ICT POLICY MANUAL

2025-2026

Matjhabeng Local Municipality

ICT Policy Manual

2025–2026

Abstract

This compilation outlines the ICT governance framework, operational policies, and strategic controls for managing Matjhabeng Local Municipality's Information and Communication Technology environment. It ensures the alignment of all ICT operations with applicable regulations, including MFMA, POPIA, ISO 27001, and COBIT, supporting the Municipality's service delivery objectives through secure and efficient digital systems.

Table of Contents

ICT Acceptable Use Policy (AUP)

1. Introduction

1.1 Purpose

The ICT Acceptable Use Policy outlines the standards and responsibilities for acceptable use of Information and Communication Technology (ICT) resources provided by Matjhabeng Local Municipality (MLM). It aims to ensure ICT assets are used effectively, ethically, legally, and securely to support municipal operations, service delivery, and governance.

1.2 Scope

This policy applies to all users, including permanent employees, contract employees, elected officials, temporary staff, consultants, volunteers, interns, and any other individuals who utilize MLM's ICT resources, systems, networks, applications, or data, regardless of location or device.

2. Authorized Use of ICT Resources

2.1 Permitted Use

- MLM ICT resources, including computers, mobile devices, software applications, internet, and email, must be primarily used for municipal business activities.
- Access to ICT resources shall be granted based on business roles, with user accounts, privileges, and permissions managed centrally by the ICT Department.

2.2 Prohibited Use

Users must NOT:

- Engage in unauthorized use of ICT resources for personal commercial purposes, profit-making, or political campaigns.
- Install unauthorized software, hardware, or services on municipal equipment or networks.
- Attempt to bypass security measures or gain unauthorized access to data, systems, or networks.
- Use ICT resources for any illegal activities or activities violating municipal policies or laws.
- Provide any external parties unauthorised usage or access to the municipality's ICT resources.

3. Security and Data Protection

3.1 User Responsibilities

All users must:

- Keep passwords confidential, secure their user accounts, and immediately report any security incidents or suspected breaches to the ICT Department.
- Regularly update passwords and follow all prescribed ICT security protocols.
- Ensure municipal data and information are adequately protected, especially sensitive or personally identifiable information, complying with relevant laws (e.g., POPIA).
- Adhere to access control mechanisms, password policies, and other security measures to protect ICT resources from unauthorized access and misuse.

3.2 Data Storage and Handling

- Users must store municipal data only on approved network storage and systems provided by the ICT Department.
- Removable media (USB drives, external drives, etc.) must be encrypted, virus-scanned, and approved by the ICT Department before use.
- Users must not transmit sensitive municipal data to unauthorized individuals or external services.

4. Email, Internet, and Social Media Usage

4.1 Email

- Official business communications must use only MLM-approved email accounts.
- Users shall not send unsolicited, spam, defamatory, discriminatory, or inappropriate emails.
- MLM retains the right to archive, monitor, and audit email communications.

4.2 Internet

- Internet usage is permitted primarily for municipal-related activities.
- Accessing illegal, offensive, inappropriate, or adult-content websites is strictly prohibited.
- Downloading unauthorized software, files, or materials that could harm MLM's ICT infrastructure is prohibited.

4.3 Social Media

- Access to social media platforms through MLM resources is permitted solely for official municipal purposes and must be authorized by relevant management.
- Users must not post confidential, inappropriate, defamatory, discriminatory, or harmful content about MLM or associated stakeholders.

5. Personal Use of ICT Resources

- Limited personal use of municipal ICT resources is permitted, provided it:
    - Does not interfere with official duties or service delivery.
    - Occurs during personal breaks and does not incur additional costs or security risks to the municipality.
    - Complies fully with all other aspects of this policy.

6. Privacy Expectations and Monitoring

- Users should not expect personal privacy when utilizing municipal ICT resources.
- MLM retains the right to monitor, audit, review, and access any data, files, communications, and activities on municipal ICT systems and networks.

- Users are reminded that all information and communications on MLM ICT systems may be subject to public disclosure under applicable laws (e.g., Promotion of Access to Information Act).
- For security and network maintenance purposes, the Head of ICT Department and any other personnel authorized may monitor equipment, systems, and network traffic at any time. MLM reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

7. Prohibited Behaviours and Content

Users must strictly refrain from:

- Engaging in activities that violate intellectual property rights or copyrights.
- Using ICT resources to harass, bully, discriminate, or engage in any form of hate speech or offensive behaviour.
- Accessing, distributing, or storing obscene, pornographic, offensive, or discriminatory material.
- Performing activities intended to disrupt the integrity or availability of ICT systems or networks.

8. Enforcement and Consequences

- Any breach or non-compliance with this policy shall result in disciplinary action, which may include warnings, suspension, termination of employment or contract, revocation of ICT privileges, or legal action, depending on the severity of the violation.
- Users are required to sign a written or electronic acknowledgment of this policy before receiving access to MLM's ICT resources.

9. Training and Awareness

- MLM commits to regular awareness sessions and training programs regarding ICT acceptable use and cybersecurity practices.
- All employees and relevant stakeholders will periodically receive updates and training on this policy.

10. Policy Review and Updates

- This ICT Acceptable Use Policy will be reviewed annually or as required by regulatory changes or ICT developments.

- Updates will be communicated to all users, who must acknowledge understanding and compliance.

