|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **APPROVAL** | **NAME** | **JOB TITLE/ ROLE** | **SIGNATURE** | **DATE** |
| Approved by | <<Name of AO>> | <<Title e.g. CEO>> | <<Signature>> | <<Date>> |

|  |  |
| --- | --- |
| **THE UNITED REPUBLIC OF TANZANIA** | |
| Applicable Public Institution  **<<insert the name of the Institution >>** | **Document Name**  ICT Development, Acquisition, Operation and Maintenance Procedures |
| **Document Number**  <<Insert your own document reference code>> |

**Table of Contents**

[1. INTRODUCTION 3](#_Toc142033329)

[**1.1.** **Overview** 3](#_Toc142033330)

[**1.2.** **Purpose** 3](#_Toc142033331)

[**1.3.** **Rationale** 3](#_Toc142033332)

[**1.4.** **Scope** 4](#_Toc142033333)

[2. THE PROCEDURES 5](#_Toc142033334)

[**2.1.** **Software Development Procedures** 5](#_Toc142033335)

[**2.1.1.** **Requirement Gathering Procedures** 5](#_Toc142033336)

[**2.1.2.** **Requirements Analysis Procedures** 6](#_Toc142033337)

[**2.1.3.** **Design Procedures** 6](#_Toc142033338)

[**2.1.4.** **Development Procedures** 7](#_Toc142033339)

[**2.1.5.** **Testing Procedures** 8](#_Toc142033340)

[**2.1.6.** **Deployment Procedures** 9](#_Toc142033341)

[**2.1.7.** **User Training Procedures** 10](#_Toc142033342)

[**2.1.8.** **Post Deployment Procedures** 10](#_Toc142033343)

[**2.2.** **ICT Acquisition Procedures** 10](#_Toc142033344)

[**2.2.1.** **Generic Acquisition Procedures** 10](#_Toc142033345)

[**2.2.2.** **Software Acquisition Procedures** 14](#_Toc142033346)

[**2.3.** **ICT Operation Procedures** 18](#_Toc142033347)

[**2.3.1.** **Start the Software** 18](#_Toc142033348)

[**2.3.2.** **System Monitoring** 18](#_Toc142033349)

[**2.3.3.** **Backup and Recovery** 18](#_Toc142033350)

[**2.3.4.** **Security Management** 19](#_Toc142033351)

[**2.3.5.** **User Access Management** 19](#_Toc142033352)

[**2.4.** **ICT Maintenance Procedures** 19](#_Toc142033353)

[**2.4.1.** **General Considerations** 19](#_Toc142033354)

[**2.4.2.** **Generic Maintenance Procedures** 21](#_Toc142033355)

[**2.4.3.** **Software Maintenance Procedures** 22](#_Toc142033356)

[**2.4.4.** **Patch Management Procedures** 25](#_Toc142033357)

[3. IMPLEMENTATION, ENFORCEMENT AND REVIEW 26](#_Toc142033358)

[4. GROSSARY AND ACRONYMS 27](#_Toc142033359)

[4.1. Glossary 27](#_Toc142033360)

[4.2. Acronyms 28](#_Toc142033361)

[5. RELATED DOCUMENTS 28](#_Toc142033362)

[6. DOCUMENT CONTROL 28](#_Toc142033363)

[APPENDICES 29](#_Toc142033364)

# INTRODUCTION

## **Overview**

Currently, ICT infrastructures and systems are the core business process supporters in many institutions and industries of the developing and developed countries. The e-Government Authorityfocuses on implementation of ICT initiatives in order to deliver valuable services to internal users. One of the goals of United Republic of Tanzania is using ICT as the tool for increasing productivity and best services to the users, so **<< include the name of the institution >>** has developed its procedures which every staff responsible for purchasing, developing or maintaining ICT equipment and systems should follow.

## **Purpose**

The purpose of this document is to describe the procedures, which will be used when performing ICT development, acquisitions, operations and maintenance in **<< include the name of the institution >>**. These procedures will focus on outlining specific steps that must be followed to ensure proper and consistent steps in delivering best ICT services. The application development, acquisition, operation and maintenance procedures document are directed at Directorate of Service Management, external contractors, consultants, and business partners which will be performing ICT development, acquisitions, operations and maintenance to **<< include the name of the institution >>**.

## **Rationale**

**<< include the name of the institution >>** uses ICT as the core organization support in order to meet its organizational goal and deliver best services to the nation. For **<< include the name of the institution >>** to meet its functional goals, it is required to follow proper channels during e-government implementation. This document outline procedures for ICT development, acquisitions, operations, and maintenance to be used.

These procedures will provide:

* + - 1. Adequate ICT development, acquisitions, operations and maintenance for all stages and processes; and
      2. A general measure for ensuring the ICT development, acquisitions, operations and maintenance procedures documents are complied with the available standards and guidelines.

## **Scope**

This document will be used by **<< include the name of the institution >>** as the guiding procedures in development, acquisition, operation, and maintenance of ICT initiatives.

