the appropriate ICT technical support and maintenance activities under Sections 6.3.1 and 6.3.2.

6.3.2.6 Upon completion of the preventive maintenance exercise, the ICT Officer shall prepare a preventive maintenance report documenting the activities undertaken, equipment and infrastructure serviced, findings and any recommended follow-up actions.

6.3.2.7 ICT shall retain the approved preventive maintenance schedule, notification memo, completed preventive maintenance forms and report as evidence of the maintenance activity.

6.3.3 ICT Equipment and Asset Management

6.3.3.1 The ICT Officer shall maintain an accurate and current inventory of ICT equipment and assets under ICT management.

6.3.3.2 Details of ICT equipment acquired shall be provided to ICT for verification, tagging and updating of the ICT asset inventory.

6.3.3.3 The ICT asset inventory shall capture, where applicable, the asset identification number, description, serial number, assigned user or location, status and warranty or support information.

6.3.3.4 ICT shall update the asset inventory when ICT equipment is transferred, replaced, decommissioned or disposed of in accordance with CEMASTEA asset-management procedures.

6.3.4 Lending of ICT Equipment

6.3.4.1 The Coordinator ICT shall receive an authorised request for ICT equipment lending sufficiently in advance to allow assessment, preparation and recording.

6.3.4.2 The ICT Officer shall record the equipment identifier, borrower, purpose, issue date, expected return date and condition of the equipment. The borrower shall acknowledge receipt and responsibility for the equipment while in their custody.

6.3.4.3 On return, the ICT Officer shall inspect the equipment, record its condition and any damage or loss, and confirm return.

6.3.4.4 Any unresolved loss or damage shall be reported and handled in accordance with CEMASTEA procedures.

6.3.5 Request for ICT Staff Services

6.3.5.1 Process owners shall submit routine ICT staff or event support requests at least three working days before the activity. Requests for major events requiring substantial ICT setup shall be submitted at least five working days in advance.

6.3.5.2 The Coordinator ICT shall acknowledge and assess the request within one working day, confirm ICT staff availability and communicate any requirements or limitations to the requesting process owner.

6.3.5.3 The Coordinator ICT shall assign ICT staff to the activity based on the approved request, required technical support and staff availability.

6.3.5.4 ICT staff shall provide the requested support and record any significant issues, additional requirements or follow-up actions arising from the activity.

6.3.6 Request for ICT Equipment Specifications

6.3.6.1 ICT receives a request from the process owner for technical specifications for ICT equipment, systems or services to be procured.

6.3.6.2 ICT shall provide technical specifications or feedback within one week, subject to the complexity of the requirement.

6.3.6.3 ICT shall participate in technical evaluation/verification, where assigned, to confirm that supplied ICT equipment or services meet approved specifications. Specifications shall consider security, compatibility, support, warranty, licensing, scalability, lifecycle, and data protection requirements.

6.4 ICT Incident Management

6.4.1 ICT incidents shall be reported to the Coordinator ICT or an ICT Officer through an authorised communication channel. Incidents may include service interruption, system or equipment failure, network disruption, suspected security incident, data loss or other ICT related disruption.

6.4.2 The Coordinator ICT shall ensure that reported incidents are recorded in the approved ICT Incident Register and assigned to an ICT Officer for assessment of their nature, impact and urgency.

6.4.3 The ICT Officer shall investigate the incident, take appropriate action to restore the affected ICT service or system, and record the actions taken and outcome in the incident record.

6.4.4 Where an incident cannot be resolved within the available ICT capability, the ICT Officer shall escalate it to the Coordinator ICT for further action, including referral to an authorised service provider where necessary.

6.4.5 Where an incident has a significant impact on ICT services, information, operations or security, the Coordinator ICT shall escalate the matter to the relevant management and other responsible parties in accordance with approved escalation requirements.

6.4.6 Security-related incidents shall be handled in accordance with 6.6 Information Security and any applicable incident response requirements.