11. Acknowledgment and Acceptance

I have read, understood, and agree to comply fully with Matjhabeng Local Municipality's ICT Acceptable Use Policy as outlined above.

Signature: _____

Name: _____

Date: _____

Approved by:

ICT Manager: _____ (Signature & Date)

Senior Manager ICT: _____ (Signature & Date)

Municipal Manager: _____ (Signature & Date)

ICT End User Access Management Policy

1. Introduction

1.1 Purpose

The ICT End User Access Management Policy establishes controls and procedures for managing and governing user access to Matjhabeng Local Municipality's (MLM) ICT resources and information systems. It ensures the principles of least privilege, segregation of duties, and secure management of user identities and authorizations.

1.2 Scope

This policy applies to all MLM employees, contractors, temporary staff, elected officials, consultants, volunteers, interns, and third-party partners requiring access to municipal ICT systems, networks, data, and resources.
Systems covered include:

- Microsoft Active Directory and Azure Active Directory
- Online Microsoft Exchange
- Cisco Meraki Network Infrastructure
- Solar ERP System (integrated with Active Directory)
- Payday Payroll System
- Cashdrawer Paypoint System
- GlobalProtect VPN System
- Palo Alto Firewall

2. Policy Principles

The following principles guide access management at MLM:

- **Least Privilege:** Users receive only the minimum level of access necessary to perform their job functions.
- **Need-to-Know:** Information and system access are granted based strictly on business needs and justified job roles.
- **Segregation of Duties:** Critical functions and privileges are separated to prevent conflicts of interest and reduce risk.
- **Accountability:** All access must be traceable and auditable, with individual accountability enforced through unique user credentials.

3. User Account Management

3.1 Account Creation and Authorization

- New accounts must be formally requested using the standard User Access Request Form and authorized by the relevant manager or department head.

- ICT department personnel shall be solely responsible for creating, configuring, and provisioning user accounts in:
    - Microsoft Active Directory/Azure AD
    - Exchange Online
    - Solar ERP
    - Payday Payroll System
    - Cashdrawer Paypoint System
    - GlobalProtect VPN

3.2 User Account Naming Convention

- MLM shall adhere to a standardized naming convention format (e.g., first name and surname: katleho.rampheng@matjhabeng.gov.za) across all directory services and integrated systems.

3.3 Access Modifications

- Changes to user access levels require formal authorization documented and approved by the relevant business unit manager and must be logged and retained.
- Access reviews and modifications shall be executed by the ICT Department exclusively.

3.4 Account Disabling and Deletion

- User accounts shall be disabled immediately upon termination, resignation, or the end of contractual agreements.
- After 30 days, disabled accounts must be deleted unless otherwise documented and approved for longer retention.

4. Privileged Access Management

4.1 Privileged Accounts

- Privileged access (domain administrators, network administrators, ERP system administrators, payroll system administrators) shall be strictly controlled, documented, and reviewed monthly.

- Privileged access to Palo Alto Firewall and Cisco Meraki infrastructure shall be limited to authorized ICT network staff only, following documented authorization procedures.

4.2 Segregation of Privileges

- ICT administrative duties must be segregated between system/network administration and application management roles, where feasible, particularly between Solar ERP and Payday Payroll System access management.

5. Password and Authentication Standards

5.1 Password Management

- Passwords must adhere to complexity and length requirements:
  - Minimum of 12 characters.
  - Combination of upper-case letters, lower-case letters, numbers, and special characters.
- Password changes are enforced every 90 days via Active Directory and Azure AD.

5.2 Multi-Factor Authentication (MFA)

- MFA is mandatory for:
  - All remote access via GlobalProtect VPN.
  - Administrator-level accounts across Azure AD, Exchange Online, Palo Alto Firewall, and Cisco Meraki Dashboard, Entrust Certificate Service Portal.
- MFA methods include authenticator applications, SMS codes, or hardware tokens.

6. Remote and External Access Controls

6.1 Remote Access

- Remote access shall occur only through MLM-approved VPN (GlobalProtect) and must utilize secure encryption methods and MFA.
- Remote sessions must time out after 30 minutes of inactivity.

6.2 External Vendor Access

- Third-party access to MLM systems requires explicit authorization, documented purpose, and limited duration.
- External access is monitored, logged, and reviewed monthly.

7. Role-Based Access Control (RBAC)

7.1 RBAC Implementation

MLM ICT Department shall define and maintain role-based access control structures clearly defining permissions for roles such as finance, HR, IT administrators, cashiers, payroll administrators, and managers.

- Solar ERP, Payday Payroll System, and Cashdrawer systems shall utilize RBAC integrated with Active Directory groups for seamless access management.

7.2 Periodic Access Reviews

- ICT Department shall conduct quarterly reviews of RBAC allocations, permissions, and user activities, documenting findings and adjustments.

7.3 Least Privilege Principle:

- User access rights shall be assigned based on predefined roles and responsibilities within the organization.
- Access permissions shall be reviewed periodically to identify and revoke unnecessary privileges.

8. Access Auditing and Monitoring

8.1 Monitoring and Logging

- Access to municipal ICT resources shall be logged and monitored via:
    - Azure AD/Active Directory audit logs.
    - Cisco Meraki security dashboard.
    - Palo Alto Firewall logging and alerting.
    - Solar ERP, Payday Payroll System, and Cashdrawer system logs.

- ICT shall proactively monitor and investigate any suspicious activities or anomalies.

