

PPROVAL	Name	Job Title/ Role	Signature	Date
Approved by	Dr. Mboni A. Ruzegea	Director General		

THE UNITED REPUBLIC OF TANZANIA

Applicable Public Institution

Tanzania Library Services Board (TLSB)**Document Name**ICT Service Management Procedures (**ICT-SMP**)**Document Number**

TLSB-ICT S01

Table of Contents

1. INTRODUCTION	2
1.1. Overview	2
1.2. Rationale	2
1.3. Purpose	2
1.4. Scope	2
2. PROCEDURES	2
2.1 ICT Service Delivery	3
2.1.1 Service Level Management	3
2.1.2 Capacity Management	5
2.1.3 Availability management	7
2.1.4 ICT Service Continuity Management	10
2.1.5 ICT Financial Management	11
2.2 ICT Service Support	12
2.2.1 ICT Service Desk	12
2.2.2 ICT Inventory Management Procedures	14
2.2.3 Incident Management	14
2.2.4 Problem Management	18
2.2.5 Release Management	21
2.2.6 Configuration Management	23
2.2.7 Change Management	24
3. IMPLEMENTATION, REVIEWS AND ENFORCEMENT	28
3.1. Implementation and Reviews	28
3.2. Exceptions	28
3.3. Roles and Responsibilities	28
3.3.1. Board of directors or accounting officer, whichever applies	28
3.3.2. ICT Steering Committee	29
3.3.3. Directors/ Managers/Head of Sections/Units.....	Error! Bookmark not defined.
3.3.5. Head of Internal Audit Unit	30
3.3.6. Users of ICT Systems	30
3.4. Monitoring and Evaluation	30
4. ACRONYMS	31
5. RELATED DOCUMENTS	31
6. DOCUMENT CONTROL	31
APPENDIX 1: CHANGE REQUEST FORM	ERROR! BOOKMARK NOT DEFINED.

1. INTRODUCTION

1.1. Overview

This ICT Service Management guideline document is used as a strategic approach to designing, delivering, managing and improving the way Information and Communication Technology (ICT) is used within Tanzania Library Services Board (TLSB).

1.2. Rationale

ICT Service delivery and support team in TLSB can ensure that ICT services are aligned to and actively support business needs.

1.3. Purpose

This document provides guidance on how to design, deliver, manage and improve ICT services within TLSB.

1.4. Scope

This document is for TLSB's Head of ICT, Infrastructure Delivery and Support team.

2. PROCEDURES

ICT Service Management is an approach to ICT management in the definition of ICT services and their requirements in such a way that the business user, ICT staff and external user can understand. It details the measurements required to identify successful delivery of these services in such a way that they are of value and use to the customer in relation to the goals that TLSB has. The ICT Service Management is broadly categorized into two main Areas:

- a. Service Delivery
 - i. Service Level Management
 - ii. Capacity Management
 - iii. Availability Management
 - iv. ICT Service Continuity Management
 - v. ICT Financial Management

- b. Service support
 - i. The Service Desk
 - ii. ICT Inventory Management procedures

- iii. Incident Management
- iv. Problem Management
- v. Configuration Management
- vi. Release Management
- vii. Change Management

2.1 ICT Service Delivery

2.1.1 Service Level Management

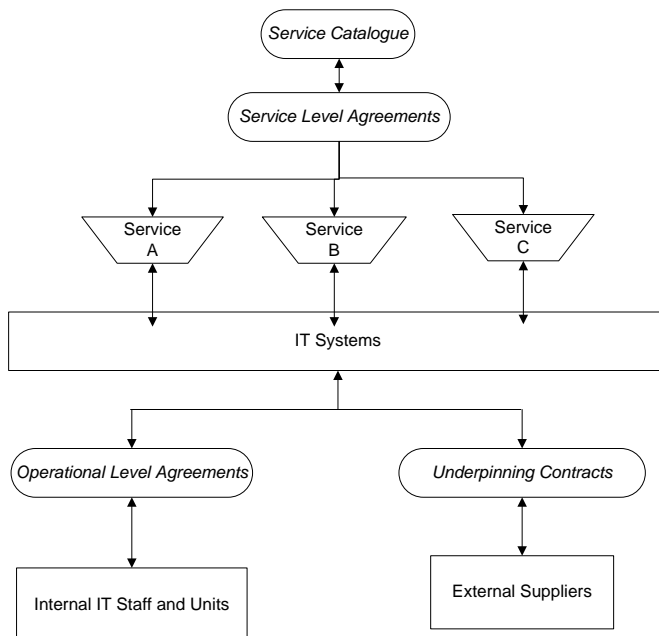
Service Level Management shall set the scope for all ICT's activities by facilitating the definition of the delivery from ICT Department to service points. This is done by defining and agreeing a catalogue of services, and then agreeing the service specifications, details and service levels with each business department.