# THE PROCEDURES

These considerations will be covered on both software development and acquisition procedures.

* + - 1. User department introduce/initiate and analyse formal requests/demands or directives to develop/acquire software;
      2. The ICT Unit submit software requests/demands or directives to the **<< include the name of the institution >>** ICT steering committee for further discussion, analysis, and approval; and
      3. The ICT Unit submit the approved ICT project concept note to e-GA for endorsement and technical advice through Government ICT Service Portal (GISP).

## **Software Development Procedures**

After clearance, here's a general outline of the steps involved in software development:

## **Requirement Gathering Procedures**

Requirements are gathered by involving all stakeholders at different business level and will be formally documented in terms of functional and non-functional requirements in Software Requirements Specification (SRS). The ICT Unit shall:

* + - 1. Perform business process analysis by involving AS IS and designing the TO BE processes;
      2. Perform business process mapping;
      3. Review existing systems;
      4. Describe data/system/process;
      5. Identify problem, areas/opportunities;
      6. Identify user needs/wants through interviews;
      7. Identify legislative/contractual/security/privacy/access requirement;
      8. Establish and document business/application requirements; and
      9. Prepare business requirement and SRS documents.

## **Requirements Analysis Procedures**

ICT Unit shall analyze requirements to understand the scope, functionality, and constraints of the software system by performing the following;

* + - 1. Describe functions and capabilities of the system;
      2. Describe business, organizational and user requirements;
      3. Describe safety, security, information, privacy, interface, operations, and maintenance requirements;
      4. Ensure presence of documentations such as systems analysis document, application requirements and specification, interface requirement/specification, operational/support requirement, system/subsystem specification and software requirement specification; and
      5. Formal sign off by user department upon successful completion of requirement gathering, review and documentation.

## **Design Procedures**

At this stage, the requirements shall be transformed into an architecture that describes the data structures, interface representations and application components of the system. The detailed design translates the requirements into a representation of the system software that can be assessed for quality assurance before coding begins. At the design stage, ICT Unit shall:

* + - 1. Design system flow, develop data model, create physical data model and develop data dictionary;
      2. Design screens, screen navigation, data entry screens, inquiry screens, help screens, online documentation, Design reports, Forms, Report distribution system, User generated reports, Design Patterns and Existing system modifications;
      3. Conduct design walkthrough;
      4. Establish and document a top-level architecture of the system;
      5. Identify the architecture hardware, application/software, and manual operations;
      6. Evaluate and document the system architecture and requirements for the application/software;
      7. Develop and document a top-level design for the database.
      8. Develop and document general interface to the application and interface between the application components of the system;
      9. Develop and document preliminary versions of user documentation, test requirements and the schedule for application integration;
      10. Develop and document a detailed design for each application module/component/service of the application. These should be refined into lower levels containing application units that can be coded, compiled, and tested;
      11. Ensure that all application requirements are allocated for the application components to application units;
      12. Evaluate and document the application detailed design and test requirements; and
      13. Ensure presence of documentation such as architecture design, system/subsystem design documentation (SDD), application architecture and design, interface design, database design and screen/report design.

## **Development Procedures**

These procedures shall involve transforming user and design requirements into actual system using agreed programming techniques. At the development stage, ICT Unit shall:

* + - 1. Prepare development and test environments;
      2. Review and analyse architecture/design documentation and construct/code to design specifications;
      3. Perform the activities/tasks related to coding using the agreed development framework;
      4. Develop test cases, unit test programs and secure code;
      5. Develop application/software documentation, Users guide, Turnover documentation and training materials;
      6. Develop and document application unit, database, test procedures and data for testing each application unit and database;
      7. Test each application unit and database ensuring that it satisfies its requirements. The test results must be documented;
      8. Evaluate and document application code and test results;
      9. Develop an integration plan to integrate the application units and components into the application;
      10. Integrate the application units and components and test if the aggregates are developed in accordance with the integration plan;
      11. Develop and document, for each requirement of the application, a set of tests, test criteria (inputs, outputs, test cases, acceptable criteria) and test procedures; and
      12. Provide documentations such as application code, application documentation, user manual and operator manual.

## **Testing Procedures**

The system shall undergo different types of testing to ensure that the solution meets quality, security, performance, and user requirements as described in the requirements documents. The test that shall be done shall include unit testing, functional testing, software performance and System Integration Testing (SIT), Security Testing and User Acceptance Testing (UAT). It must be ensured that the implementation of each application requirement is tested for compliance. At testing stage, the ICT Unit shall:

* + - 1. Develop a comprehensive test plan based on the requirements and design;
      2. Prepare test environment;
      3. Prepare test cases, scenarios and scripts;
      4. Perform unit test, functional test, integration test, run parallel test, stress test and document results;
      5. Perform security test against the security requirements such as penetration test and vulnerability assessment to ensure security controls are implemented such that the software can generate and store audit logs, has strong authentication and authorization, well implemented user management and session management;
      6. Perform UAT and document results. UAT shall involve users in testing of the system in accordance with the requirements specification documented during requirement gathering stage and should attain at least 75% acceptance rate;
      7. Execute test cases to verify that the software functions correctly and meets the specified requirements;
      8. Perform regression testing to ensure that changes or fixes do not introduce new issues;
      9. Issue production readiness recommendation after the system has passed the security test and user acceptance test; and
      10. Provide the minimum set of documentation such as application test plan, testing scripts/scenarios, application testing procedures, software test reports, security test report, defect/error reports and documented changes to the system.