8.2 Audit Trails

- User access logs must be securely retained for at least one year and be accessible for forensic investigations or compliance audits as necessary.

9. Incident Management and Response

- Any suspected unauthorized access or breach must be immediately reported to ICT's Information Security Officer and Manager: ICT.
- Security incidents shall be investigated promptly with documented findings and appropriate corrective actions.

10. Training and Awareness

- Regular user awareness training on access management and information security responsibilities shall be conducted annually.
- Privileged users must receive specialized training in administrative security and best practices.

11. Enforcement and Compliance

- Violations of this policy may result in disciplinary measures including warnings, suspension, termination of employment, revocation of access privileges, and potential legal actions.

12. Policy Review and Maintenance

- This policy shall be reviewed annually or as required by changes in technology, legislation, or municipal requirements.
- Updates to the policy shall be communicated formally to all stakeholders.

13. User Acknowledgment

By signing below, users acknowledge they have read, understood, and agree to adhere strictly to this ICT End User Access Management Policy.

Username: _____

Signature:_____

Date: _____

ICT Assets Control and Disposal Policy

1. Introduction

1.1 Purpose

This policy outlines the procedures for managing ICT assets throughout their lifecycle, from acquisition and use to eventual disposal. It ensures that Matjhabeng Local Municipality (MLM) ICT assets are effectively managed, safeguarded, and disposed of securely and in compliance with relevant regulations and standards.

1.2 Scope

This policy applies to all ICT assets owned or managed by MLM, including:

- Computers (desktops, laptops, tablets)
- Mobile devices (smartphones, cellular modems)
- Network equipment (switches, routers, wireless access points, firewalls)
- Printers, scanners, copiers
- Software licenses and subscriptions
- Storage media (hard drives, USB devices)
- Servers and infrastructure equipment

2. Policy Principles

- **Asset Lifecycle Management:** All ICT assets must be tracked from acquisition to disposal.
- **Responsibility and Accountability:** Clear roles and responsibilities for asset management.

- **Security and Confidentiality:** Protection of municipal data during asset disposal.
- **Compliance and Sustainability:** Adherence to laws, environmental sustainability, and audit requirements.

3. Roles and Responsibilities

3.1 ICT Department

- Maintains central ICT Asset Register.
- Manages the allocation and retrieval of ICT assets.
- Ensures assets are disposed of securely, ethically, and sustainably.

3.2 Managers and Supervisors

- Approve asset requests for their departments.
- Ensure assets allocated to their employees are returned upon termination or transfer.

3.3 Employees (End Users)

- Protect and use assets responsibly.
- Promptly report lost, damaged, or stolen assets to ICT.

4. Asset Management Procedures

4.1 Asset Acquisition and Registration

- All ICT assets must be purchased following MLM's approved procurement procedures.
- Upon delivery, the ICT Department must register each asset into the ICT Asset Register, including:
    - Asset Tag (unique identifier)
    - Serial Number
    - Asset Description
    - Assigned User or Location
    - Acquisition Date and Cost

4.2 Asset Allocation

- Assets are allocated based on departmental and operational requirements.
- ICT Department records all allocations and updates the Asset Register accordingly.

4.3 Asset Transfers

- Transfers between departments must be recorded and approved by department heads and ICT Department.

5. Asset Security and Risk Management

- All mobile ICT devices must be physically secured when not in use.
- Users must immediately report lost or stolen assets to ICT for action, including remote wiping if applicable.
- ICT Department conducts periodic audits and physical inventory checks annually.

6. Asset Disposal Procedures

6.1 Conditions for Disposal

ICT assets are eligible for disposal if they are:

- Obsolete or technologically outdated.
- Damaged beyond economical repair.
- No longer required operationally.

6.2 Disposal Methods

- Disposal methods include donation, recycling, sale, or destruction.
- Secure erasure or destruction of storage media is mandatory, verified by ICT Department.

6.3 Disposal Process

- ICT Department identifies assets for disposal and completes an **Asset Disposal Form**.
- Approval from Senior ICT Management is required before disposal.

- Assets containing sensitive data require secure data wiping using certified data erasure tools or physical destruction (shredding, crushing).
- ICT Department updates Asset Register accordingly.
- Data destruction processes shall be documented and verified to ensure compliance with privacy and security regulations.

6.4 Environmental and Regulatory Compliance

- All disposals must comply with environmental laws (National Environmental Management Act).
- Proper disposal certificates must be obtained from approved disposal vendors.
- ICT assets containing hazardous materials or electronic waste must be disposed of in compliance with environmental regulations and industry nest practices.

7. Documentation and Records Management

- Records of asset lifecycle (acquisition, allocation, disposal) must be securely maintained for audit and regulatory purposes.
- Disposal certificates and data wiping confirmations must be stored for at least five years.

8. Compliance and Enforcement

- Non-compliance with this policy may result in disciplinary actions, including written warnings, asset use suspension, or termination.

9. Monitoring and Review

- Regular asset audits are conducted annually.
- This policy shall be reviewed at least every two years or as required due to legislative changes or operational needs.

10. User Acknowledgment

All users receiving ICT assets must acknowledge this policy.

Acknowledgment:

I acknowledge receipt and agree to comply with the ICT Assets Control and Disposal Policy.