- i. TLSB shall list down the service catalogue identifying the users for each service and obtain an understanding of the levels of service required as per table below;
- ii. A list of service catalogue along with identified users for each service and the levels of service required as shown in the table below;

SN.	Service Catalog	Types of services and expected service level requirements
1	Name of the Service	
2	Service Level Responsibility	
3	Short description of Service	
4	Users of the ICT Service on the client-side	
5	Breakdown of the offered Service into Service groups, e.g. along Infrastructure Components or ICT Applications	
6	For each Service group:	
	i. Which Services are offered	
	ii. Handling of Service interruptions (by telephone, by remote access, on site?)	

	iii. User Services (user administration, installation)	
	iv. What quality is required of the offered Services	
	v. Service times	
	vi. Availability requirements	
	vii. Number of interruptions allowed	
	viii. Availability thresholds (80 %)	
	ix. Downtimes for maintenance (number of allowed downtimes, pre-notification periods)	
	x. Procedure for announcing interruptions to the Service (planned/ unplanned)	
6	Service Level Agreement(SLAs) with External Supplier	
7	Performance requirements	

The diagram below represents the service level agreements with respect to different business services within TLSB as part of service catalogue.



iii. TLSB shall list down the key indicators and management metrics to evaluate the performance of service level management. Refer to example below:

- a. Agreement by senior management that the catalogue is complete;
 - b. 90% of services in the catalogue covered by SLAs;
 - c. SLA monitoring and reporting occurring on time, delivered to the correct parties, reflecting the agreed items;
 - d. SLA review meetings, on schedule, attended, minutes kept and actioned;
 - e. Service Level manager, has followed up on issues reflected in the minutes, and report back next meeting;
 - f. Service Level Agreement reviews are performed on schedule;
 - g. Formal follow up on Service level Breaches, documented and discussed at next service performance review;
 - h. Service Levels improving without excessive costs;
 - i. Costs decreasing without negative effect on service levels; and
 - j. Customer and user perceptions are improving.
- iv. Operational Level Agreements (OLAs) Reviews on schedule, Signed by Head of ICT, OLAs have not demonstrably fallen short of requirements.

2.1.2 Capacity Management

Capacity management ensures that the performance of services, capability of handling and storing and managing the required volumes of information by the infrastructure meets the Institutional requirements. This shall be achieved in a cost-effective way.

- i. TLSB shall describe the scenarios analysed in terms of, business process impact, to understand true capacity requirements. This includes consideration for items such as scalability, interoperability, throughput, availability requirements, storage, resource utilization, security and backups. Also, TLSB shall describe the strategy for developing these scenarios and a list of the individuals involved.
- ii. TLSB shall describe plans for growth and how they will be addressed and managed. TLSB shall consider not only the requirements for additional hardware, software, building materials, and space but also where financial resources for these items will come from, additional resource allocation requirements, staffing, training and other expenditures consider the table below:

Capacity Type	Current Capacity Analysis	Planned/Expected Growth and Recommendations
<i>[Describe the capacity scenario analyzed. Enter details on current & future capacity requirements.]</i>	<i>[Describe currently available capacity.]</i>	<i>[Describe how future growth expectations have been identified and analyzed. Outline recommendations for managing and addressing this expected growth.]</i>

iii. TLSB shall describe how expected growth will be monitored and managed. Below is a basic example of a table that may be used to illustrate one approach for monitoring and managing future capacity. The approach used to illustrate these requirements may differ from project to project;

Area/Item Monitored	Capacity Requirement(s)	% Increase Needed Per <time period>	Capacity Threshold(s)	Threshold Response Strategy (Action to Be Taken Upon Reaching Threshold(s))
<Hard Drive Storage>	<enter capacity requirements and measures>	<enter projected increases over intervals of time>	<enter acceptable capacity threshold(s)>	<enter response strategies to varying threshold limits. Threshold is defined as the level at which an event or change occurs>
<Meeting Room Tables>				
<Number of Project Staff>				
<Ratio of Quality Development Staff requirements>				

-
- iv. TLSB shall list down the key indicators and management metrics to evaluate the performance of capacity management. Refer to example below;
 - a. The annual plan is produced on time and is accepted by senior management. And is linked to the supplied business plans. It provides accurate forecasts of planned expenditure
 - b. Recommendations for hardware or software upgrades that are identified in the Capacity Plan are accurate both in terms of the financial cost and the timescale in which they are required. These recommendations are acted on.

2.1.3 Availability management

Availability Management is the planning, implementation, management and optimization of ICT Services within **TLSB** so that they can be used where and when the business requires them.

For each service included in Availability Management, the following sections will be completed:

- a. **Service Name & Description:** The name of the service, along with a high level description of what is included in the service as well as what is excluded;
- b. **Current SLAs:** Lists the identifier for each SLA that applies to this service, along with the location of the SLA;
- c. **Current OLAs:** Lists the identifier for each OLA that applies to this service, along with the location of the OLA;
- d. **Current Availability Status:** Describes the recorded availability for this service over the past year;
- e. **Current Availability Problems:** Describes any availability problems which were encountered during the past year, along with an evaluation of the cause of the issues;
- f. **Primary Service Components:** Lists the major components which are being monitored in terms of availability for this service. The components shall be identified as: Hardware and Software;
- g. **Anticipated New Business Requirements:** Outlines any new business requirements which have been identified for the coming year; and
- h. **Availability Impacts:** Identifies the impact on availability of delivering these business Requirements.

Recommendations: Lists different options for addressing the new business requirements or of improving the availability for the current requirements.

