Veterinary Medicines Directorate

Standard Operating Procedure

for

Information Communication Technology Management

Document Review Sheet

The signatures below certify that this SOP has been reviewed, accepted, and that the signatories are committed to ensuring its provisions.

	Name & Signature	Position	Date
Developed by	Baraka Nyinge Karima Baraka	ICT Officer	28/07/2025
Reviewed by	———	Principal ICT Officer	
Approved by	Dr. Emily Muema. Muema.	Ag. CEO, VMD	30/7/2025

Table of Contents

2.0 General

2.1 Purpose

To ensure efficient, secure, and compliant management of ICT systems within the Veterinary Medicines Directorate (VMD) to support regulatory oversight of veterinary medicinal products (VMPs), pharmacovigilance, inspections, and stakeholder communication, while adhering to national and international standards.

2.2 Scope

This SOP applies to all ICT systems, hardware, software, and data management processes within the VMD, including regulatory databases, internal department operations, and external stakeholder interfaces.

2.3 References

- VSVP Act 2011 (VMD Regulations 2015)
- VMD Strategic Plan, 2023-2027
- VMD ICT Policy, 2025
- Data Protection Act, 2019

2.4 Abbreviations/Acronyms

Abbreviation	Definition
VMD	Veterinary Medicines Directorate
ICT	Information Communication Technology
MA	Marketing Authorization
VMP	Veterinary Medicinal Product
HOD	Head of Department
LAN	Local Area Network
WAN	Wide Area Network
MIS	Management Information System
SQL	Structured Query Language
VPN	Virtual Private Network
SLA	Service Level Agreement
TOR	Terms of Reference
AD	Active Directory
PABX	Private Automatic Branch Exchange
UPS	Uninterruptible Power Supply

2.5 Definitions

- **Potent Risk:** Potential raw risk anticipated in ICT operations.

- **Regulatory Database:** Systems storing VMP registrations, pharmacovigilance, and inspection data.
- **Pharmacovigilance:** Monitoring and reporting adverse events or adverse reactions related to VMPs.

2.6 Responsibility

The Manager, ICT is primarily responsible for ensuring this SOP is implemented and remains adequate. All ICT Division staff (ICT Officer, Senior ICT Officer, Principal ICT Officer) are responsible for executing their assigned duties as outlined in Section 3.0. Other VMD departments, divisions, sections and units to provide inputs and ensure compliance.

3.0 Administrative Structure

The ICT Division operates under the VMD's Directorate of Corporate Services, reporting to the CEO of VMD. The structure and duties are as follows:

3.1 Manager, ICT

- Reports to: CEO, VMD
- Duties:
    - Select and implement technology to streamline operations.
    - Test and evaluate computer security measures.
    - Analyze and resolve operational ICT issues.
    - Identify and evaluate emerging technologies.
    - Participate in performance reviews and business process improvements.
    - Forecast and plan ICT needs.
    - Analyze user requirements to automate processes.
    - Enhance existing systems' capabilities.
    - Evaluate software application requests for feasibility.
    - Ensure implementation and monitoring of ICT policies.

3.2 Principal ICT Officer

- Reports to: Manager, ICT
- Duties:
    - Research and recommend new technologies.
    - Develop and coordinate network security measures.
    - Plan and implement network infrastructure upgrades.
    - Maintain messaging systems, intranet, and extranet.
    - Manage outsourced ICT service providers per SLAs.
    - Develop ICT SOPs.
    - Prepare technical specifications for ICT purchases.
    - Modify ICT systems to meet standards.

3.3 Senior ICT Officer

- Reports to: Principal ICT Officer
- Duties:
    - Manage servers (e.g., email, backup) and their software.
    - Administer user accounts and permissions in AD and systems.
    - Research, plan, and install new servers.
    - Control database access and recommend upgrades.
    - Design and implement backup and security measures.
    - Manage firewalls, antivirus, and intrusion detection systems.
    - Develop and maintain network administration policies.
    - Propose solutions for network upgrades.
    - Manage network asset inventory and documentation.

3.4 ICT Officer

- Reports to: Senior ICT Officer
- Duties:
    - Operate and support business applications, hardware, and LAN.
    - Provide user administration and support.
    - Maintain on-site and off-site data centers.
    - Implement security measures (e.g., antivirus, patches).
    - Commission, repair, and maintain ICT equipment (e.g., PCs, printers, CCTV).
    - Review and test hardware/software for efficiency and compatibility.
    - Implement ICT policies.
    - Conduct staff awareness on cybersecurity risks.
    - Maintain backups of user data, CCTV, and biometric data.
    - Monitor network traffic and capacity.