Name: _____

Signature: _____

Date: _____

ICT Backup and Disaster Recovery Policy

1. Introduction

1.1 Purpose

The ICT Backup and Disaster Recovery Policy provides guidelines for the backup, storage, recovery, and continuity of data and critical systems for the Matjhabeng Local Municipality (MLM). It ensures municipal operations can recover swiftly and effectively from data loss, system failures, or disasters.

1.2 Scope

This policy applies to all ICT systems and data managed by MLM, including but not limited to:

- Microsoft Active Directory and Azure Active Directory
- Microsoft Exchange Online
- Solar ERP System
- Payday Payroll System
- Cashdrawer Paypoint System
- File servers and shared drives
- Network infrastructure configurations (Cisco Meraki)
- Firewall and VPN configurations (Palo Alto Firewall, GlobalProtect VPN)

2. Policy Principles

- **Reliability and Continuity:** Ensure rapid restoration of municipal data and systems after incidents.
- **Data Integrity:** Secure and reliable backup processes that guarantee data accuracy.
- **Compliance and Auditability:** Maintain records and procedures aligned with regulations, including MFMA and POPIA.
- **Responsibility and Accountability:** Clear roles and responsibilities for backup and disaster recovery management.

3. Roles and Responsibilities

3.1 ICT Department

- Ensures regular backups of data and critical systems.
- Manages and periodically tests Disaster Recovery (DR) plans.
- Coordinates data restoration during incidents.
- Minimizes downtime and maintains operational continuity.

3.2 Departmental Managers

- Identify critical data and systems within their departments for inclusion in backup and DR procedures.
- Support recovery operations in incidents.

3.3 Employees (End Users)

- Store all critical work files on designated shared drives or municipal cloud storage (OneDrive/SharePoint).

4. Backup Procedures

4.1 Backup Types

- **Full Backups:** Weekly (every weekend).
- **Incremental Backups:** Daily (every evening).

4.2 Critical Systems Backups

Regular backup schedules must be maintained for:

System	Backup Frequency	Backup Method	Retention Period
Active Directory / Azure AD	Daily Incremental, Weekly Full	Cloud & Local storage	6 months
Exchange Online (Email)	Continuous incremental, weekly full	Cloud storage	1 year
Solar ERP	Daily Incremental, Weekly Full	Local & offsite cloud	1 year
Payday Payroll	Daily Incremental, Weekly Full	Local & offsite cloud	1 year
Cashdrawer System	Daily Incremental, Weekly Full	Local & offsite cloud	1 year
Shared drives & File servers	Daily Incremental, Weekly Full	Local & offsite cloud	6 months
Palo Alto Firewall & Cisco Meraki configurations	Weekly	Local & cloud storage	6 months

4.3 Backup Storage and Security

- Backups must be encrypted and securely stored both locally and off-site (cloud-based or disaster recovery site).
- Access to backup data is restricted to authorized ICT personnel only.

4.4 Recovery of Backup Data:

- Backup documentation must be maintained, reviewed and updated periodically to account for new technology, business changes, and migration of applications to alternative platforms. This includes, but not limited to:
    - Identification of critical data and systems.

    - Documentation and support items necessary to perform essential tasks during a recovery process.
- Documentation of the restoration process must include:
    - Procedures for the recovery of data or systems.
    - Provision for key management should the data be encrypted.

5. Disaster Recovery (DR) Procedures

5.1 DR Plan Elements

MLM maintains a comprehensive Disaster Recovery Plan including:

- Identification and classification of critical systems.
- Clear recovery procedures for each system.
- Roles and responsibilities for DR execution.
- Communication plan during recovery events.

5.2 Recovery Objectives

- **Recovery Time Objective (RTO):**
    - Critical systems (ERP, Payroll, Email): Maximum 4 hours
    - Non-critical systems: Maximum 12-24 hours
- **Recovery Point Objective (RPO):**
    - Critical data: Maximum data loss of 4 hours

5.3 DR Testing

- DR plans shall be tested semi-annually, documented thoroughly, and any identified gaps resolved promptly.

5.4 DR Site and Cloud Backup

- MLM utilizes cloud storage (Azure Cloud or approved cloud vendor) as primary offsite DR storage.
- A secondary offsite DR site is identified and maintained for critical systems continuity.

6. Incident Response and Data Restoration

- In the event of data loss or system disruption, the ICT Manager must be informed immediately.
- Authorized ICT personnel manage the restoration process following documented recovery procedures.
- Restoration priority order:
    1. Active Directory / Azure AD
    2. Network connectivity (Meraki, Palo Alto)
    3. Email (Exchange Online)
    4. Solar ERP System
    5. Payday Payroll System
    6. Cashdrawer Paypoint System
    7. File Servers and Shared Drives

7. Compliance and Enforcement

- ICT Department maintains backup and recovery logs for audit and compliance purposes.
- Non-compliance with backup processes or negligence causing data loss may result in disciplinary action.

8. Monitoring and Review

- ICT Department monitors daily backup reports and resolves failures immediately.
- Quarterly reviews of backup and recovery effectiveness are conducted and documented.

9. User Training and Awareness

- Regular awareness training on data backup best practices provided annually.
- Training provided to ICT personnel involved in DR procedures semi-annually.

10. Policy Review

- Reviewed annually or as technology or regulations change.

11. User Acknowledgment

Acknowledgment of understanding and compliance by all ICT personnel.