- i. TLSB shall list down the key indicators and management metrics to evaluate the performance of capacity management as per format below:

Service 1- Service Description	
Provide description of the service	
Service 1- Current SLA and Location	
SLA Identifier	SLA Location
[SLA-1 ID]	[Service Level Management Repository]
Service1 –Current OLA & Location	
OLA Identifier	OLA Location
[OLA-1 ID]	[Operational Level Management Repository]
Service1 –Current Availability Status	
Insert the Availability status for this service for the past year. (This could be tables, graphs, or text.)	
Service 1-Primary Service Components	
Hardware: <ul style="list-style-type: none"> • Component 1: [Component Identifier] • Component 2: [Component Identifier] • Component 3: [Component Identifier] Software: <ul style="list-style-type: none"> • Component 1: [Component Identifier] • Component 2: [Component Identifier] • Component 3: [Component Identifier] 	
Service 1-Anticipated business requirements changes	
Identify any new business requirements that have been identified for this service for the next year. These are not the technical requirements, so use layman’s terms where possible.]	

Service 1- Availability impact of new business requirements
[Identify any impacts to Availability should the Business Requirements be delivered. In this situation, it could be necessary to identify the impacts to individual infrastructure components]
Service 1- Recommendation
<p>[Identify any impacts to Availability should the Business Requirements be delivered. In this situation, it could be necessary to identify the impacts to individual infrastructure components]</p> <ul style="list-style-type: none"> • Recommended changes in monitoring, analysis, or tuning • Identification of potential bottlenecks • Performance guidelines for design and development • Prediction of future service performance • Tools to be used • Project bandwidth availability sizing • Application sizing, if appropriate • Monitoring requirements and alarm settings • Performance Management tuning • New storage requirements • New technologies • Estimated costs • Threshold audits • Projections & Forecasting • Availability analysis recommendations from all previous procedures • Single Point of Failure (SPoF) analysis recommendations • Technical Observation recommendations

TLSB shall indicate the key indicators and management metrics to evaluate the performance of availability management. Refer to the below;

- a. Improvement in Service Availability
- b. Lowering of costs associated with downtime

- c. Reduction in the number, level of business impact and frequency of incidents
- d. Time to restore service is reduced overall
- e. New services have fewer problems and incidents related to them.

2.1.4 ICT Service Continuity Management

The ICT Service Continuity Plan contains information about measures that serve the purpose of disaster preparation, in that they counteract identified risks within TLSB. This activity was initially called ICT Disaster Recovery Planning (DRP).

- i. TLSB shall list down all identified non-tolerable risks for business services as per table below. Also refer to the Institutional ICT Disaster recovery Guide.

Headers	<Provide your response as per bullets highlighted>
•Name of the risk	
•Affected business processes	
•Affected business data	
•Affected ICT Services	
•Affected infrastructure components	
•Measure for reducing/ eliminating the risk	
✓ Description	
✓ Costs and resources	
✓ Person in charge of the measure	
✓ Target date	
✓ Status	
✓ Name of the risk	
✓ Affected business processes	

- ii. TLSB shall list down the key indicators and management metrics to evaluate the performance of ICT Service Continuity management. Refer to the list below;
 - a. Plan reviewed on annual basis;
 - b. Actions documented from the review are completed;
 - c. Tests are conducted according to schedule, reports produced from the testing;

- d. Reports of actions to be taken as a result of the testing;
- e. Actions completed from the review;
- f. Number of incidents occurring from failed risk countermeasures, and the number of times the countermeasures were effective;
- g. Number of times SLA were breached;
- h. Strategy document covers all services in the catalogue. Services from the catalogue covered or explicitly left out of the planning. Exceptions not covered or reviewed at all;
- i. Risk assessment project performed; follow up projects on an annual (or other regular basis) completed;
- j. Countermeasures that were identified have been implemented;
- k. Standby arrangements: Lists up to date. Staff aware of their responsibilities;
- l. Staff training – up to date with changes in role allocations; and
- m. Standby site(s) kept up to date with changes on live sites.

2.1.5 ICT Financial Management

ICT financial management deals with ICT related costs and expenditure and to provide a sound financial basis for business decisions regarding ICT within TLSB. This is achieved by budgeting, identifying and accounting for the costs of providing ICT services.

- i. TLSB shall list down its budget requirements for costs associated with the recurrent ICT projects. The budget exercise is an ongoing monitoring of current budget and is reviewed bi-annually. As part of budget exercise, the following factors will be considered:
 - a. Limits on capital expenditure;
 - b. Limits on operational expenditure;
 - c. Limits on variance between actual and predicted spend;
 - d. Agreed workload and set of services to be delivered;
 - e. Limits on expenditure outside the institutions; and
 - f. Agreements on how to cope with exceptions.
- ii. To make easier identification of expenditure, a list of cost elements shall be performed. See the cost element below:
 - a. Hardware;

- b. Software;
 - c. People and Training;
 - d. Accommodation;
 - e. Underpinning or external Services; and
 - f. Transfer Costs – within the institution.
- iii. Key indicators and management metrics to evaluate the performance of ICT financial management shall be listed. Below are the metrics;
- a. The processes used to track expenditure are in place and working;
 - b. The budget is produced;
 - c. Regular (monthly or quarterly) budget and expenditure comparison reports re produced for senior management;
 - d. Costing reports are produced;
 - e. If charging has been implemented then invoices are sent at the correct time, and income is collected and monitored; and
 - f. Involvement in major change decisions to ensure financial viability of the proposed solutions.