4.0 Processes

4.1 Overview

The ICT Division ensures secure, reliable, and efficient ICT systems to support VMD's core functions, including:

- Management of regulatory databases (e.g., VMP authorizations, pharmacovigilance).
- Maintenance of ICT hardware and software.
- User support and cybersecurity training.
- Protection of sensitive regulatory data.
- Website and portal management for stakeholder communication.

4.2 Process for Data Backup and Archiving (VMD/SOP/ICTD/001/DB)

Source: Regulatory, Pharmacovigilance, Inspection, Finance, HR, Supply Chain Management.
Required Inputs/Resources:

- Backup media (external hard drives, cloud storage).
- Regulatory databases (e.g., VMP, adverse event reports).
- ICT Officer, Senior ICT Officer.
- Secure server room.
- Budget allocations.

Expected Outputs: Real-time and archived data backups.

Receivers: VMD departments, external auditors.

Process Details:

SN	Description	Output	Responsibility	Timeline
1	Prepare backup plan for VMD systems.	Backup plan	Senior ICT Officer	Quarterly
2	Document and ratify plan; file in Backup Inventory.	Ratified plan	Manager, ICT	Quarterly
3	Perform daily incremental and weekly full backups.	Backed-up data	ICT Officer	Daily/Weekly

4	Prepare special backup plan for sensitive data (e.g., MA records) at year-end.	Special backup plan	Senior ICT Officer	Annually
5	Ratify and file special plan.	Ratified special plan	Manager, ICT	Annually
6	Archive critical data offsite.	Archived data	ICT Officer	Annually
7	Document backup media details.	Backup inventory	ICT Officer	Ongoing

Flow Diagram:

START

↓

Prepare Backup Plan (Senior ICT Officer)

↓

Ratify & File (Manager, ICT)

↓

Perform Backups (ICT Officer) → Document Media

↓

Prepare Special Backup Plan (Senior ICT Officer) → Ratify (Manager, ICT)

↓

Archive Data (ICT Officer)

↓

END

4.3 Process for Data Restoration (VMD/SOP/ICTD/001/DR)

Source: Regulatory Affairs, Pharmacovigilance, Finance.
Required Inputs/Resources:

- Backup media.
- Restoration platform (e.g., SQL server).
- ICT Officer, Senior ICT Officer.

Expected Outputs: Restored data, inspection report.

Receivers: VMD departments, auditors.

Process Details:

SN	Description	Output	Responsibility	Timeline
1	Document restoration procedure.	Restoration procedure	Senior ICT Officer	Quarterly
2	Restore backup quarterly on test server; inspect accuracy.	Inspection report	ICT Officer	Quarterly

Flow Diagram:

START

↓

Document Procedure (Senior ICT Officer)

↓

Restore Backup → Inspect (ICT Officer)

↓

Generate Report (ICT Officer)

↓

END

4.4 Process for ICT Equipment Repair (VMD/SOP/ICTD/001/ER)

Source: VMD departments.

Required Inputs/Resources:

- Faulty equipment (e.g., PCs, printers).
- ICT Officer, repair toolkit.
- Budget allocations.

Expected Outputs: Repaired equipment, inspection report.

Receivers: VMD staff.

Process Details:

SN	Description	Output	Responsibility	Timeline
1	Prepare repair responsibility matrix.	Responsibility matrix	Manager, ICT	Annually
2	Users log repair requests via Helpdesk.	Repair request	ICT Officer	As needed
3	Resolve issue within 24 hours.	Resolution status	ICT Officer	1 day
4	Escalate to vendors if unresolved; check warranty.	Resolution status	Senior ICT Officer	2 days
5	Document repairs in repairs book.	Work ticket	ICT Officer	Ongoing
6	Review repairs book; submit quarterly report.	Inspection report	Senior ICT Officer	Quarterly

Flow Diagram:

START

↓

User Logs Request (ICT Officer)

↓

Resolve Issue (ICT Officer) → Document

↓

If Unresolved → Escalate (Senior ICT Officer)

↓

Review Repairs Book (Senior ICT Officer)

↓

END

4.5 Process for ICT Equipment Maintenance (VMD/SOP/ICTD/001/EM)

Source: VMD departments.
Required Inputs/Resources:

- ICT equipment.
- ICT Officer, maintenance toolkit.
- Budget allocations.

Expected Outputs: Maintenance report.

Receivers: VMD staff.