6.4.7 Upon resolution, the ICT Officer shall update the incident record with the resolution, date of closure and any required follow-up action.

6.4.8 ICT shall periodically review incident records to identify recurring incidents, underlying causes and opportunities for improvement, and shall retain records of significant incidents and corrective actions.

6.5 User Account and Access Management

6.5.1 User accounts and access rights shall be created, modified and disabled based on an authorised request from the relevant process owner or authorised officer.

6.5.2 ICT shall assign user access rights based on the user's role and authorised requirements, applying the principle of least privilege.

6.5.3 ICT shall maintain records of user account creation, modification and deactivation, including the approval and access rights granted.

6.5.4 User accounts shall be disabled promptly when a user leaves CEMASTEA or no longer requires access to the relevant ICT service or system, based on notification from the responsible office.

6.5.5 ICT shall periodically review user accounts and access rights for critical ICT systems and take corrective action where unauthorised, excessive or outdated access is identified.

6.5.6 Privileged or administrative accounts shall be restricted to authorised ICT Officer and shall be managed separately from ordinary user accounts.

6.6 Information Security

6.6.1 ICT shall implement and maintain information security controls to protect CEMASTEA information and ICT resources against unauthorised access, disclosure, alteration, loss, destruction and disruption.

6.6.2 ICT shall ensure that ICT systems, devices and network resources are configured and maintained in accordance with approved security requirements.

6.6.3 ICT shall ensure that security updates, patches and approved security software are applied to ICT systems and devices in accordance with established maintenance requirements.

6.6.4 ICT shall record and escalate significant information security events and incidents in accordance with Section 6.4 ICT Incident Management.

6.6.5 ICT shall periodically review information security controls and implement corrective actions where weaknesses or gaps are identified.

6.7 Digital Platforms, Applications and Cloud Services

6.7.1 ICT shall maintain and support CEMASTEA digital platforms and applications used to support institutional operations, training, research and service delivery.

6.7.2 ICT shall monitor the availability and functionality of critical digital platforms and applications and address or escalate identified service disruptions in accordance with Section 6.4 ICT Incident Management.

6.7.3 ICT shall administer and support CEMASTEA cloud services provided through authorised service providers in accordance with approved requirements.

6.7.4 ICT shall ensure that administration and access to digital platforms, applications and cloud services are carried out in accordance with approved access and information security requirements.

6.7.5 ICT shall maintain records of significant technical support, service disruptions and actions taken in relation to critical digital platforms, applications and cloud services.

7.0 Key Performance Indicators

Key Performance Indicator	**Target**	**Frequency of monitoring & evaluation**	**Responsibility**
Website approved content published within two working days	≥95%	Quarterly	ICT Officers
Scheduled backups completed successfully	≥95%	Quarterly	ICT Officers
Planned backup restoration tests completed	100%	Quarterly	Coordinator ICT/ICTO
ICT support requests attended to within the approved service timeframe	≥90%	Quarterly	ICT Officers
Preventive maintenance completed as scheduled	≥95%	Annually	ICT Officers
ICT asset register updated for ICT	≥95%	Quarterly	ICT/ICT Officer

Key Performance Indicator	Target	Frequency of monitoring & evaluation	Responsibility
equipment acquired, transferred, replaced, decommissioned or disposed of			
Critical digital platforms and applications available and functional	≥95%	Quarterly	ICT

8.0 Retained Documentation

1. ICT service request and support records/job cards
2. ICT incident records and corrective-action records
3. ICT installation and configuration checklists
4. Preventive maintenance schedules, PM Forms and maintenance reports
5. ICT asset register and asset assignment/transfer records
6. ICT equipment lending and return records
7. Website content approval and publication records
8. Website availability and performance monitoring records
9. Backup schedules and backup monitoring/verification records
10. Backup restoration test records and corrective-action records
11. User access requests, approvals and access review records
12. Information security event and incident records
13. ICT equipment technical specifications and technical verification records
14. Digital platform, application and cloud service support and administration records
15. ICT KPI and performance reports
16. Other records required by the CEMASTEA Quality Manual, ICT Policy and applicable legal and regulatory requirements