2.2 ICT Service Support

2.2.1 ICT Service Desk

ICT service desk aims to drive and improve ICT services within an Institution. The service desk provides a point of contact where customers can report incidents, obtain assistance with the use of ICT services, or request basic changes.

- i. **TLSB** shall list down the service desk responsibilities and the service request form as below.

Service Unique ID	Name of Person	Date and time of service request
Detail of service request		
No of Users Affected	System usage in hours per week	

TANZANIA LIBRARY SERVICES BOARD

1, 2-5, 6-10 or more	1, 2-10, 11-20 or more	
Technician required	Date and time of response	
How was the incident resolved		
Further action required		
Was the equipment repaired or replaced.		
Configuration management database updated		

- ii. TLSB shall list down the key indicators and management metrics to evaluate the performance of ICT service desk. These metrics includes:
 - a. Call taking – times taken, lost/abandoned calls;
 - b. Time for each call;
 - c. Logging of calls or updating for queries VS number of incoming calls;
 - d. Content of incidents – complete, classifications etc. for reporting purposes complete and accurate;
 - e. Escalation- Where manual interference is required on lack of acceptance follow up personally with relevant management; and
 - f. Outgoing contacts two users and customers according to defined timeframes and impacts.

- iii. Any ICT service request will be reported to ICT Management Services through: ictsupport@tlsb.go.tz, and/or ictsecurity@tlsb.go.tz. If available, it may include the Helpdesk system.

- iv. The escalation levels of the service request shall be defined by the Head of ICT.

- v. When necessary to escalate to eGA, then Head of ICT can use egov.helpdesk@ega.go.tz and/or logging to eGA helpdesk through <http://helpdesk.ega.go.tz/>

2.2.2 ICT Inventory Management Procedures

ICT inventory Management Procedures to TLSB helps to deliver its strategic priorities and services in line with risk, providing value for money services for the benefit of TLSB.

All the ICT Inventory Management Procedures shall ensure;

- i. Records are kept regarding the purpose, location, ownership and usage of ICT related inventories.
- ii. Acquisition of ICT inventories, accounting & storage of ICT inventories, aging analysis for the ICT inventories, perpetual stocking and annual ICT stock taking shall be in accordance to the Public Asset Management Guideline document of the year 2019 by the ministry of Finance.
- iii. There shall be a preventive maintenance for all ICT assets at TLSB. This is a routine maintenance of ICT equipment and assets in order to keep them running and prevent any costly unplanned downtime from an unexpected equipment failure.
- iv. TLSB shall prepare accordingly a preventive maintenance schedule of its ICT assets and retain documentation of results after maintenance is performed.
- v. The acquisition, recognition, valuation, verification, transfer, depreciation, disposal and impairment of all ICT assets shall be performed in accordance to the Public Asset Management Guideline document of the year 2019 by the ministry of Finance.

2.2.3 Incident Management

Incident Management is an approach to managing the lifecycle of all incidents within TLSB. It aims to return ICT services to users as quickly as possible. A comprehensive incident management procedure should be in place to address ICT related incidents within TLSB.

- i. TLSB shall record and priorities the incident with appropriate diligence, in order to provide a quick resolution to an incident.
- ii. At TLSB, all ICT incidences shall be recorded on the incident record sheet. Below is the record incident sheet.

Incident Record Sheet					
Unique ID:	Date and Time of recording:				
Method of Notification (<i>i.e. telephone, email, internet</i>):					
Incident Urgency <<Use the templates below to derive to the incident priority>>	High <input type="checkbox"/>	Medium <input type="checkbox"/>		Low <input type="checkbox"/>	
Incident Impact <<Use the templates below to derive to the incident priority>>	High <input type="checkbox"/>	Medium <input type="checkbox"/>		Low <input type="checkbox"/>	
Incident Priority <<Use the templates below to derive to the incident priority>>	Critical <input type="checkbox"/>	High <input type="checkbox"/>	Medium <input type="checkbox"/>	Low <input type="checkbox"/>	Very Low <input type="checkbox"/>
Service Desk Officer					
Caller / User Contact					
Call back Method					
Description of Symptoms					
Affected users, Locations, and/or business areas					
Affected Services					

<i>Incident Priority</i> << Determine the Incident Urgency and the Incident Impact to determine the incident priority. Use the templates below to derive to the incident priority>>		
Links to related incident records:		
Resolution Process: <<State how the incident was resolved>>		
IT Staff Name:	Resolution Date	Signature:

a. Incident Urgency

To determine the incident category, highest relevant category is chosen:

Category	Description
Highest (H)	<ul style="list-style-type: none"> i. Several critical users are affected ii. Work that cannot be completed by staff is highly time sensitive iii. The damage caused by the incident increases rapidly
Medium (M)	<ul style="list-style-type: none"> i. The damage caused by the incident increases considerably over time ii. Few critical users are affected
Low (L)	<ul style="list-style-type: none"> i. The damage caused by the incident increases marginally over time ii. Work that cannot be completed by staff is not time sensitive