Name:_____

Signature:_____

Date: _____

Policy Approvals:

ICT Manager: _____

Senior ICT Manager: _____

Municipal Manager: _____

ICT Change Management Policy

Matjhabeng Local Municipality

Policy Version: 1.0

Date: [Insert Date]

Next Review Date: [Insert Review Date]

1. Introduction

1.1 Purpose

This ICT Change Management Policy defines the process to manage all changes made to the ICT environment at Matjhabeng Local Municipality (MLM). It ensures that changes are systematically planned, approved, tested, communicated, and documented to minimize service disruptions and risks.

1.2 Scope

This policy applies to all ICT changes affecting MLM's production systems, networks, infrastructure, software, and applications, including:

- Microsoft Active Directory and Azure AD

- Exchange Online
- Solar ERP System
- Payday Payroll System
- Cashdrawer Paypoint System
- Network Infrastructure (Cisco Meraki)
- Firewall and VPN configurations (Palo Alto Firewall, GlobalProtect VPN)
- Servers, databases, and operating systems

2. Policy Principles

- **Risk Minimization:** All ICT changes must undergo thorough risk assessment.
- **Transparency and Accountability:** Changes must be documented, approved, and auditable.
- **Standardization:** Consistent methods for proposing, reviewing, authorizing, and implementing ICT changes.
- **Communication:** Clear notification and communication procedures for all stakeholders affected by changes.

3. Roles and Responsibilities

3.1 ICT Change Advisory Board (CAB)

- Reviews and approves proposed ICT changes.
- Ensures adherence to policy and procedure compliance.
- Consists of ICT management and relevant department heads.

3.2 ICT Manager

- Ensures proper implementation and monitoring of the policy.
- Coordinates change approval and communication.

3.3 ICT Staff

- Submits detailed change requests.
- Executes approved changes following documented procedures.

3.4 Users and Department Managers

- Assess impact of proposed changes on business operations.
- Provide feedback on implemented changes.

4. Change Management Procedures

4.1 Change Request Submission

All ICT changes require formal submission through a standardized **ICT Change Request Form**, detailing:

- Purpose and justification of the change
- Impact and risk assessment
- Proposed implementation plan and timeline
- Rollback procedures

4.2 Classification of Changes

- **Standard Changes:** Routine, low-risk, pre-approved (e.g., minor software updates).
- **Normal Changes:** Require CAB approval (e.g., system upgrades, firewall changes).
- **Emergency Changes:** Critical security or stability risks; immediate but documented and retrospectively reviewed by CAB.

5. Change Approval Process

5.1 Change Advisory Board (CAB)

- Reviews submitted change requests weekly.
- Approves, defers, or rejects changes based on risk assessment and business needs.

5.2 Emergency Changes

- Emergency changes require immediate approval by ICT Manager or Senior Manager ICT.
- Documented post-implementation review by CAB required within 48 hours.

6. Change Implementation

- Only authorized and trained ICT personnel implement approved changes.
- Changes should occur during scheduled maintenance windows unless emergency conditions exist.
- All implementations require detailed documentation, testing, and validation.

7. Testing and Validation

- Changes must undergo testing in a controlled (non-production) environment before production deployment.
- Approval of test results by relevant system owners required prior to full deployment.

8. Communication Procedures

- ICT Department communicates planned changes to affected stakeholders at least 48 hours in advance (except emergency changes).
- Communications include nature of the change, expected impact, implementation date/time, and contact information for queries.

9. Documentation and Record-Keeping

- ICT Department maintains detailed records of all changes, approvals, test results, implementation logs, and rollback actions for auditing.
- Records are retained for at least five years.

10. Post-Implementation Review (PIR)

- Conducted after all Normal and Emergency changes to assess effectiveness, identify issues, and confirm system stability.
- Results documented and reviewed by CAB within seven days post-change.

11. Compliance and Enforcement

- Non-compliance with this policy may result in disciplinary action.
- Continuous non-compliance can lead to revocation of change implementation privileges.

12. Monitoring and Review

- Quarterly reviews of the change management effectiveness by ICT management.
- Annual review of this policy to accommodate emerging technologies and regulations.

13. User Training and Awareness

- Annual training sessions provided to ICT staff and relevant stakeholders on change management procedures.

14. User Acknowledgment

All ICT staff involved in changes must acknowledge this policy.

Acknowledgment:
I have read, understood, and agree to comply with the ICT Change Management Policy.

Name:_____
Signature:_____
Date: _____

Policy Approvals:

ICT Manager: _____

Senior ICT Manager: _____

Municipal Manager: _____

ICT Password Management Policy

1. Introduction

1.1 Purpose

This policy establishes password creation, use, and management requirements to protect the confidentiality, integrity, and availability of Matjhabeng Local Municipality's (MLM) ICT systems and data.

1.2 Scope

This policy applies to all users—including employees, contractors, vendors, and third parties—who access MLM's ICT systems, including but not limited to:

- Microsoft Active Directory and Azure AD
- Microsoft Exchange Online
- Solar ERP System
- Payday Payroll System
- Cashdrawer Paypoint System
- VPN (GlobalProtect)
- Network Equipment (Cisco Meraki)
- Firewall Systems (Palo Alto)

2. Policy Principles

- **Security:** Passwords are a critical first line of defense for ICT assets.
- **Accountability:** Each user is responsible for the security of their credentials.
- **Compliance:** Aligns with POPIA, ISO 27001, and Microsoft cybersecurity best practices.