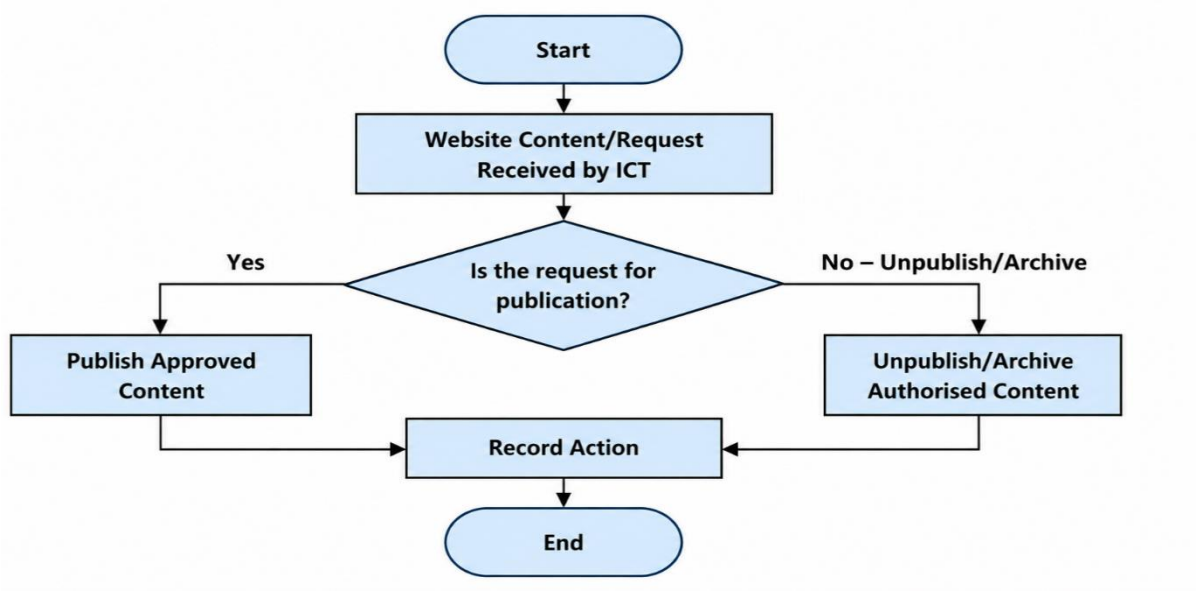
9.0 Annexes

9.1 Process interaction matrix

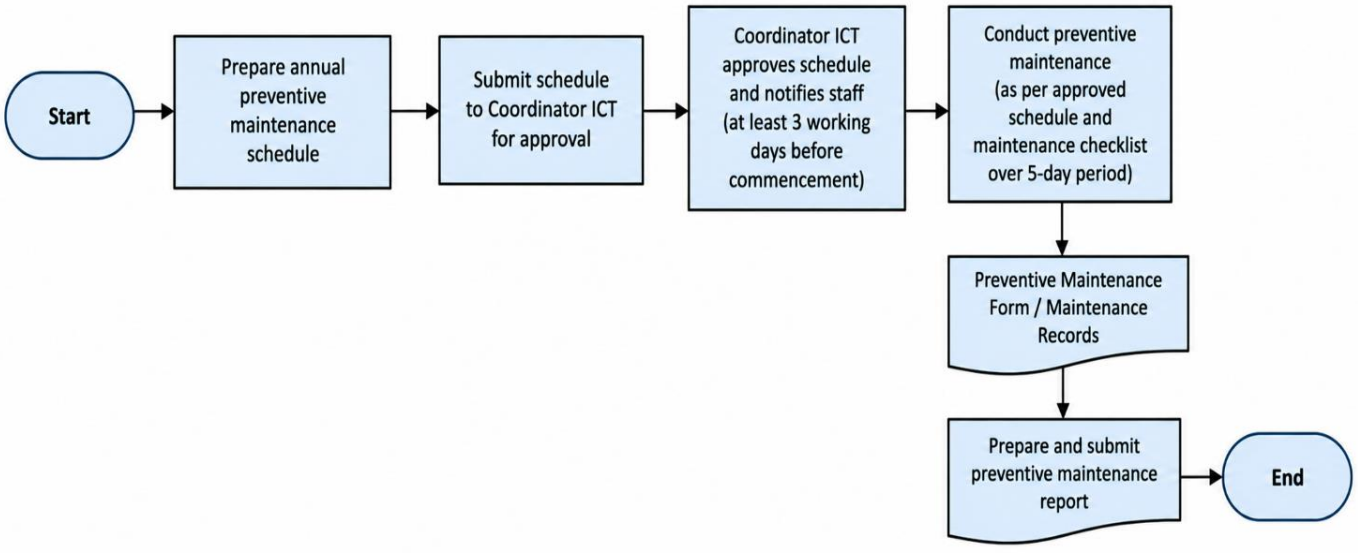
Suppliers	Inputs	Activities	Outputs	Customer
KENET	Membership subscription fee, contract for ICT services Domain name (cemastea.ac.ke), Payment for virtual server space.	Web hosting Hosting a learning management system	Working website Working learning management system	CEMASTEA
Google Kenya	Domain name (cemastea.ac.ke). Proof of being a registered public learning institution, a list of staff members using emails	Email hosting, online storage of docs (backup)	Working staff emails with cemastea.ac.ke domain suffix, Online Google Drive for backup of official documents	CEMASTEA Staff
Antivirus supplier	Contract, payment for the licence renewal fee	Antivirus administration and maintenance (updates, etc)	Protected data in client PCs	CEMASTEA Staff