However, the above can be relied to the Institutional Risk Rating as per the Risk Management Framework i.e. Extreme, High, Medium, Low etc.

b. Incident Impact

To determine the incident impact, choose the highest relevant category:

Category	Description
Highest (H)	<ul style="list-style-type: none"> i. A large number of staff are affected and/or not able to do their job ii. The financial impact of the Incident is likely to exceed <<Insert amount likely to be incurred from the incident>> iii. The damage to the reputation of the Institution is likely to be high
Medium (M)	<ul style="list-style-type: none"> i. A moderate number of staff are affected and/or not able to do their job properly ii. The financial impact of the Incident is (for example) likely to exceed << Insert lowest amount to be incurred from incident >> but will not be more than<< Insert highest amount likely to be incurred from the incident >> iii. The damage to the reputation of the Institution is likely to be moderate
Low (L)	<ul style="list-style-type: none"> i. A minimal number of staff are affected and/or able to deliver an acceptable service but this requires extra effort ii. The financial impact of the Incident is (for example) likely to be less than << insert lowest amount likely to be incurred from incident >> iii. The damage to the reputation of the Institution is likely to be minimal

c. Incident priority

Incident priority is a combination of the incident's urgency and level of impact to TLSB. An Incident Priority Matrix is used to determine the level of priority to be given to any incident.

Priority Code	Description	Target Response Time	Target Resolution Time
1	Critical	Immediate	<< based on institution's acceptable time>>
2	High	<< based on TLSB's acceptable time>>	<< based on TLSB's acceptable time>>
3	Medium	<< based on TLSB's acceptable time>>	<< based on TLSB's acceptable time>>
4	Low	<< based on TLSB's acceptable time>>	<< based on TLSB's acceptable time>>
5	Very Low	<< based on TLSB's acceptable time>>	<< based on TLSB's acceptable time>>

- iv. TLSB shall list down the key indicators and management metrics to evaluate the performance of incident management. The metrics are as below:
- Number of incidents in total and by category;
 - Average time to resolve incidents by impact code;
 - Percentage of incidents handled within the agreed times;
 - Percentage of incidents resolved by the Service Desk;
 - Average cost per incident;
 - Number of outstanding or unresolved incidents per day over SLA time;
 - Number of incidents resolved remotely;
 - Number of incidents re-opened if closed incorrectly; and
 - Number of ineffective workarounds or resolutions.

2.2.4 Problem Management

Problem management is the process of managing the lifecycle of all ICT related problems. The objective of problem management is to prevent the occurrence of incidences causing the problems and their impact to the Institution. Proactive problem

management can reduce the frequency of incidences through the identification and review of trends over a period of time.

- vi. At TLSB, ICT problems shall be identified and recorded on the problem record sheet. The objective of using a problem record sheet is to document all the relevant details of the problem including its history in an effort to properly manage the problem from identification to closure. A problem record sheet is shown below;

Problem Record Sheet		
Unique ID:	Date and Time of detection:	
Problem Owner:		
Description of Symptoms:		
Affected Staff / Departments:		
Problem Priority << Determine the Incident Urgency and the Incident Impact to determine the incident priority. Use the templates above in Incident Management to derive to the incident priority>>:		
Problem Category (<< hardware error, software error, network error etc.		
Links to related problem records		
Links to related incident records		
Resolution Process: << State how the problem was resolved>>		
ICT Staff Name:	Resolution Date:	Signature:

vii. Problem Categorization and Prioritization

The priority of a problem is a function of urgency and the overall impact to the Institution daily activities. By using the incident priority matrix, the ICT staff can derive to the problem priority rating and resolve it using the 3 level support approach.

viii. Problem Diagnosis and Resolution

The purpose of performing a diagnosis is to determine the root cause of a problem in order to identify a suitable solution. Misdiagnosis can lead to increased loss of ICT services to staff and loss of resources (staff time and money). During problem diagnosis, the ICT team led by the Head ICT shall identify a workaround that would temporarily reduce or eliminate the problem whilst waiting for the full resolution.

ix. Problem Closure and Evaluation

All resolved problems shall be properly documented on the Problem Record sheet with full details of how they were resolved. During closing of the problem, the following shall be checked:

- a. Documentation of the root cause of the Problem
 - b. Documentation of possible Workarounds
 - c. Documentation of the applied (causal) resolution
 - d. Date of Problem resolution
 - e. Date of Problem closure
- x. TLSB shall list down the key indicators and management metrics to evaluate the performance of problem management. Below are the metrics;
- a. From a representative sample of incidents an evaluation of whether Problem Management is identifying underlying or common problems and recording these
 - b. From a representative sample of problem records, verify that problems are correctly diagnosed.
 - c. From all problem and known error records identify that those with the greatest impact are resolved or scheduled for resolution.
 - d. That Problem Management staff are adhering to escalation thresholds managed by Incident Management.

- e. That overall numbers and level of impact of incidents is decreasing
- f. That incidents re-occur less frequently

2.2.5 Release Management

The aim of Release Management is to plan and oversee the successful rollout of hardware and software changes into production within TLSB. This also ensure that the changes made to hardware and software can be tracked, using the services of Configuration Management, and that only correct, authorized and tested hardware/software versions are installed.