## **Deployment Procedures**

These procedures shall involve deployment of the developed system into production environment after UAT sign-off. Deployment stage ensures that all pre-requisite activities in other previous stages have been successfully completed. At deployment stage, the ICT Unit shall:

* + - 1. Develop a plan to install the application product in the target environment as designated;
      2. Prepare all resources and information necessary to install the application product such as production environment;
      3. Prepare the software/application for deployment, including packaging, configuration and specific software installation instructions;
      4. Execute the deployment process, considering hardware, software and infrastructure requirements and ensure that the application code and databases initialize, execute and terminate;
      5. Conduct database setup and necessary data migration;
      6. Document the installation events and results;
      7. Complete and hand-over the application product to user’s department; and
      8. Prepare application user and operator manual.

## **User Training Procedures**

Training is an important stage of the lifecycle that addresses aspect of solution stability. The training shall cover at least all user department of the system such as end users and administrators. At training stage, the ICT Unit shall:

* + - 1. Provide user training and support materials to facilitate a smooth transition to the new software system;
      2. Provide hands-on system training sessions to users using test environments; and
      3. Provide application user manual, operator manual and implementation document.

## **Post Deployment Procedures**

Once the system is operational, it shall be monitored for continued performance in accordance with user requirements. Any identified gaps shall be fixed in accordance with the change management procedure in place. Moreover, ICT Unit shall

* + - 1. Measure the system/application operating performance and efficiency and ensure Return on Investment (ROI) is attained;
      2. Perform security monitoring by employing relevant security monitoring tools;
      3. Perform a post implementation review to support continuous improvement of the implemented application system;
      4. Lessons learned and improvement plans for future projects are documented; and
      5. Results or report of a post-implementation review of the application development system should be documented and retained for periodic reviews.

## **ICT Acquisition Procedures**

Procurement unit shall not procure any ICT System, Service, Equipment, Consumable or Accessory if the request is not originating from ICT **<<section/unit/department>>.**

## **Generic Acquisition Procedures**

Before procurement of any ICT System/Equipment, **<< include the name of the institution >>** should define the ICT requirements based on the operations. The following procedures shall be adhered to:

* + - 1. Define the problem to be solved;
      2. Define the goals to be achieved in relation to the operation goals;
      3. Identify the system process to be accomplished;
      4. Identify user expectations;
      5. Identify the system deliverables;
      6. Incorporate information about the system inputs, information being processed by the system and the information expected out of the system;
      7. Identify specifications for equipment acquisition;
      8. Identify system requirements, this can be gathered through interviews, questionnaires, existing system derivation, benchmarking with related system, prototyping and Rapid Application Development;
      9. All ICT acquisitions made by **<< include the name of the institution >>** should follow the Tanzania Public Procurement procedures;
      10. ICT Officer shall be a member of an Inspection Committee when inspecting ICT System/ Equipment;
      11. All ICT acquisitions must be approved by **<< include the name of the institution >>**’s accounting officer; and
      12. Due care must be taken to ensure that the required technical and software specifications are clearly translated to suppliers when acquiring ICT equipment and with reference to the Government Hardware and Software Standards and Specifications.
      13. **Due Diligence**
      14. Prior to appointing an external service provider / vendor / supplier/ distributor for ICT procurement or services, reasonable due diligence must be performed. This includes a review of their ability to provide the proposed service;
      15. Clearly understand and categorize all third-party providers;
      16. **<< include the name of the institution >>** will use questionnaire in ***Appendix I*** as part of the procedures on categorizing the third-party providers; and
      17. All third-party providers must be screened to identify whether:

1. They are liable to financial sanctions from the government of Tanzania;
2. Directors or related parties are not being sued for money laundering offences;
3. To identify any possible conflict, independence issue and commercial sensitivities; and
4. The due diligence checklist in Appendix II can be used for reference purposes.
   * + 1. **Contractual Agreements**

Arrangements involving third party access to **<< include the name of the institution >>** information processing facilities and data should be based on formal agreements or contracts containing, or referring to, all of the relevant security requirements to ensure compliance with the **<< include the name of the institution >>** security policies, regulations, standards and guidelines including the risks, security controls and procedures for information systems, networks and/or desktop environments between the parties. The contracts should contain at least the following clauses to protect **<< include the name of the institution >>** information:

* + - 1. Description of the information to be provided or accessed and methods of providing or accessing the information;
      2. Legal and regulatory requirements, including data protection, intellectual property rights and copyright, and a description of how it will be ensured that they are met;
      3. Obligation of each contractual party to implement an agreed set of controls including access control, performance review, monitoring, reporting and auditing;
      4. **<< include the name of the institution >>**’s ICT Acceptable Use Policy;
      5. Either select explicit list of supplier’s personnel authorized to access or receive the **<< include the name of the institution >>**’s information/procedures/conditions for authorization, and removal of authorization;
      6. **<< include the name of the institution >>** policies relevant to the specific contract;
      7. Relevant regulations for sub-contracting, including the controls that need to be implemented; and
      8. Relevant agreement partners, including a contact person for the resolution of issues:

1. Right to audit the supplier processes and controls related to the agreement;
2. Supplier’s obligation to periodically deliver an independent report on the adherence to the contractual terms and agreement on timely correction of relevant issues raised in the report; and
3. Supplier’s obligations to comply with the **<< include the name of the institution >>**’s security requirements.
   * + 1. **Non-Disclosure Agreement**
       2. Ensure that an authorized signatory at the third-party organization agrees in writing that, under no circumstances, will they disclose any data, or any information regarding hardware, software/application or other programs to any person other than authorized **<< include the name of the institution >>** personnel without the prior written consent of a designated employee of **<< include the name of the institution >>** duly authorized to give such consent; and
       3. Supplier/vendor and Service Provider should fill in a Non-Disclosure Agreement.

## **Software Acquisition Procedures**

Software acquisition refers to all stages from buying, introducing, applying, adopting and adapting a software solution. This option should be considered after analyzing and agreeing that **<< include the name of the institution >>** internal ICT team cannot develop the software in house and have failed to obtain assistance from other public institutions. Software acquisition considers the “Off the Shelves” software solution, “Software as a Service (SaaS)” and outsourced software development and internal ICT team should fully participate on implementations. **<< include the name of the institution >>** must adhere to the following procedures when acquiring software/application.

* + - 1. **Identifying the Application Requirements**

Application requirements can be gathered through interviews, questionnaires, existing system derivation and benchmarking with related application. The output of this stage is a decision to go with specific application, timetable, budget and application expectations. The below are requirements gathering procedures:

* + - 1. Involve relevant stakeholders to gather their inputs and ensure all requirements are considered;
      2. Assess the **<< include the name of the institution >>**'s needs then determine the specific requirements for the software solution if it is an “Off the Shelves” software solution, “Software as a Service (SaaS)” or outsourced software development;
      3. Identify the functional and non-functional requirements that the software must fulfil;
      4. Conduct a feasibility analysis considering risk, security, economical, technical, operational, legal and contractual aspects; and
      5. Document the software requirements, including desired features, performance criteria, scalability, interoperability, and security.
      6. **Conduct Market Research**
      7. Research the market to identify potential software vendors or solutions;
      8. Evaluate available software options that align with the defined requirements;
      9. Gather information about vendors, their reputation, and customer reviews;
      10. Explore industry reports, online resources and user communities for insights;
      11. Develop a Request for Information (RFI) document outlining the **<< include the name of the institution >>**'s needs and requirements;
      12. Send the RFI to the potential vendors to gather more detailed information about their software solutions; and
      13. Evaluate vendor responses to determine if their solutions align with **<< include the name of the institution >>**'s requirements and assess vendor capability of providing maintenance and support.
      14. **Perform Procurement Procedures**
      15. Issue the software solution specifications to the procurement management unit for further actions; and
      16. Define evaluation criteria for assessing the proposals, such as functionality, scalability, support, and cost.
      17. **Proposal Evaluation and Vendor Selection.**
      18. Evaluate the received bids based on the defined evaluation criteria;
      19. Review each proposal for compliance with the requirements, feasibility, and alignment with **<< include the name of the institution >>**’s objectives;
      20. Consider vendors based on their proposal quality, credibility, and ability to meet the **<< include the name of the institution >>**’s needs;
      21. Conduct interviews, demonstrations or presentations with prospect vendors to assess their software and capabilities; and
      22. Select the vendor that best meets the **<< include the name of the institution >>**’s requirements, budget and long-term goals.
      23. **Contract Negotiation and Review**
      24. Initiate contract negotiations with the selected vendor;
      25. Review and analyse the proposed contract, paying attention to terms and conditions, licensing, customer support and maintenance;
      26. Engage legal and procurement units to ensure compliance with **<< include the name of the institution >>** policies and legal requirements; and
      27. Negotiate and finalize the contract terms, including pricing, open-source codes ownership, knowledge transfer, payment schedules and service level agreements (SLAs).
      28. **Software Demo Testing (if Applicable)**
      29. Request a trial version or access to a test environment to test the software; and
      30. Perform thorough testing of the software to validate its functionality, user experience and compatibility with the **<< include the name of the institution >>**’s infrastructure.
      31. **Implementation**

Consider these procedures if it is an outsourced software development only.