9.2 ICT Processes Maps

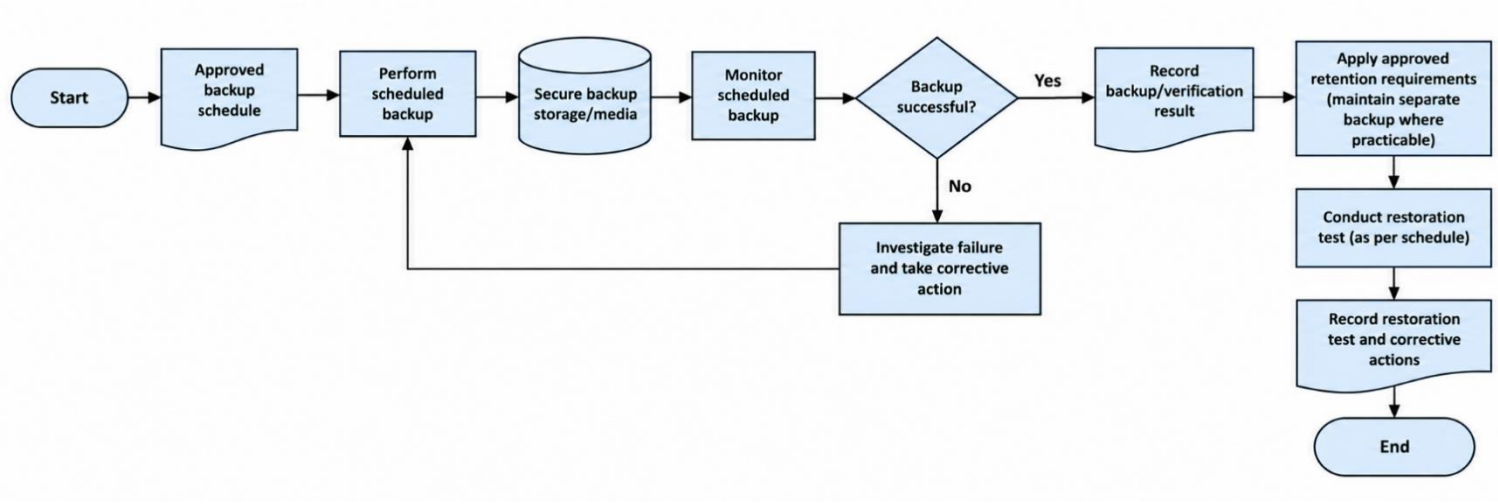
9.2.1 Website Management