- i. At TLSB, after the software has been tested in the test environment and is ready to be moved to the live environment. The ICT personnel responsible shall fill-in a release Management. The release management form is provided below:

Ref No.	
Release Date	
Initiator	
Name of application	
Nature of Software Release	1) New Software 2) Bug Fix 3) Functionality Change
Deployment Path	4) Production environment 5) Other – Please Specify _____
Proposed Release Start Date/Time	
Proposed Release Completion Date/Time	
Downtime Required	6) Yes - Specify No of. Hours _____ 7) No
Backup Requirements	8) Code files

TANZANIA LIBRARY SERVICES BOARD

	<p>a. Entire Application</p> <p>b. Only released code files</p> <p>9) Database</p>
Rollback Plan (time to start rollback if any issue encountered)	<p>10) Immediate</p> <p>11) Other - Please specify</p> <p>_____</p> <p>_____</p>

ii. Please fill in the table below before any release. This will be authorized by Head of ICT within TLSB.

Line of Service	Name	Decision		Justification	Signature	Date
		Accepted	Refused			
Final decision for the activity				Name :		
				Comments :		
				Signature :		
				Date :		

iii. The release Head of ICT shall then deploy the software on the live environment and ensure that the software is working as expected.

Name of official who carried out the activity	Date	Signature
Change Status	1) Successful 2) Unsuccessful – Specify reason	

- iv. TLSB shall list down the key indicators and management metrics to evaluate the performance of release management. Refer key indicators below:
- a. Releases built on schedule within budgeted resources;
 - b. Liaison with application development is adequate to remove problems of communication over delays caused by them, if they do not fall within OLAs and cannot guarantee results on time ;
 - c. Low numbers or no back-out of releases;
 - d. No evidence of software that has not passed QA checks;
 - e. Compliance of all legal restrictions on bought in software;
 - f. Accurate distribution of software to all sites;
 - g. Implementation of releases on all sites as scheduled;
 - h. No evidence of unauthorized software at any site;
 - i. Planned composition of releases matches the actual release, exceptions beyond the control of Release Management – e.g. suppliers not meeting commitments/contracts shall be excluded. That issue should be referred to Service Level Management and the contract review process; and
 - j. Evidence of adequate forward planning for technical and human resources for Release Management.

2.2.6 Configuration Management

Configuration management provides accurate information on configuration and their documentation in order to support all the ICT management and service management processes within TLSB.

- i. A list is prepared as per table below to detail the status of the configuration which involves the collection, processing, and reporting of the configuration data for all Configuration items at any given time. This also includes management stored

configuration information held in the Configuration Management Database (CMDB). The configuration management form is provided below:

Configuration Item (CIs)	Unique Identifier	Manufacturer	Description	Location	Assigned to	Date Recorded	Date Last updated
Desktop Computer	1	IBM	Desktop Pro	Room1	XYZ	1-Oct 15	
	2	HP	HP Book	Room 2	ABC	1-Oct 15	
	3	IBM	Lenovo	Room 3	XYZ	1-Oct 15	
File Server	4	Compaq	Proliant	Computer room	Head of ICT	1-Oct 15	

- ii. Below are key indicators and management metrics to evaluate the performance of configuration management. Below are the metrics;
- Are regular configuration database audits carried out and are the results recorded and follow up actions performed?
 - Are archived CIs retained and recorded correctly?
 - Are the versions of software used in multiple locations correct?
 - Do CI names, version numbers, etc. adhere to naming conventions?
 - Are CI variants created and handled according to procedures?
 - Do the contents of the Digital Subscriber Line (DSL) and CMDB match?
 - Is CMDB housekeeping carried out according to procedures?
 - Are reviews held regularly and followed up?

2.2.7 Change Management

a. Formally Request a Change

- Any proposed change to the equipment or system which forms part of or supports TLSB ICT environment for which ICT is responsible, must be supported by a formal change request documentation, initiated by Change Requestor (CR) and approved by appropriate ICT management levels. Refer Change Request Form in Appendix 1.

- ii. All change details as well as configuration records must be maintained for all changes, major, minor, routine and emergent and updated in a proper order. The change request specification must contain:
- Date of submission, date of change and date of completion;
 - Authorization by a line manager and all corresponding levels;
 - Completed by sign off or in case of emergency change it can be completed by email or over the phone, and then it should be later on finalized under official procedures;
 - Full Change description details, service affected scope (if any), key contacts;
 - Indication of success or failure and updated change scope/details; and
 - For all emergency (unplanned) changes, a post-mortem report/feedback is a must after the changes.
- iii. All unplanned/ad hoc changes should be treated as emergent changes and must be highly discouraged;
- iv. Request for changes should be submitted for authorization in a specific time frame prior to target implementation date and must adhere to user notification timeframe to enable risk assessment process to expose threats that may be encountered thereof. Expectation will be provided on emergency changes only (Refer to APPENDIX 1.1 Change Request Form). Please refer to the below table.