3. Password Requirements

3.1 General Password Rules

All user and administrative accounts must follow these minimum requirements:

- Minimum length: 12 characters
- At least one uppercase letter
- At least one lowercase letter
- At least one number
- At least one special character (!@#$%^&*)
- Must not contain the user's name, username, or ID
- Must not be identical to any of the previous **5** passwords

3.2 Account Types and Specific Rules

Account Type	Password Expiry	Multi-Factor Authentication (MFA)	Additional Notes
Standard User Accounts	30 days	Required for remote access	Azure/AD-integrated
Administrator Accounts	45 days	Mandatory	Must use password vault
System/Service Accounts	180 days	Not applicable (but strong complexity required)	Access reviewed quarterly

4. Multi-Factor Authentication (MFA)

MFA must be enabled for the following systems:

- Azure AD and Exchange Online
- VPN access via GlobalProtect
- Firewall and Meraki Dashboard Access
- Administrative access to ERP, Payroll, and Server environments
- Entrust Certificate Service Portal

  MFA may use Microsoft Authenticator, SMS codes, or security tokens.

5. Password Storage and Sharing

- Passwords must **never be written down**, emailed, or stored in unencrypted text.
- Use of **approved password managers or vaults** (e.g., Microsoft Defender for Identity, Entra, or a secure internal vault) is mandatory for privileged accounts.
- Passwords may not be shared under any circumstances, including among ICT staff. Shared or group accounts are discouraged and must be reviewed with justification.

6. Forgotten or Compromised Passwords

6.1 Reset Requests

- Users must contact ICT Helpdesk via official channels to reset forgotten passwords.
- Identity verification (employee number, ID, or manager confirmation) is required.

6.2 Compromised Accounts

- Any suspected password compromise must be reported **immediately**.
- ICT will reset the account, review access logs, and notify the Information Security Officer for incident handling.

7. Password Change Triggers

Users must change their password immediately if:

- They suspect their credentials have been compromised.
- There is evidence of unauthorized access.
- ICT has issued a reset as part of a security response.

8. Password Policy Enforcement

- Automated password policies must be enforced via Group Policy Objects (GPOs) in Active Directory and through Microsoft Azure security baselines.
- Systems that do not support centralized policy enforcement must be audited monthly.

9. Roles and Responsibilities

Role	Responsibility
ICT Department	Enforce password policy, conduct password audits, provide secure reset mechanisms
End Users	Create and maintain strong passwords, report any compromise
System Owners	Ensure password protection for their respective systems
Information Security Officer	Investigate security incidents involving credential misuse

10. Monitoring and Review

- Quarterly password audit logs reviewed for policy adherence.
- Annual policy review or upon introduction of new systems/risks.

11. Training and Awareness

- Mandatory user training during onboarding and annually on password hygiene.
- Periodic reminders via email and municipal intranet on strong password practices.

12. Non-Compliance and Disciplinary Action

- Users found violating this policy (e.g., sharing passwords, using weak or repeated passwords) will face disciplinary action which may include access revocation, written warnings, or further sanctions in line with the municipality's HR policies.

13. User Acknowledgment

I acknowledge that I have read, understood, and will comply with the MLM ICT Password Management Policy.

Name:_____

Signature:_____

Date: _____

Policy Approvals:

ICT Manager: _____

Senior ICT Manager: _____

Municipal Manager: _____

ICT Patch Management Policy

1. Introduction

1.1 Purpose

This policy provides a structured and consistent approach for the management and application of software patches and updates across Matjhabeng Local Municipality's (MLM) ICT environment. It aims to reduce the risk of vulnerabilities, improve system stability, and ensure compliance with security standards.

1.2 Scope

This policy applies to all operating systems, applications, and network infrastructure owned or managed by MLM, including:

- Microsoft Windows Server/Desktop Operating Systems
- Azure AD and Exchange Online
- Solar ERP System
- Payday Payroll System
- Cisco Meraki firmware
- Palo Alto Firewall OS (PAN-OS)

- GlobalProtect VPN
- Virtualization platforms (e.g., Hyper-V, VMware)
- Antivirus and endpoint protection software

2. Policy Principles

- **Security:** Regular patching reduces exposure to known vulnerabilities.
- **Compliance:** Aligns with ISO 27001, CIS Benchmarks, and other applicable frameworks.
- **Continuity:** Ensures stability and minimal disruption through scheduled patching and testing.
- **Accountability:** Ensures roles and responsibilities for patch deployment are clear and enforced.

3. Roles and Responsibilities

Role	Responsibility
ICT Infrastructure Team	Identify, test, schedule, deploy, and document all patches
System Owners	Approve and validate the impact of patches on department systems
ICT Manager	Authorize emergency patches and monitor compliance
Information Security Officer	Monitor threat intelligence and advise on patch prioritization

4. Patch Management Procedures

4.1 Patch Identification

- Monitor vendor portals (Microsoft, Cisco, Palo Alto, etc.) for security advisories.
- Use automated tools like Microsoft WSUS, Azure Update Management, or other patch scanners.
- Subscribe to cybersecurity alerts from CISA, SANs, and Microsoft Security Response Center.

4.2 Patch Classification

Patch Type	Definition	Response Time
Critical	Known to be actively exploited or causes major security exposure	Within 48 hours
High	High-risk vulnerabilities but no known exploitation	Within 7 days
Medium	Moderate risk but not urgent	Within 14 days
Low	Cosmetic or minor feature enhancements	As part of monthly cycle

5. Testing and Approval

- All non-critical patches must be tested in a staging or test environment that replicates production systems.
- System owners must verify that updates do not adversely affect system functionality (especially Solar ERP, Payday Payroll).
- Emergency patches may bypass full testing with ICT Manager approval but must undergo post-deployment validation.