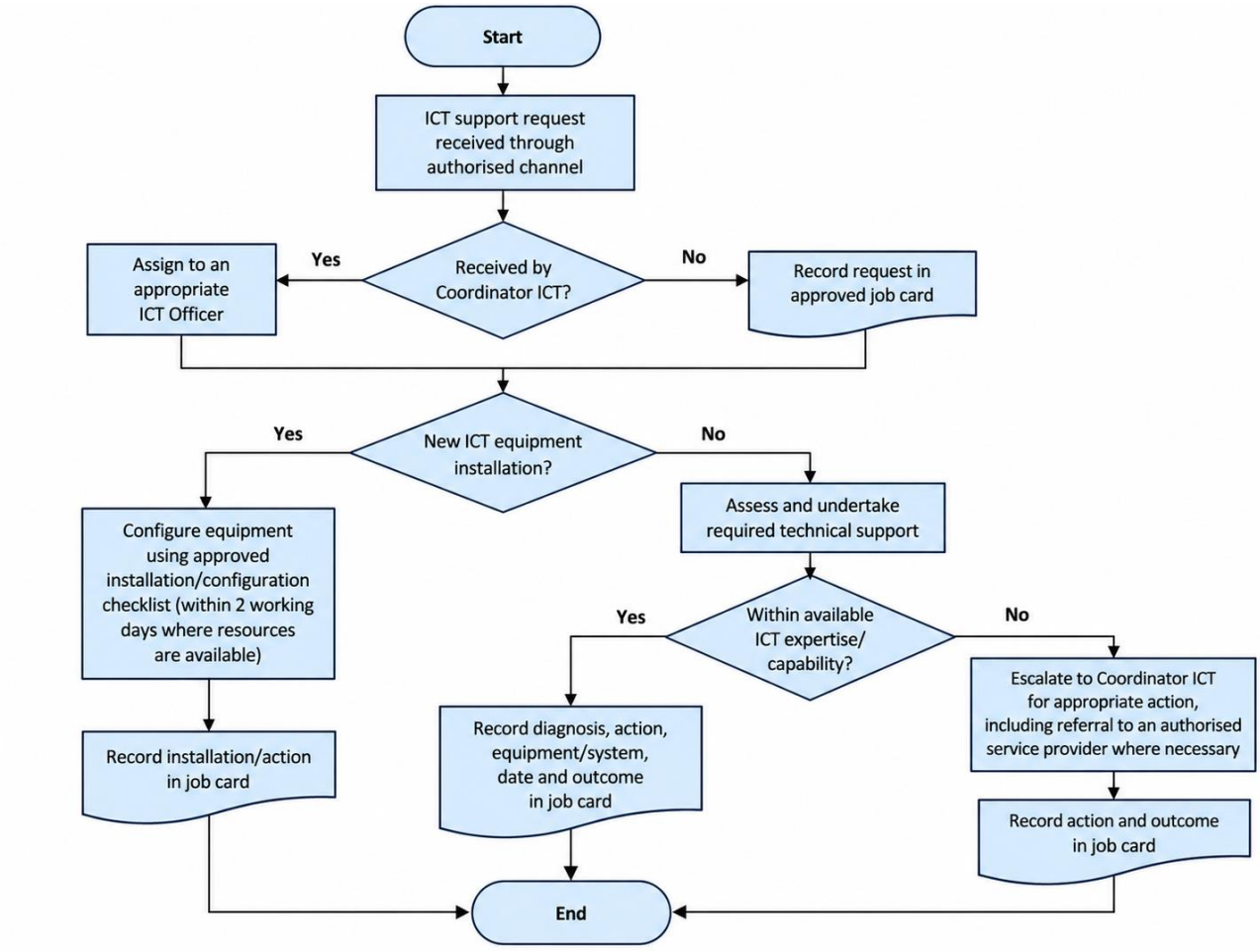
9.2.2 ICT Equipment and Infrastructure Maintenance