CHANGE TYPE	RISK ASSESSMENT	SUBMITTAL AND APPROVAL REQUIREMENTS	USER NOTIFICATION TIMEFRAME
1: Major Change [e.g. Planned Operation Systems Patches, Database Patches, Planned Hardware Upgrade, Planned Application Upgrade]	High Risk - Potential to disrupt critical business and activities for many Public Institutions - Will affect all users if not implemented successfully. - Affects multiple systems or elements of the infrastructure - Complex or lengthy implementation and back-out.	- Change Request must be submitted 14 days prior to target implementation date. - Reviewed and approved at CAC Level	7 days prior to target implementation date

TANZANIA LIBRARY SERVICES BOARD

<p>2: Minor Change</p> <p>[e.g. Firewall configuration, Security Patches, Fixing a disaster recovery system]</p>	<p>Medium Risk</p> <ul style="list-style-type: none"> - Minor visibility to users and minimal business and/or Public Institutions impact - Impact limited to specific portions of infrastructure - Quick and fairly simple back-out. 	<ul style="list-style-type: none"> - Change Request must be submitted 7 days prior to target implementation date. - Reviewed and approved at supervisor or department Director level 	<p>2 days prior to target implementation date</p>
<p>3: Routine Change</p> <p>[e.g. Installation of a new printer model, deletion of user]</p>	<p>Low Risk</p> <ul style="list-style-type: none"> - No visibility to users and no business and/or Public Institutions impact - Has been implemented in many other areas with no errors. - Routinely done without any failures on the first attempt. 	<ul style="list-style-type: none"> - Change Request must be submitted 1 day prior to target implementation date - Reviewed and approved at Manager level 	<p>1-24 hours prior to target implementation</p>
<p>4: Emergency Change</p> <p>[Fixing systems problems, Fixing System attacks, Unplanned Upgrades]</p>	<p>High or Medium Risk</p> <ul style="list-style-type: none"> - Critical service is down or severely impaired with disruption to business and/or student activities - Fix first, and document change after the fact - Can be unplanned major or minor change 	<ul style="list-style-type: none"> -If it is emergent due to lack of planning, The change must be approved before execution on a time frame approved by the respective director. - Otherwise Change Requestor notifies the Help Desk and CAC and ensure that change Request is documented within 2 working days after implementation and release of change 	<ul style="list-style-type: none"> -If it is emergent due to lack of planning, respective director may determine the user notification time frame, otherwise it should be immediate

b. Analyse and Justify Change

- i. The change requestor will work to develop a specific justification for the change and identify the impact on infrastructure, business operations and budget, identify business as well as technical risks, develop technical requirements, and review specific implementation steps;
- ii. Any change request to the system must have a full testing procedure attached explaining all required tests to be performed with their expected outcome documented, including roll-back procedures (critical components) for all unsuccessful changes;
- iii. All change request received must be assessed, verified to ensure that the request contain the adequate details, including completion date and have been approved by authorized representatives of respective directorates;

- iv. Any amendments to the original scope of the change request and planned implementation schedule must be re-submitted to CAC for approval to facilitate implementation on the revised schedule;

c. Approve and Schedule the Change

- i. Unauthorized change request or requests with insufficient details must be rejected and returned to the requester including remarks or justifications for rejection. A requester is supposed to re-establish the request and justify the course and expected enhancement/output;
- ii. For all planned changes, all issues relating to potential business impact, resource requirements, implementation plans, back out details and conflicting requests must be resolved prior to its final sign off authorization for execution;
- iii. Change requests must be authorized by respective manager and all other appropriate managers, logged and recorded in a Change Management System, with reference ticket numbers;
- iv. The TLSB Head of ICT will chair a Change Management Team (CMT) consisting of chosen representatives from members of different field such as Network Engineering, Server Administration, Operations, Applications Support, Security Administration, ICT Service Management, ICT Service Control, Database Administration, Desktop Support and Business Operations. The group will assess the urgency and impact of the change on the infrastructure, Institutions productivity and budget. The CMT will have a permanent Change Coordinator that will coordinate all changes. In the event of a Major Change, the change request must be approved by the Change Approval Committee/ Change Advisory Board (CAC)- (Consisting of Executive Directors - and where appropriate Accounting Officer such as Director General (DG) as agreed by Executive Directors or on recommendation by the Change Management Team).

d. Plan and Complete change

- i. The Change Management Team will assign appropriate members to complete the change in a manner that will minimize impact on the infrastructure and Public Institutions. In the event that the change does not perform as expected or causes issues to one or more areas of the production environment, the team will determine if the change should be removed and the production environment returned to its prior stable state;

- ii. All unsuccessfully/failed changes and changes not completed within a week as per their scheduled date must be closely followed-up by Change Management Team /Change Requestor for closure /explanation/re-scheduling.

3. IMPLEMENTATION, REVIEWS AND ENFORCEMENT

3.1. Implementation and Reviews

- 3.1.1.** This document shall come into operation once tabled and agreed in management meeting, and approved in its first page, and then shall be considered mandatory for all TLSB business operations.
- 3.1.2.** TLSB's management will use this document in conjunction with the documents in Section 6, below to ensure that it is operated within a well geared ICT ecosystem.
- 3.1.3.** All employees and other authorised users of TLSB shall comply with requirements in this document.
- 3.1.4.** The Head of ICT shall enforce compliance by using audit trails and triggering access denial to TLSB systems and networks.
- 3.1.5.** TLSB staff found to have violated this policy may be subject to withdrawal and or suspension of systems and network privileges or disciplinary action in accordance with rules defined by TLSB administrative regulations.
- 3.1.6.** This document shall be reviewed within five years, or whenever business environment of TLSB changes in a way that affects this current document.