Process Details:

SN	Description	Output	Responsibility	Timeline
1	Prepare annual maintenance schedule.	Maintenance schedule	Senior ICT Officer	Annually
2	Perform maintenance; users sign work tickets.	Work ticket	ICT Officer	Quarterly
3	Submit annual maintenance report.	Maintenance report	Senior ICT Officer	Annually

Flow Diagram:

START

↓

Prepare Schedule (Senior ICT Officer)

↓

Perform Maintenance (ICT Officer) → Sign Tickets

↓

Submit Report (Senior ICT Officer)

↓

END

4.6 Process for Updating the VMD Website (VMD/SOP/ICTD/001/WU)

Source: Regulatory Affairs, Communications.
Required Inputs/Resources:

- New content (e.g., advisories, MA updates).
- Principal ICT Officer, ICT Officer.
- Web hosting platform.

Expected Outputs: Updated website, archived documents.

Receivers: Public, stakeholders. **Process Details:**

SN	Description	Output	Responsibility	Timeline
1	Identify update need (e.g., safety alert).	Update request	Principal ICT Officer	As needed
2	Vet content for suitability.	Vetted request	Manager, ICT	1 day
3	Provide content to ICT Officer.	Vetted request	Principal ICT Officer	1 day
4	Update website; notify originator.	Updated website	ICT Officer	1 day
5	Verify content accuracy.	Acknowledgement	Originator	1 day
6	Archive documents.	Document archive	ICT Officer	Ongoing

Flow Diagram:

START

↓

Identify Need (Principal ICT Officer)

↓

Vet Content (Manager, ICT)

↓

Update Website (ICT Officer) → Notify

↓

Verify Content (Originator) → Archive (ICT Officer)

↓

END

4.7 Process for Providing Technical Specifications (VMD/SOP/ICTD/001/TS)

Source: Procurement, VMD departments.

Required Inputs/Resources:

- Specification request.
- Principal ICT Officer, ICT Officer.
- Budget approval.

Expected Outputs: Approved specifications.

Receivers: Procurement.

Process Details:

SN	Description	Output	Responsibility	Timeline
1	Receive specification request.	Request received	ICT Officer	As needed
2	Authorize preparation.	Authorized request	Principal ICT Officer	1 day
3	Prepare and verify specifications.	Specifications	ICT Officer	2 days
4	Sign and forward specifications.	Approved specifications	Principal ICT Officer	1 day

Flow Diagram:

START

↓

Receive Request (ICT Officer)

↓

Authorize (Principal ICT Officer)

↓

Prepare Specifications (ICT Officer)

↓

Sign & Forward (Principal ICT Officer)

↓

END

4.8 Process for Creating, Updating, and Deactivating User Accounts (VMD/SOP/ICTD/001/UA)

Source: VMD staff, stakeholders (e.g., veterinarians).
Required Inputs/Resources:

- Account request/clearance forms.
- Senior ICT Officer, ICT Officer.

Expected Outputs: User account actions.

Receivers: VMD staff, stakeholders.

Process Details:

SN	Description	Output	Responsibility	Timeline
1	Receive account creation request.	Request received	ICT Officer	As needed
2	Verify user validity (e.g., HR database).	User account	Senior ICT Officer	1 day
3	Update account upon request.	Updated account	ICT Officer	1 day
4	Deactivate account upon clearance.	Deactivated account	Senior ICT Officer	1 day

Flow Diagram:

START

↓

Receive Request (ICT Officer)

↓

Verify User (Senior ICT Officer)

↓

Create/Update Account (ICT Officer)

↓

If Clearance → Deactivate (Senior ICT Officer)

↓

END

4.9 Process for ICT Requirements Planning (VMD/SOP/ICTD/001/RP)

Source: VMD departments.

Required Inputs/Resources:

- ICT requirements.
- Manager, ICT, Principal ICT Officer.
- VMD Strategic Plan.

Expected Outputs: Work plan, procurement plan.

Receivers: Procurement, VMD departments.

Process Details:

SN	Description	Output	Responsibility	Timeline
1	Request department ICT requirements.	Requirements submitted	Manager, ICT	3 months prior
2	Compile work plan and budget.	Proposed work plan	Principal ICT Officer	1 month
3	Review and approve work plan.	Approved work plan	CEO, VMD	2 weeks
4	Prepare procurement plan.	Procurement plan	Principal ICT Officer	2 weeks
5	Prepare annual work plan.	Annual work plan	Manager, ICT	1 month

Flow Diagram:

START

↓

Request Requirements (Manager, ICT)

↓

Compile Work Plan (Principal ICT Officer)

↓

Approve Plan (CEO, VMD)

↓

Prepare Procurement Plan (Principal ICT Officer)

↓

Implement Work Plan (Manager, ICT)

↓

END

4.10 Process for Systems Development and Management (VMD/SOP/ICTD/001/SD)

Source: VMD departments, stakeholders.