6. Patch Deployment

6.1 Standard Deployment Schedule

- **Monthly Maintenance Window:** First Saturday of every month from 18:00–00:00
- **Critical Patch Out-of-Band:** As needed, with ICT Manager and affected departments' approval

6.2 Deployment Methods

- Group Policy (GPO) and WSUS for Windows endpoints
- Microsoft Endpoint Manager or Azure Update Management for cloud-managed systems
- Vendor-recommended CLI or UI updates for Cisco Meraki and Palo Alto Firewall
- ERP and Payroll systems require coordinated application-level patching with vendor support

7. Patch Verification and Documentation

- Confirm all patches are applied successfully using audit logs and system reports.
- Maintain a **Patch Registry** containing:
    - System name
    - Patch name/ID
    - Date applied
    - Method of deployment
    - Test results (if applicable)
    - Rollback instructions

8. Rollback and Remediation

- Establish rollback plans for all critical patches.
- In case of failure or system instability, ICT must:
    - Immediately initiate rollback
    - Notify affected departments
    - Log the incident and update the CAB (if applicable)

9. Compliance and Enforcement

- Patch compliance shall be included in internal audits.
- Systems not patched within the defined timeframes may be disconnected from the municipal network.
- Repeated failure to apply patches may result in disciplinary actions against responsible personnel.

10. Monitoring and Reporting

- Weekly patch status reports shall be generated and reviewed by the ICT Manager and ISO.
- High-risk system areas (e.g., public-facing services, domain controllers) shall be monitored in near real-time.

11. Training and Awareness

- Annual training for ICT personnel on secure patching practices and change control.

- General awareness for users on software updates and avoiding unauthorized installations.

12. Policy Review

- Reviewed annually, or in response to major changes in system architecture, risk posture, or vendor requirements.

13. User Acknowledgment

I acknowledge that I have read and understood the ICT Patch Management Policy and will comply accordingly.

Name:_____
Signature:_____
Date: _____

Policy Approvals:

ICT Manager: _____
Senior ICT Manager: _____
Municipal Manager: _____

ICT Security Policy

1. Introduction

1.1 Purpose

The ICT Security Policy defines the framework and control measures to protect the confidentiality, integrity, and availability of Matjhabeng Local Municipality's (MLM) ICT resources. It ensures that municipal digital assets, systems, and services are protected against internal and external threats.

1.2 Scope

This policy applies to all employees, contractors, consultants, interns, and third parties accessing MLM's ICT systems, including:

- Microsoft Active Directory & Azure AD
- Microsoft Exchange Online
- Solar ERP System
- Payday Payroll System
- Cashdrawer Paypoint System
- Cisco Meraki & Palo Alto Networks
- Servers, storage, firewalls, routers, switches
- Laptops, desktops, mobile and remote devices
- Municipal databases, cloud platforms, and applications

2. Policy Principles

- **Confidentiality:** Protecting sensitive information from unauthorized access.
- **Integrity:** Ensuring accuracy and trustworthiness of data.
- **Availability:** Ensuring systems and information are accessible when required.
- **Accountability:** Assigning responsibility for safeguarding assets.

3. Roles and Responsibilities

Role	Responsibility
ICT Department	Implement and monitor all ICT security controls
Information Security Officer (ISO)	Oversight of ICT security incidents, risk assessments, policy compliance
System Owners	Implement operational security within their systems
Employees and Users	Abide by security policies, report suspicious activity

4. Access Control and Authentication

- All systems must enforce **role-based access control (RBAC)** and least-privilege principles.
- Use of **strong passwords** and **multi-factor authentication (MFA)** is mandatory on:

    - Email, VPN, Solar ERP, Admin consoles (Palo Alto, Azure, Meraki)
- Shared and generic accounts are prohibited unless explicitly approved by the ICT Manager and monitored.
- Access must be reviewed **quarterly** and revoked upon exit or change in employment.

5. Physical and Environmental Security

- Server rooms and data centres must be:
    - Access-controlled using biometric or card systems
    - Monitored via CCTV
    - Equipped with UPS, fire suppression, cooling, and temperature/humidity monitors
- Visitors must sign access logs and be escorted by authorized personnel.

6. Device and Endpoint Security

- Only MLM-approved hardware and software may connect to the network.
- All endpoint devices (laptops, desktops) must:
    - Be enrolled in endpoint protection (e.g., Microsoft Defender or equivalent)
    - Be centrally managed using Microsoft Endpoint Manager or equivalent
    - Lock after 10 minutes of inactivity
- USB ports and removable media usage must be restricted and monitored.

7. Network and Perimeter Security

- Firewall policies must be defined and enforced on Palo Alto devices.
- Public-facing services must be protected by:
    - Next-generation firewalls
    - Network segmentation
    - Intrusion detection/prevention systems (IDS/IPS)
- Cisco Meraki networks must be configured for:
    - Client isolation
    - Access control lists (ACLs)
    - Centralized logging

8. Data Protection and Information Classification

- Municipal data must be classified as:
    - **Public**
    - **Internal**
    - **Confidential**
    - **Restricted**

Data handling must align with POPIA and MFMA regulations:

- Personal information must be encrypted at rest and in transit.
- Backups of confidential and restricted data must be encrypted and stored offsite or in the cloud (with MFA enabled).
- Logs must be kept of access to sensitive data (Solar, Payroll, and financial systems).