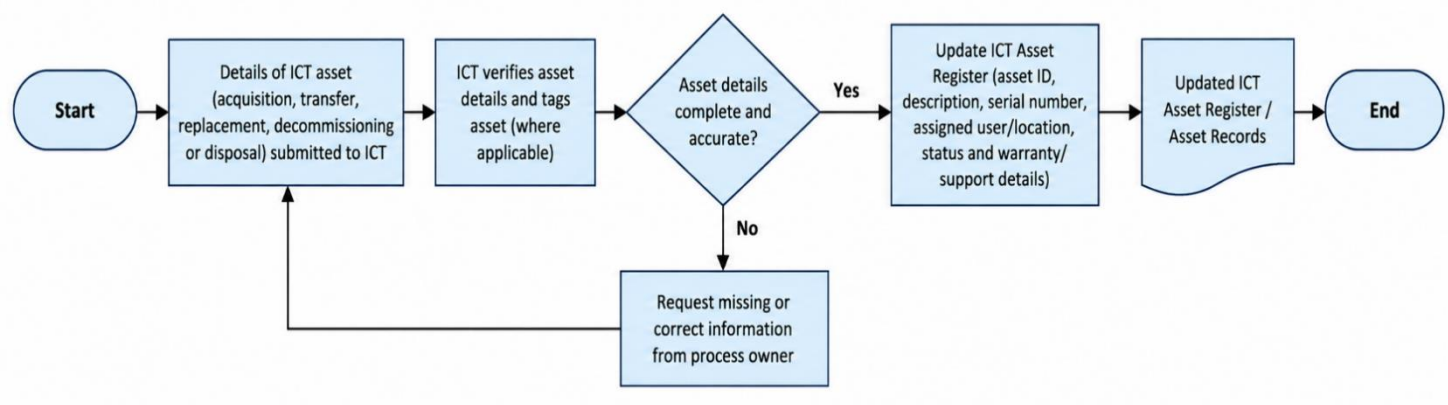
9.2.3 Data Backup and Security



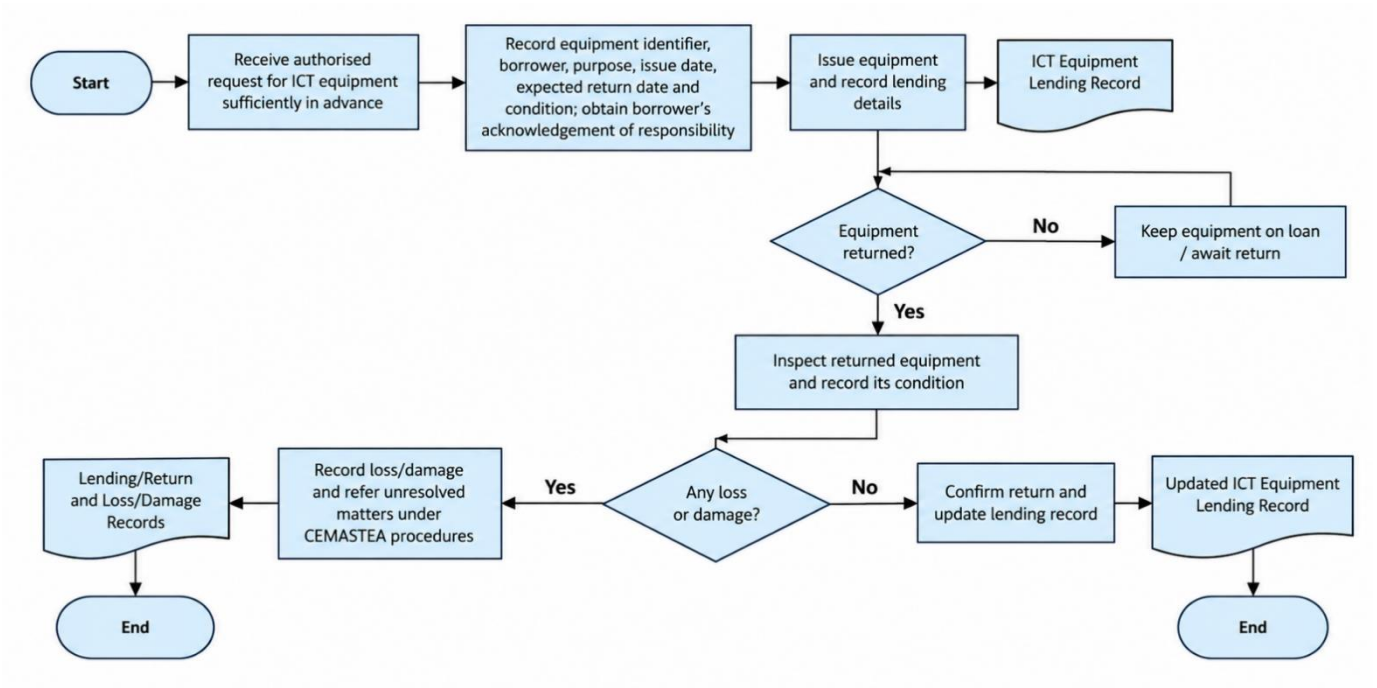
9.2.4 ICT Equipment Installation and Technical Support