Required Inputs/Resources:

- System requests (e.g., pharmacovigilance portal).
- Manager, ICT, Principal ICT Officer, Senior ICT Officer.
- Budget allocations.

Expected Outputs: Developed systems, TOR.

Receivers: VMD departments.

Process Details:

SN	Description	Output	Responsibility	Timeline
1	Receive/propose system request.	Request received	Manager, ICT	As needed
2	Form project team.	Project team	Principal ICT Officer	1 week
3	Conduct preliminary investigation.	Investigation report	Senior ICT Officer	2 weeks
4	Recommend acquisition method.	Recommendation	Principal ICT Officer	1 week
5	Develop TOR for in-house systems.	TOR	Senior ICT Officer	2 weeks
6	Develop system via SDLC.	Developed system	Senior ICT Officer	Varies
7	Manage in-house systems.	System updates	ICT Officer	Ongoing
8	Supervise outsourced systems per SLA.	SLA compliance	Principal ICT Officer	Ongoing

Flow Diagram:

START

↓

Receive Request (Manager, ICT)

↓

Form Team (Principal ICT Officer)

↓

Conduct Investigation (Senior ICT Officer)

↓

Recommend Method (Principal ICT Officer)

↓

Develop TOR/System (Senior ICT Officer)

↓

Manage/Supervise System (ICT Officer/Principal ICT Officer)

↓

END

4.11 Process for Securing ICT Systems (VMD/SOP/ICTD/001/SC)

Source: VMD staff, stakeholders.

Required Inputs/Resources:

- User rights forms.
- Senior ICT Officer, ICT Officer.
- Computer hardware/software.

Expected Outputs: Secured systems, access rights list.

Receivers: VMD staff.

Process Details:

SN	Description	Output	Responsibility	Timeline
1	User requests access.	Access request	ICT Officer	As needed
2	Recommend access rights.	Recommended services	HOD	1 day
3	Authorize rights.	Authorized rights	Manager, ICT	1 day
4	Assign passwords/rights.	Access rights list	Senior ICT Officer	1 day

Flow Diagram:

START

↓

User Requests Access (ICT Officer)

↓

Recommend Rights (HOD)

↓

Authorize Rights (Manager, ICT)

↓

Assign Rights (Senior ICT Officer)

↓

END

4.12 Process for Cybersecurity and Regulatory Data Protection (VMD/SOP/ICTD/001/CY)

Source: Regulatory Affairs, Pharmacovigilance.
Required Inputs/Resources:

- Firewall, antivirus, intrusion detection systems.
- Senior ICT Officer, ICT Officer.
- Secure VPN.

Expected Outputs: Secure data, cybersecurity reports.

Receivers: VMD staff, auditors.

Process Details:

SN	Description	Output	Responsibility	Timeline
1	Develop ICT security plan.	Security plan	Manager, ICT	Annually
2	Install/update security systems.	Secured systems	Senior ICT Officer	Ongoing
3	Monitor unauthorized access.	Intrusion logs	ICT Officer	Daily
4	Conduct security audits.	Audit report	Principal ICT Officer	Quarterly
5	Train staff on cybersecurity.	Trained staff	ICT Officer	Semesterly

Flow Diagram:

START

↓

Develop Plan (Manager, ICT)

↓

Install Security Systems (Senior ICT Officer)

↓

Monitor Access (ICT Officer)

↓

Conduct Audits (Principal ICT Officer)

↓

Train Staff (ICT Officer)

↓

END

4.13 Process for Change Request Management (VMD/SOP/ICTD/002/CR)

Source: VMD departments, external stakeholders (e.g., veterinarians, manufacturers), or ICT Division.

Required Inputs/Resources:

- Change Request Form (see Section 4.3).
- ICT Division staff (Manager, Principal, Senior, ICT Officer).
- Technical documentation (e.g., system specifications, SLAs).
- Budget allocations (if applicable).
- Testing environment (e.g., test server for software changes).

Expected Outputs: Approved/implemented change, change implementation report, updated system documentation.

Receivers: Requesting department/stakeholder, VMD ICT Division, auditors.