* + - 1. Develop an implementation plan, including milestones and deliverables, timelines and resource allocation;
      2. Define roles and responsibilities for the implementation team members;
      3. Determine data migration requirements and plan for system integration, if necessary; and
      4. Develop a communication plan to inform stakeholders about the upcoming software implementation.
      5. **Software Testing**
      6. Involve end-users and relevant stakeholders in the testing process to gather feedback and evaluate user experience and satisfaction;
      7. Perform security test such as penetration and vulnerability assessments to ensure the security is implemented such as the software can generate and store audit logs, has strong authentication and authorization, well implemented user and session management; and
      8. Evaluate the software against predefined acceptance criteria and conduct a risk assessment.
      9. **Software Deployment and Training**

After the completion of software testing, respective software vendor/supplier in cooperation with **<< include the name of the institution >>** technical team and users’ department will perform the below software deployment and training procedures: -

* + - 1. Install and configure the software in the production environment;
      2. Perform necessary data migration or integration tasks;
      3. Provide training sessions to users’ department and administrators to ensure they can effectively use and manage the software/system; and
      4. Develop user documentation and support materials to assist users during the transition.
      5. **Post-Implementation Support**
      6. Monitor the software's performance and gather feedback from end-users; and
      7. Address any raised issues or bugs that arise during the initial deployment with the system vendor/supplier.

## **ICT Operation Procedures**

ICT operation procedures are step-by-step procedures that outline the process for operating or using a particular software application in compliance with the standards and guideline for Development, Acquisition, Operation and Maintenance for e-Government Application. Below procedures will be used by **<< include the name of the institution >>** in software operation to ensure consistency, efficiency, and effectiveness.

## **Start the Software**

* + - 1. Launch the appropriate startup scripts or executing the necessary commands or instructions; and
      2. Verify if the software has started successfully and is running without errors.

## **System Monitoring**

* + - 1. Monitor the system to track the performance, availability and health of the software;
      2. Monitor system resources such as CPU usage, memory utilization, and disk space;
      3. Respond on alerts or notifications for critical events or abnormal system behaviour; and
      4. Periodically review system logs and error messages to address performance-related issues.

## **Backup and Recovery**

* + - 1. Perform proper backup mechanism while adhering to the **<< include the name of the institution >>** backup plan and DRP;
      2. Test the backup and recovery processes to ensure data integrity and system recoverability; and
      3. Store backups in secure locations and maintain a proper retention policy in accordance with the **<< include the name of the institution >>** DRP.

## **Security Management**

* + - 1. Regularly review and update security configurations, including firewall rules, access controls, and encryption settings;
      2. Conduct security audits or vulnerability assessments to identify and address potential security risks;
      3. Stay up to date with security best practices and industry standards to ensure the software remains secure; and
      4. Document common issues, solutions and troubleshooting steps to facilitate efficient problem resolution.

## **User Access Management**

These procedures will be done by System Administrator from **<< include the name of the institution >>** internal ICT team. The procedures will be performed after users’ access forms have been well filled and approved by appropriate personnel. Below procedures will follow:

* + - 1. Create user accounts;
      2. Assign appropriate permissions and privileges; and
      3. Regularly review and update user access rights based on changes in roles or responsibilities.

## **ICT Maintenance Procedures**

ICT maintenance procedures are essential for ensuring the consistency, reliability, performance, and security of ICT systems in the **<< include the name of the institution >>** while adhering to the change management procedures. Here is an outline of **<< include the name of the institution >>** ICT maintenance procedures:

## **General Considerations**

These general maintenance considerations cover on both hardware and software/systems:

* + - 1. **Performance of Maintenance by Third Party on Internal Systems**

Access by a third party to perform systems maintenance on internal systems and infrastructures, such as a contractor for temporary access to maintain a system or device could lead to exposure or loss of confidentialinformation. Due care will be taken to ensure that the following controls are followed to minimize risks of unauthorized access and disclosure of information: -

* + - 1. SLA between **<< include the name of the institution >>** and vendor should be in place which will ensure both sides having a common understanding of the requirements, an SLA will pull together information on all of the contracted services and their agreed-upon expected reliability into a single document.
      2. Access by a third party to perform systems maintenance must be restricted to authorized third party staff members only and access levels will remain under control of **<< include the name of the institution >>**;
      3. Periodically change the passwords used by the third party. In addition, the passwords must be changed whenever there is a change in third party personnel;
      4. Establish a mechanism which will require a third party to notify the **<< include the name of the institution >>** on personnel changes;
      5. If the administrator/accounting officer account and password are provided to a third party for problem resolution, change the password immediately upon resolution of the problem; and
      6. Establish a preventive maintenance plan stating the accountability, frequency of maintenance, mode of maintenance performance as well as maintenance report preparation.
      7. **Monitoring and Review of Supplier Services**

**<< include the name of the institution >>** shall monitor and review the supplier services to ensure that, the terms and conditions of the agreements are being adhered to and that any issues arising are managed properly. **<< include the name of the institution >>** shall review the supplier service performance by including at least the following:

* + - 1. Monitor service performance levels to verify adherence to the agreements;
      2. Review service reports produced by the supplier and arrange regular progress meetings as pre-described by the agreements;
      3. Conduct audits of suppliers, in conjunction with review of independent auditor’s reports, if available, and follow-up on issues identified.
      4. Resolve and manage any identified problems; and
      5. Ensure that the supplier maintains sufficient service capability together with workable plans designed to ensure that agreed service continuity levels are maintained following major service failures or disaster.