3.2. Exceptions

- 3.2.1.** In case of any exceptions to this document, it shall be thoroughly documented and follow through a proper channel of authorization using the same authority which approved this document.

3.3. Roles and Responsibilities

3.3.1. Board of directors or accounting officer, whichever applies

- 3.3.1.1.** Review and approve the Policies, and provide strategic directives on utilisation of ICT in order to enhance productivity by ensuring effective and efficient systems;

- 3.3.1.2.** Appoint an ICT Steering Committee (or equivalent) and determine its terms of reference [Could be the Management Team Sitting with a focus on ICT Matters]; and
- 3.3.1.3.** Ensure implementation of the ICT services management processes.

3.3.2. ICT Steering Committee

- 3.3.2.1.** Shall review and provide advice on ICT investment portfolio and priorities;
- 3.3.2.2.** Shall ensure alignment of ICT with the TLSB's business needs;
- 3.3.2.3.** Shall ensure e-Government guidelines and standards are implemented by TLSB;
- 3.3.2.4.** Shall ensure continuous monitoring and evaluation of TLSB ICT projects;
- 3.3.2.5.** Shall review and approve TLSB disaster recovery plan and ensure its effective implementation;
- 3.3.2.6.** Shall approve any other TLSB e-Government sub-committee as may, from time to time, be constituted and address specific ICT related matters;
- 3.3.2.7.** Shall prepare and submit quarterly Ministerial e-Government progress report to the Authority;
- 3.3.2.8.** Shall perform such other functions as may be directed by the Accounting Officer or the Authority; and
- 3.3.2.9.** Shall perform such other functions as may be directed by the TLSB Director General/ Accounting Officer or the Authority.

3.3.3. Head of ICT /department /unit /section

- 3.3.3.1.** Shall ensure that all users under their supervision are aware and comply with this document;
- 3.3.3.2.** Shall provide adequate and appropriate protection of ICT assets and resources under their control;
- 3.3.3.3.** Shall ensure availability, integrity and confidentiality of information produced by systems under their areas of functional responsibilities and thereby ensure continuity of operations; and
- 3.3.3.4.** Shall review and approve procedures, standards, policies and guidelines developed from this policy for the purpose of maintaining business continuity and security of TLSB's ICT resources; and

3.3.3.5. Shall be custodian of "Data and Information" for their respective Departments/sections/Units.

3.3.4. Directors/ Head of Department/Units /Sections

Subject to general oversight of Board of Directors or accounting officer, whichever applies and advice of the ICT Steering Committee, the Head responsible for ICT shall oversee the overall implementation of this policy; and in particular he/she shall;

3.3.4.1. Coordinate the review and amendment of this document, as and when required in order to accommodate new technologies or services, applications, procedures and perceived dangers;

3.3.4.2. Plan and develop ICT Strategy and TLSB's Enterprise Architecture and ensure its implementation;

3.3.4.3. Keep abreast of ICT developments in respect of ICT industry in General and TLSB's systems in particular;

3.3.4.4. Initiate and recommend proposals to change, modify or improve this document;

3.3.4.5. Recommend procedures, standards and policies for effective implementation of this policy in line with e-Government Standards and Guidelines; and

3.3.4.6. Be the custodian of all ICT resources of TLSB including those centrally stored in server room/data centre.

3.3.5. Head of Internal Audit Unit

3.3.5.1. Shall audit the ICT Function of TLSB and ensure compliance with the document.

3.3.6. Users of ICT Systems

3.3.6.1. Shall be responsible to safeguard ICT assets of TLSB in their custody.

3.3.6.2. Shall comply with this document.

3.4. Monitoring and Evaluation

3.4.1. ICT Steering Committee shall meet at least quarterly to monitor and evaluate the achievements in ICT initiatives against TLSB ICT Policy, Strategic Plan and Enterprise Architecture.

4. ACRONYMS

CI	Configuration Item
CMDB	Configuration Management Database
DRP	Disaster Recovery Plan
DSL	Digital Subscriber Line
ICT	Information and Communication Technology
ICT-SMP	ICT Service Management Procedures
OLA	Operational Level Agreement
QA	Quality Assurance
SLA	Service Level Agreement
TLSB	Tanzania Library Services Board

5. RELATED DOCUMENTS

- 5.1. e-Government Guidelines, 2017
- 5.2. Standards for Creation of Government ICT Management Documents
(eGA/EXT/AVS/003)
- 5.3. eGovernment Business Architecture – Standards and Technical Guidelines
(eGA/EXT/BSA/001)
- 5.4. Public Asset Management Guideline document of the year 2019

6. DOCUMENT CONTROL

REVISION	NAME	COMMENT	DATE
Rev. 1.0	ICT-SMP	Adopt and Review ICT-SMP	11.11.2022

-----*For TLSB Control Only*-----

Name: ICT Service Management Procedures

Reference: **TLSB/EXT/ SMP /01**

Version: **1.0**

Effective Date: **November, 2021**

Creation: **Tanzania Library Services Board**

Changes: **None**