SN	Description	Output	Responsibility	Timeline
1	Submit Change Request Form via ICT Helpdesk or email.	Change Request Form	Requestor (HOD, Stakeholder, ICT Staff)	As needed
2	Log and assign CR a unique ID (e.g., VMD/CR/[YYYY]/001).	Logged CR	ICT Officer	1 day
3	Conduct initial assessment (feasibility, impact, risks).	Initial Assessment Report	ICT Officer	2 days
4	Review CR and assessment; conduct detailed impact analysis.	Impact Analysis Report	Senior ICT Officer	3 days
5	Evaluate CR for approval/rejection; consult relevant departments if needed.	Approval/Rejection Decision	Principal ICT Officer	2 days
6	Approve or reject CR; notify requestor.	Signed CR Form	Manager, ICT	1 day
7	Develop implementation plan (e.g., timeline, resources, testing).	Implementation Plan	Senior ICT Officer	3 days
8	Implement change in test environment; verify functionality.	Test Results	ICT Officer	Varies (1-5 days)
9	Deploy change in production environment; monitor performance.	Deployed Change	ICT Officer	Varies (1-3 days)

10	Document change and update system records.	Change Implementation Report	ICT Officer	2 days
11	Review implementation; file report for audit.	Finalized Report	Principal ICT Officer	2 days

Flow Diagram

START

↓

Requestor Submits Change Request Form (ICT Helpdesk/Email)

↓

ICT Officer Logs CR → Assigns Unique ID

↓

ICT Officer Conducts Initial Assessment → Produces Initial Assessment Report

↓

Senior ICT Officer Reviews CR → Conducts Impact Analysis

↓

Principal ICT Officer Evaluates CR → Recommends Approval/Rejection

↓

Manager, ICT Approves/Rejects CR → Notifies Requestor

↓

If Rejected → Notify Requestor → END

↓

If Approved → Senior ICT Officer Develops Implementation Plan

↓

ICT Officer Implements Change in Test Environment → Verifies Functionality

↓

ICT Officer Deploys Change in Production Environment → Monitors Performance

↓

ICT Officer Documents Change → Produces Implementation Report

↓

Principal ICT Officer Reviews Implementation → Files Report

↓

END

5.0 Records/Evidence/Retained Documented Information

- Backup inventory file
- Repairs book
- Maintenance file
- Specification file
- Website update file
- User accounts file
- Preliminary investigation reports
- TORs and SLAs
- Cybersecurity audit reports
- Change implementation reports.
-

6.0 Key Performance Indicators/Objectives

6.1 Indicators

- Number of backups performed.
- Number of restoration reports.
- Percentage of resolved work tickets.
- Number of website updates.
- Number of approved specifications.
- Number of accounts managed.
- Percentage of intrusion incidents mitigated.
- Number of staff trained.
- Number of change requests submitted.

6.2 Quality Objectives

Objective	Strategy	Responsibility	Resources	Timeline	KPIs
Achieve 100% successful backups for critical systems (e.g., VMP Database)	Implement daily incremental and weekly full backups, verify with automated tools	Senior ICT Officer	Backup media (cloud, NAS, offsite tapes), MIS, staff	Daily/Weekly	Success rate of backups (%), No. of backups performed
Minimize backup failures to <2% monthly	Use redundant backup systems, retry mechanisms	ICT Officer	Network monitoring tools, budget	Monthly	Failure rate (%)
Ensure 95% successful restoration tests quarterly	Conduct quarterly tests in controlled environment, verify data integrity	Senior ICT Officer	Test server, backup media, departmental input	Quarterly	Success rate of restorations (%), No. of restoration reports
Reduce average restoration time to <4 hours	Optimize restoration procedures, train staff	ICT Officer	Restoration platform (e.g., SQL server), staff	Quarterly	Average restoration duration (hrs)
Resolve 90% of repair tickets within 24 hours	Prioritize high-impact equipment, enforce vendor SLAs	Senior ICT Officer	Repair toolkit, vendor contracts, ICT Helpdesk	Ongoing	Percentage of resolved tickets (%), SLA compliance rate (%)
Minimize repeat repairs to <5%	Document repairs, analyze failure patterns	ICT Officer	Repairs book, diagnostic tools	Monthly	Repeat repair rate (%)
Achieve 100% adherence to maintenance schedule	Follow annual maintenance plan, use predictive tools	Senior ICT Officer	Maintenance toolkit, budget, staff	Quarterly	Maintenance schedule adherence (%), No. of

					maintenance reports
Reduce equipment downtime due to maintenance to <1% annually	Schedule maintenance during low-usage periods	ICT Officer	Scheduling software, staff	Annually	Downtime percentage (%)
Publish 100% of vetted website updates within 2 days	Streamline content approval, use test environment	Principal ICT Officer	Web hosting platform, ICT Helpdesk, staff	As needed	No. of website updates, Time to publish (days)
Ensure zero errors in published content	Implement stakeholder verification process	ICT Officer	Content management system, departmental input	Monthly	Error rate in updates (%)
Approve 95% of compliant specifications within 5 days	Align with [National e-Government Standards], peer review	Principal ICT Officer	Standards documentation, budget approval	Quarterly	No. of approved specifications, Approval time (days)
Reduce specification rejections to <5%	Pre-validate requests with procurement	ICT Officer	Procurement guidelines, staff	Quarterly	Rejection rate (%)
Process 100% of account actions within 2 days	Automate verification via HR/stakeholder database	Senior ICT Officer	Active Directory, ICT Helpdesk, staff	Monthly	No. of accounts managed, Processing time (days)
Achieve zero unauthorized account actions	Implement strict approval and audit processes	Senior ICT Officer	Audit logs, authentication systems	Monthly	Unauthorized action incidents (No.)