## **Generic Maintenance Procedures**

These considerations cover on general ICT maintenance procedures including both hardware and software/systems.

* + - 1. **Preventive Maintenance Procedures**

ICT preventive maintenance procedures are proactive measures taken to prevent issues, minimize downtime, and optimize the performance and lifespan of ICT systems and infrastructure. These procedures involve regular inspections, monitoring, and scheduled activities to identify and address potential problems before they cause disruptions or failures. Here is an overview of ICT preventive maintenance procedures on both hardware and software systems:

* + - 1. Conduct semi-annual inspections of hardware components, such as servers, routers, switches, storage devices, computers and peripherals, to check for any signs of damage, overheating, loose connections, or dust accumulation;
      2. Semi-annually clean and remove dust from computer systems, cooling fans, vents, and other hardware components;
      3. Verify and organize cable connections to ensure proper functioning, minimize cable stress, and prevent accidental disconnections;
      4. Monthly check and apply software patches, updates, and security fixes provided by vendors to address known vulnerabilities and ensure system stability and security;
      5. Maintain an inventory of software licenses, track license expirations, and ensure compliance with licensing agreements to avoid legal and operational risks;
      6. Monitor the performance of software applications, databases, and services to identify any performance degradation or anomalies that could impact system functionality; and
      7. After conducting preventive maintenance, ensure reports are prepared.
      8. **Security Maintenance Procedures**
      9. Quarterly update security measures, such as firewalls, intrusion detection systems, antivirus software, and access controls, to protect against unauthorized access, data breaches, and cyber threats; and
      10. Conduct quarterly vulnerability assessments and penetration testing to identify and address security vulnerabilities and ensure all results are documented.

## **Software Maintenance Procedures**

Software maintenance procedures generally involve a series of steps to ensure that software remains functional, secure, and up to date over its lifecycle. The appointed maintenance leader should monitor the progress of the implementation as well as the use of allocated resources. Here's a step-by-step guide to software maintenance procedures:

* + - 1. **Identify the Need for Maintenance**
      2. This can be triggered by maintenance schedule, bug reports, user feedback, changing requirements, security vulnerabilities, or performance issues.
      3. **Review the Maintenance Request**
      4. This will be done by the maintenance team. The maintenance review will consider terms of their needs, urgency, benefits, etc;
      5. Assess the priority of the change requests if necessary;
      6. Appropriately fill the change request forms and submit for approval;
      7. ICT steering committee approve the maintenance request where the accepted change request will be passed to next stage for impact analysis; and
      8. Perform thorough requirements gathering, analysis and documentation for the expected system changes while involving relevant stakeholders.
      9. **Perform Impact Analysis**
      10. Analyse and document the impact of the maintenance activities on the software system;
      11. Identify potential risks, dependencies and implications of making changes; and
      12. Estimate required resources in terms of software and hardware, manpower, cost and schedule.
      13. **Planning the Maintenance Activities**
      14. Plan the maintenance activities;
      15. Determine the scope of the maintenance; and
      16. Allocate resources and create a schedule while considering factors like urgency, impact on users, and available resources.
      17. **Backup and Version Control**
      18. Create a backup of the existing software in order to ensure that you can revert to a known working state if something goes wrong; and
      19. Use version control systems to track changes and manage different versions of the software.
      20. **Perform Software Maintenance**
      21. Conduct detailed design for the change request. The impact analysis result and resources estimation produced will be used as input for the design work;
      22. Identify the affected software modules based on the analysis results;
      23. Identify the software modules to be modified;
      24. Modify the system documentation to reflect the new design;
      25. Develop a test plan and implementation plan which should clearly state how the testing, implementation and delivery of the changes are to be accomplished with a minimal impact to current users;
      26. Build/code the approved change into the application systems according to the new design;
      27. After the modification are coded perform unit-test to the modified codes at appropriate interval during coding;
      28. Integrate and test the modified part with the system;
      29. Assess the effect of the modification on the existing system and all unacceptable impacts should be noted;
      30. Any large discrepancy in the schedule and resource utilization should be reported to the management team for consideration and should ensure that the changes align with user requirements and have been properly reviewed;
      31. Address the software update security vulnerabilities;
      32. Keep track of security patches and updates from relevant sources; and
      33. Apply security fixes promptly to mitigate potential risks.
      34. **Test Implemented Change**

Once changes have been made to the software modules:

* + - 1. Perform thoroughly test to ensure the change is correct and does not introduce other errors to existing functions;
      2. Where appropriate perform UAT by the user representative to ensure that the implemented change is satisfactory; and
      3. Perform functional testing and integration testing to verify that existing features work as intended and new changes do not introduce unexpected issues.
      4. **Deliver the Modified Software**
      5. Document the delivery procedures to ensure minimal impact on the user and the system due to unforeseen software failures not detected during testing; and
      6. Deploy the updated software to the production environment, follow established deployment processes to minimize disruptions and ensure a smooth transition.
      7. **User Training and Support**
      8. Provide necessary training and support to users for using the updated software;
      9. Communicate the changes, new features, and any known issues; and
      10. Address user queries and issues promptly to ensure a positive user experience.
      11. **Document the Changes**
      12. Develop a thorough documentation of the maintenance activities performed, including the changes made, reasons for the changes, and any issues encountered.
      13. **Monitor and Evaluate**
      14. Continuously monitor the software in the production environment;
      15. Monitor performance and error logs to identify any new issues or areas for improvement; and
      16. Collect feedback from users to understand their experience and identify potential enhancements.

## **Patch Management Procedures**

These procedures involve the systematic process of identifying, evaluating, testing, and deploying patches or updates provided by software vendors to address vulnerabilities, fix bugs, and improve software functionality. Here is an outline of patch management procedures: -

* + - 1. **Patch Identification**
      2. Regularly monitor software vendors' websites, security advisories, mailing lists, and other trusted sources to stay updated on the latest patches and updates;
      3. Conduct quarterly vulnerability assessments to identify potential security vulnerabilities within **<< include the name of the institution >>**’s systems; and
      4. Assess the severity and impact of identified vulnerabilities to prioritize patching based on the risk they pose to the **<< include the name of the institution >>**’s systems and data.
      5. **Patch Evaluation and Testing**

Perform patch testing and evaluation by using test environment that mirrors the production environment.

* + - 1. Test and evaluate the impact of patches on system configurations and software dependencies; and
      2. Perform functional and regression testing to ensure that the patch does not introduce new issues or affect system performance, functionality, or user experience.
      3. **Patch Deployment**
      4. Develop a patch deployment schedule that minimizes disruptions and ensures that critical systems receive priority attention while considering maintenance schedule and user impact;
      5. Perform the patch deployment process using deployment tool to streamline the distribution and installation of patches across the intended systems;
      6. Perform post-deployment to confirm that the patches have been successfully applied and address the identified vulnerabilities or issues; and
      7. Implement systems or tools to monitor and track patch compliance, ensuring that all systems and software components have the latest security patches installed.
      8. **Documentation**
      9. Document the patch management process, including the rationale for patch prioritization, testing results, deployment schedules, and any incidents or exceptions encountered during the process; and
      10. Develop and maintain a comprehensive inventory of all applied patches, including information on the software, version, patch level, deployment date, and any related notes or observations.

# IMPLEMENTATION, ENFORCEMENT AND REVIEW

* 1. Effective upon being reviewed by **<< include the name of the institution >>** Board of Directors and signed by the Board chairperson on its first page;
  2. Subjected to review at least once every three years or whenever necessary changes are needed and
  3. Consistently complied with, any exceptions to its application must duly be authorized by the Board chairman.

# GROSSARY AND ACRONYMS

# Glossary

|  |  |
| --- | --- |
| **ICT Development, Acquisition, Operation and Maintenance Procedures** | There are systematic and organized procedures involved in managing various aspects of an organization’s ICT infrastructure, software applications and e-services. These procedures ensure that ICT resources are developed, acquired, operated and maintained efficiently and effectively to support the organization’s goals and objectives. |
| **ICT Development Procedures** | These procedures focus on creating new software applications, systems or digital solutions to meet specific business requirements. |
| **ICT Acquisition Procedures** | These procedures involve the process of procuring hardware, software and services from external vendors to fulfil specific organizational needs. |
| **ICT Operation Procedures** | These procedures focus on the day-to-day management and monitoring of the organization’s ICT infrastructure and services. |
| **ICT Maintenance Procedures** | These procedures involve the ongoing upkeep, updates and improvements of ICT resources to keep them in optimal working condition. |

# Acronyms

|  |  |
| --- | --- |
| **Term** | **Description** |
| **ICT** | Information & Communication Technology |
| **RFB** | Request for Bid |
| **RFI** | Request for Information |
| **ROI** | Return on Investment |
| **SDD** | Software Design Documentation |
| **SIT** | System Integration Testing |
| **SLA** | Service Level Agreements |
| **SRS** | Software Requirement Specification |
| **UAT** | User Acceptance Test |

# RELATED DOCUMENTS

* + - 1. ICT Policy;
      2. ICT Project Management Procedures
      3. ICT Security Policy;
      4. e-Government Application Architecture – Standards and Technical Guidelines;
      5. Guidelines for Development, Acquisition, Operation and Maintenance of e-Government Applications;
      6. Standards for Development, Acquisition, Operation and Maintenance of e-Government Applications; and
      7. Quality Assurance Compliance Guidelines for e-Government Applications.