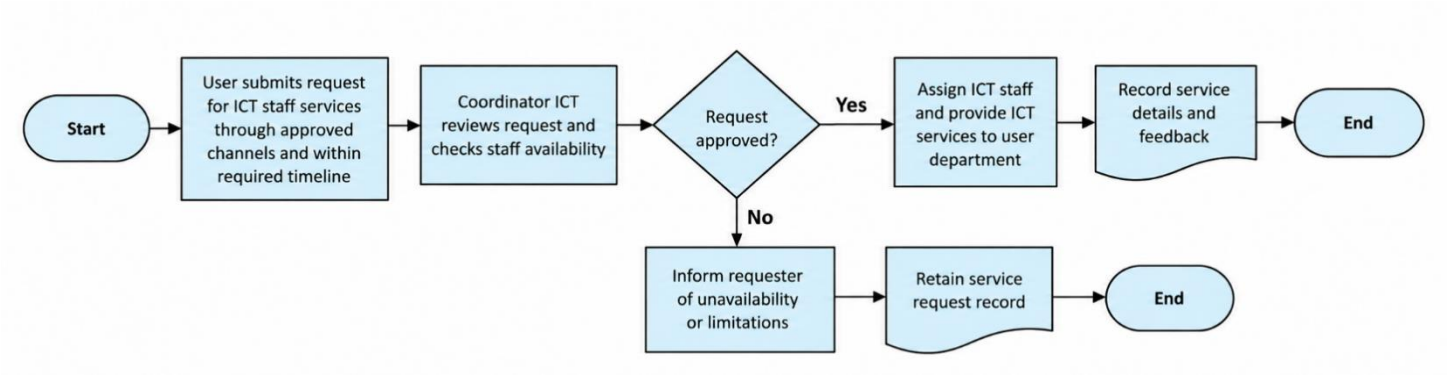
9.2.5 ICT Equipment and Asset Management



9.2.6 Lending of ICT Equipment



9.2.7 Request for ICT Staff Services



9.2.8 Request for ICT Equipment Specifications