Mitigate 95% of intrusion incidents within 24 hours	Deploy IDS, firewalls, and antivirus updates	Senior ICT Officer	Security software, VPN, staff	Ongoing	Percentage of incidents mitigated (%), Response time (hrs)
Train 100% of staff on cybersecurity semiannually	Conduct interactive training sessions	ICT Officer	Training materials, trainers	Semesterly	No. of staff trained, Feedback score (1-5)
Align 100% of ICT plans with VMD Strategic Plan	Conduct departmental consultations, prioritize regulatory needs	Manager, ICT	VMD Strategic Plan, budget, staff	Annually	Plan alignment rate (%), No. of approved plans
Complete work plans within 1 month of request	Streamline planning process, use templates	Principal ICT Officer	Planning software, departmental input	Annually	Planning completion time (days)
Achieve 90% successful system deployments	Follow SDLC, test in controlled environment	Senior ICT Officer	Development tools, test environment, staff	Per project	Deployment success rate (%), No. of systems developed
Ensure 100% SLA compliance for outsourced systems	Monitor vendor performance, regular audits	Principal ICT Officer	SLAs, vendor contracts	Ongoing	SLA compliance rate (%)
Maintain zero unauthorized access incidents	Implement multi-factor authentication, role-based access	Senior ICT Officer	Authentication systems, audit logs	Ongoing	No. of unauthorized access incidents

Patch 100% of critical vulnerabilities within 48 hours	Regular vulnerability scans, automated patch management	ICT Officer	Patch management software, staff	Weekly	Patching time (hrs), Vulnerability resolution rate (%)
Process 90% of change requests within 10 days	Streamline assessment and approval workflows	Principal ICT Officer	ICT Helpdesk, staff, test environment	Ongoing	Percentage of CRs processed on time (%), Processing time (days)
Achieve 95% successful change implementations	Test changes in controlled environment, rollback plans	Senior ICT Officer	Test server, staff, documentation	Per change	Implementation success rate (%)
Minimize change-related incidents to <5%	Conduct thorough impact analysis, stakeholder consultation	Senior ICT Officer	Risk assessment tools, departmental input	Per change	No. of change-related incidents

7.0 Risk Register

Risk	Consequences	Likelihood	Consequence	Potent Risk	Mitigations	Risk Owner	Monitoring
Data storage media failure	Loss of regulatory data (e.g., VMP registrations, pharmacovigilance data)	2	2	4	Daily backups, offsite storage, redundant media	Senior ICT Officer	Continuous monitoring via backup logs
Insufficient backup capacity	Inability to store critical data	2	3	6	Regular capacity planning, cloud storage expansion	Senior ICT Officer	Quarterly review
Backup process failure	Incomplete or corrupted backups	3	3	9	Automated backup verification, retry mechanisms	ICT Officer	Daily checks
Restoration failure	Inability to recover critical data	2	3	6	Regular test restorations, multiple backup sources	Senior ICT Officer	Quarterly test reports

Data integrity issues	Restored data inaccurate or incomplete	2	3	6	Data verification with departments, checksum validation	ICT Officer	Per restoration test
Delayed repairs	Disruption of VMD operations (e.g., regulatory reporting)	3	2	6	Prioritize high-impact equipment, vendor SLAs	Senior ICT Officer	Weekly review of repairs book
Vendor non-compliance	Prolonged downtime due to poor vendor response	2	3	6	Strict SLA enforcement, backup vendors	Manager, ICT	Quarterly vendor audits
Equipment failure due to missed maintenance	System downtime, data loss	2	3	6	Adhere to maintenance schedule, predictive maintenance tools	Senior ICT Officer	Quarterly maintenance reports
Insufficient maintenance resources	Delayed or incomplete maintenance	2	2	4	Budget planning, staff training	Manager, ICT	Annual budget review

Incorrect content published	Misinformation to stakeholders (e.g., public, veterinarians)	2	3	6	Content vetting by Manager, ICT, stakeholder verification	Principal ICT Officer	Per update review
Website downtime during updates	Reduced stakeholder access	2	2	4	Schedule updates during low-traffic periods, test environment	ICT Officer	Continuous monitoring
Non-compliant specifications	Incompatible or substandard equipment/software	2	3	6	Align with [National e-Government Standards], peer review	Principal ICT Officer	Per request review
Budget overruns	Financial strain on VMD	2	2	4	Budget approval before specification finalization	Manager, ICT	Quarterly budget checks