# DOCUMENT CONTROL

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Name | Comment | Date |
| Ver. 1.0 | Responsible Section | <<What has been done>> | <<Date>> |

# APPENDICES

***Appendix I***

**Questionnaire for Third party vendors**

**The Third Party’s information:**

Third Party’s Name: ­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Principal Contact: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Address: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Mobile number: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

E-mail address: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**The Third party’s organization:**

Full legal name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Operational address: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Phone number: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Fax number: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Website: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Type of business (Check one):**

* Individual
* Corporation
* Partnership

**The Third Party’s Operations**

Q1. What are the services being provided by the third party?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Q2. List previous or current relationships with our organization showing the period when such relationship was active.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

***Appendix II***

**Due Diligence Checklist**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Due Diligence Questions#** | **Yes** | **No** | **N/A** | **Comments** |
| 1. How did we come to know of the third party? |  |  |  |  |
| 1. What other parties were considered as candidates? |  |  |  |  |
| 1. Why was this third party chosen? |  |  |  |  |
| 1. List any previous or current relationships with the Authorityshowing the period when such relationship was active. |  |  |  |  |
| 1. Describe the nature of the proposed relationship and the services to be provided by the third party. |  |  |  |  |
| 1. From the screening performed on the third parties, have any issues been identified that raise concern about the third party. |  |  |  |  |
| 1. Do they have a security policy? |  |  |  |  |
| 1. Do they utilize subcontractors? |  |  |  |  |
| If Yes, are there controls to ensure subcontractors meet appropriate Authoritysecurity requirements |  |  |  |  |
| 1. Do they have a complete accountability of the following asset types: information, software, physical and services? |  |  |  |  |
| 1. Does the supplier have policies and procedures for performing background checks for personnel if the latter will be administering systems which have access to Authorityinformation? |  |  |  |  |
| 1. Does the third party understand and appreciate the information security threats and concerns, as relates to Authoritysecurity policies and standards? |  |  |  |  |
| 1. Does the third party have a comprehensive incidence response and escalation methodology that captures different types of incidences (e.g. security breaches, threats, vulnerabilities, security-related hardware and software malfunctions) that might affect Authorityoperations? |  |  |  |  |
| 1. Does Third party house or access any critical information? |  |  |  |  |
| If yes, are Business information processing, storage or distribution facilities housed in areas protected by a defined security perimeter, with appropriate security barriers and entry controls. Are they physically protected from unauthorized access, damage, loss or compromise |  |  |  |  |
| 1. Does the third party have well-structured operation procedures and responsibilities? |  |  |  |  |
| 1. Does the third party have a well-established documentation and testing process prior to user acceptance and use in production and live environment? |  |  |  |  |
| 1. Does the third party, have protection against malicious software in the following levels:    1. Recovery plans in case of incidence    2. Anti-virus protection in place and current    3. Vulnerability testing for systems to ensure that systems are appropriately protected |  |  |  |  |
| 1. Do they have a well-defined change management process? |  |  |  |  |
| 1. Does the third party have access control policies with clear authentication, authorization and audit trail procedures that dictate the least privilege use? |  |  |  |  |
| 1. Do they have clear leavers and transfer policies that also involve Authority being told about thus events for clean-up and housekeeping in terms of system access? |  |  |  |  |
| 1. Do they have proper patch management procedures? |  |  |  |  |
| 1. Do they have a Business Continuity Plan in place? |  |  |  |  |
| If No. Do they have a level of business continuity and service recoverability |  |  |  |  |
| 1. Do they have a proper records methodology? |  |  |  |  |
| 1. Does Third party house or access any critical information? |  |  |  |  |
| 1. If yes, are Business information processing, storage or distribution facilities housed in areas protected by a defined security perimeter, with appropriate security barriers and entry controls. Are they physically protected from unauthorized access, damage, loss or compromise |  |  |  |  |
| 1. Does the third party have well-structured operation procedures and responsibilities? |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. Does the third party have a well-established documentation and testing process prior to user acceptance and use in production and live environment? |  |  |  |  |
| 1. Does the third party, have protection against malicious software in the following levels:    1. Recovery plans in case of incidence    2. Anti-virus protection in place and current    3. Vulnerability testing for systems to ensure that systems are appropriately protected |  |  |  |  |
| 1. Do they have a well-defined change management process? |  |  |  |  |
| 1. Does the third party have access control policies with clear authentication, authorization and audit trail procedures that dictate the least privilege use? |  |  |  |  |
| 1. Do they have clear leavers and transfer policies that also involve Authoritybeing told about thus events for clean-up and housekeeping in terms of system access? |  |  |  |  |
| 1. Do they have proper patch management procedures? |  |  |  |  |
| 1. Do they have a Business Continuity Plan in place? |  |  |  |  |
| If No. Do they have a level of business continuity and service recoverability |  |  |  |  |
| 1. Do they have a proper records methodology? |  |  |  |  |

*-----------------------------****For e-GA Control Only****----------------------------------*

Sample Name: **ICT Development, Acquisition, Operation and Maintenance Procedures**

Sample Reference: **eGA/EXT/SAM/008**

Sample Version: **01**

Sample Effective Date: **May 2024**

Sample Creation: **e-Government Authority**

Sample Changes: **None**