Unauthorized account creation	Security breach, data exposure	2	4	8	Verify user validity via HR/stakeholder database	Senior ICT Officer	Continuous audit logs
Delayed deactivation	Unauthorized access by former users	3	3	9	Automate deactivation via HR integration	Senior ICT Officer	Monthly account audits
Unauthorized access	Breach of VMP/pharmacovigilance data	2	3	6	Authentication, intrusion detection systems, VPN	Senior ICT Officer	Daily monitoring of logs
Virus/malware attack	Data corruption, system disruption	3	3	9	Regular antivirus updates, restricted external devices	ICT Officer	Continuous scanning
Insufficient staff awareness	Increased vulnerability to phishing	3	2	6	Semesterly cybersecurity training	ICT Officer	Training feedback analysis
Inaccurate requirements	Misaligned ICT investments	2	3	6	Departmental consultations, strategic alignment	Manager, ICT	Annual planning review

Budget constraints	Inability to meet ICT needs	3	2	6	Prioritize critical systems, phased implementation	Manager, ICT	Quarterly budget review
System development failure	Non-functional or delayed systems	2	3	6	Use SDLC, test in controlled environment	Senior ICT Officer	Per project review
Vendor non-compliance	Substandard outsourced systems	2	3	6	Strict SLAs, regular vendor audits	Principal ICT Officer	Ongoing SLA monitoring
Weak access controls	Unauthorized data access	2	4	8	Multi-factor authentication, role-based access	Senior ICT Officer	Continuous access log review
System vulnerabilities	Exploits leading to breaches	3	3	9	Regular patch management, vulnerability scans	ICT Officer	Weekly scans
Implementation failure	System downtime, data loss	2	3	6	Test in controlled environment, rollback plans	Senior ICT Officer	Per change review

Unauthorized changes	Security breach, non-compliance	2	4	8	Strict approval process, audit logs	Principal ICT Officer	Continuous monitoring
Inadequate impact analysis	Unforeseen disruptions	3	3	9	Detailed risk assessment, stakeholder consultation	Senior ICT Officer	Per change request
Resource constraints	Delayed implementation	3	2	6	Budget planning, vendor SLAs	Manager, ICT	Quarterly resource review

8.0 Opportunities Register

S/N	Opportunities	Action Plan	Timeline	Effectiveness Status
1	Enhanced data redundancy	Implement hybrid backup (cloud + offsite) for critical systems (e.g., VMP Database)	Q4 2025	80% (Planning phase)
2	Automated backup monitoring	Deploy AI-based tools for real-time backup verification	Annual	70% (Tool evaluation)
3	Faster restoration times	Upgrade test server hardware for quicker restoration tests	Q1 2026	75% (Budget approval pending)
4	Improved data integrity checks	Integrate automated checksum validation in restoration process	Semesterly	85% (Pilot testing)
5	Reduced repair downtime	Establish in-house repair capabilities for common issues (e.g., printers)	Annual	80% (Staff training initiated)
6	Stronger vendor partnerships	Negotiate long-term SLAs with reliable vendors	Q4 2025	70% (Vendor shortlisting)
7	Predictive maintenance	Adopt IoT-based monitoring for equipment health	Q2 2026	65% (Research phase)
8	Extended equipment lifespan	Implement proactive maintenance schedules	Annual	90% (Schedule implemented)
9	Enhanced stakeholder access	Develop mobile-responsive VMP submission portal	Annual	90% (Beta testing)
10	Real-time advisories	Enable push notifications for safety alerts	Q1 2026	75% (Feature design)
11	Streamlined procurement	Create a digital specification template library	Q4 2025	80% (Template drafting)

12	Cost optimization	Evaluate open-source alternatives for ICT purchases	Semesterly	70% (Cost analysis)
13	Automated account management	Integrate with HR system for real-time account updates	Q2 2026	75% (System integration planning)
14	Enhanced user experience	Implement single sign-on (SSO) for VMD systems	Annual	80% (SSO pilot)
15	Advanced threat detection	Deploy AI-driven intrusion detection systems	Q1 2026	70% (Vendor evaluation)
16	Improved staff compliance	Gamify cybersecurity training for higher engagement	Semesterly	85% (Training module developed)
17	Strategic ICT alignment	Link ICT plans to WOAH global standards	Annual	80% (Consultation with WOAH)
18	Resource optimization	Use predictive analytics for budget forecasting	Q4 2025	75% (Analytics tool selection)
19	Agile development	Adopt agile methodologies for faster system delivery	Q2 2026	70% (Staff training on agile)
20	Global interoperability	Integrate VMD systems with international regulatory databases	Annual	80% (API development)
21	Zero-trust security model	Implement zero-trust architecture for critical systems	Q1 2026	65% (Architecture design)
22	Proactive vulnerability management	Automate vulnerability scanning and patching	Semesterly	85% (Automation tools deployed)
23	Automated change tracking	Integrate CR module in ICT Helpdesk	Q4 2025	70% (Module development)
24	Improved change efficiency	Use AI to predict change impacts	Q2 2026	60% (AI tool research)

25	Enhanced staff proficiency	Conduct annual change management training	Annual	85% (Training schedule set)

9. Reporting Templates

1. Backup Report Template
Title: Backup Activity Report
Period: [Month/Year]

Date	System/Server	Type of Backup (Daily/Weekly/Monthly)	Backup Location (Local/Cloud)	Status (Success/Failed)	Remarks
01/07/2025	ERP Database	Daily	Local NAS	Success	
02/07/2025	Email Server	Daily	Cloud Storage	Success	

Total Backups Performed: [Number]
Total Successful Backups: [Number]
Success Rate: [Number]%

2. Data Restoration Report Template
Title: Restoration Test Report
Period: [Quarter/Year]

Date	System Restored	Backup Source (Date/Location)	Test Result (Pass/Fail)	Duration (hrs)	Data Integrity (Verified / Not Verified)	Remarks
05/07/2025	ERP Database	01/07/2025 / Cloud Storage	Pass	3	Verified	

Total Restorations Performed: [Number]
Total Successful Restorations: [Number]
Success Rate: [Number]%

3. ICT Support Work Ticket Resolution Report
Title: ICT Support Ticket Resolution Rate
Period: [Month/Year]

Ticket ID	Date Logged	User Department	Issue Description	Status (Resolved/Unresolved)	Resolution Date	SLA Met (Yes/No)	Remarks
ICT-124	02/07/2025	Finance	Printer not responding	Resolved	02/07/2025	Yes	

Total Tickets Logged: [Number]
Total Tickets Resolved: [Number]
Percentage Resolved: (Resolved ÷ Logged) × 100 = [XX%]

4. Website Update Report
Title: Website and Portal Updates
Period: [Month/Year]

Date	Section/Page Updated	Type of Update (Content/Design/Feature)	Approved By	Status	Remarks
04/07/2025	Home Page	Content (News)	ICT Manager	Done	

Total Updates Performed: [Number]
Total Published: [Number]
Total Archived: [Number]

5. Approved ICT Specifications Report
Title: ICT Technical Specifications Approvals
Period: [Month/Year]

Date	Department	Item Requested	Prepared By	Approved By	Remarks
03/07/2025	Procurement	Laptops (10 Units)	ICT Officer	ICT Manager	

Total Specifications Approved: [Number]
Total Specifications Rejected: [Number]

6. User Account Management Report
Title: User Accounts Creation/Updates/Deactivation
Period: [Month/Year]

Date	Username	Account Type (Email/ERP/Portal)	Action (Created/Updated/Deactivated)	Approved By	Remarks
05/07/2025	J. Mwangi	Email	Created	ICT Manager	

Total Accounts Created: [Number]
Total Accounts Updated: [Number]
Total Accounts Deactivated: [Number]
Total Accounts Managed: [Number]

7. Intrusion Incident Mitigation Report
Title: ICT Security Incident Report
Period: [Month/Year]

Date	Incident Description	Detected By (System/User)	Mitigation Action	Resolved (Yes/No)	Remarks
02/07/2025	Suspicious Login	IDS	Password Reset	Yes	

Total Intrusion Attempts: [Number]
Total Incidents Mitigated: [Number]
Percentage Mitigated: (Mitigated ÷ Total) × 100 = [XX%]

8. ICT Training Report
Title: Staff Training Report
Period: [Month/Year]

Date	Training Topic	Target Group	No. of Staff Trained	Trainer Name	Remarks
10/07/2025	Cybersecurity Awareness	All Staff	25	ICT Officer	

Total Staff Trained: [Number]

9. Title: ICT Change Request Management Report
Period: [Month/Year]

Date	Change Description	Requested By (Dept/User)	Approved By (ICT/Management)	Implementation Action	Status (Completed/Pending)	Remarks
02/07/2025	Upgrade of ERP Database	Finance Department	ICT Manager	Applied Database Patch	Completed	

Total Change Requests: [Number]
Total Implemented Changes: [Number]
Percentage Implemented: (Implemented ÷ Total) × 100 = [XX%]