9. Secure Configuration and Patch Management

- All systems must:
    - Be hardened following CIS Benchmarks or vendor security guidelines
    - Disable default accounts and services not in use
    - Have current security patches as per the **Patch Management Policy**
- Configuration changes must be tracked through a **Change Management Process**.

10. Monitoring, Logging, and Auditing

- System and security event logs must be:
    - Enabled across all critical systems
    - Retained for a minimum of **12 months**
    - Reviewed monthly by the Information Security Officer
- Unauthorized access attempts must trigger real-time alerts via SIEM or firewall dashboard.

11. Incident Response

- All users must report security breaches or suspicious behavior immediately to the ICT Helpdesk or ISO.
- Incident handling must follow the **Security Incident Management Policy**, including:
    - Containment
    - Investigation
    - Reporting
    - Lessons learned
    - Recovery

12. Remote Access and Mobile Device Control

- All remote connections must be via **GlobalProtect VPN**, with enforced MFA.
- Mobile devices must:
    - Be registered with the municipality's MDM (Mobile Device Management) platform
    - Comply with encryption and locking policies
    - Have remote wipe capabilities enabled

13. User Awareness and Training

- All users must receive ICT security induction training during onboarding.
- Refresher training and simulated phishing campaigns shall be conducted annually.
- Users shall be made aware of their role in:
    - Password security
    - Email safety
    - Device usage
    - Social engineering prevention

14. Compliance and Disciplinary Measures

- Violations of this policy may result in:

    - Suspension of access
    - Formal disciplinary action
    - Legal action if breach involves criminal misconduct
- Annual security audits will assess compliance across departments.

15. Review and Maintenance

- The ICT Security Policy will be reviewed **annually** by the ISO and ICT Manager.
- Updates will reflect technological advancements, changes in threats, and compliance requirements.

16. User Acknowledgment

I acknowledge that I have read, understood, and agree to comply with the ICT Security Policy.

Name:_____
Signature:_____
Date: _____

Policy Approvals:

ICT Manager: _____
Information Security Officer: _____
Senior ICT Manager: _____
Municipal Manager: _____

ICT Security Incident Management Policy

1. Introduction

1.1 Purpose

This policy outlines the approach to identifying, reporting, managing, and resolving ICT security incidents within Matjhabeng Local Municipality (MLM). It ensures a consistent, timely, and effective response to mitigate risk, limit impact, and ensure recovery.

1.2 Scope

This policy applies to all employees, contractors, consultants, and third parties who use or manage MLM's ICT systems, including:

- Microsoft Active Directory & Azure AD
- Microsoft Exchange Online
- Solar ERP and Payday Payroll Systems
- Cashdrawer Paypoint System
- Cisco Meraki infrastructure
- Palo Alto Firewall & GlobalProtect VPN
- File servers, databases, desktops, laptops, and mobile devices

2. Policy Principles

- **Preparedness:** Maintain readiness to detect and respond to security incidents.
- **Responsiveness:** Respond swiftly to minimize damage and restore normal operations.
- **Accountability:** Clearly define roles and escalation pathways.
- **Continuous Improvement:** Learn from incidents to strengthen security posture.

3. Definition of a Security Incident

A **security incident** includes but is not limited to:

- Unauthorized access attempts to ICT systems
- Malware or ransomware infection
- Data breach or data loss (intentional or accidental)
- Denial of Service (DoS) or Distributed DoS attacks
- Phishing, spoofing, or social engineering attacks
- Unauthorized use or disclosure of municipal data
- Policy violations (e.g., misuse of admin rights, password sharing)

4. Roles and Responsibilities

Role	Responsibilities
All Users	Promptly report any suspicious activity or incident
ICT Helpdesk	First-line triage and logging of reported incidents
Information Security Officer (ISO)	Coordinates incident response, forensics, reporting, and lessons learned
ICT Manager	Escalation management, authority on critical incident decisions
System Administrators	Containment, recovery, and root cause analysis of technical incidents
External Vendors	Assist in managing incidents involving their technologies or support scope

---

5. Incident Reporting Procedure

5.1 Reporting Channels

Users must report incidents **immediately** via one of the following:

- ICT Helpdesk (Email or Phone)
- Direct escalation to the Information Security Officer (ISO)
- Online incident reporting form on municipal intranet

5.2 Required Information When Reporting

- Time and date of incident detection
- System(s) or data affected

- Description of suspicious behaviour
- Screenshots, error messages, or evidence (if possible)
- User's contact information

6. Incident Response Lifecycle

6.1 Identification

- Detect incidents via user reports, security monitoring tools, or automated alerts (e.g., firewall logs, Defender ATP).

6.2 Logging

- All incidents are logged in the **ICT Incident Register** with unique ID, date, and status.

6.3 Classification

- **Low:** Minimal impact, non-sensitive data, quickly contained
- **Medium:** Moderate impact, internal exposure, short recovery time
- **High/Critical:** Service downtime, public exposure, legal/regulatory risk

6.4 Containment

- Isolate affected devices or systems (e.g., disconnect from network, disable accounts).
- Disable access to compromised services.

6.5 Eradication

- Remove malware or malicious access.
- Apply patches, configuration changes, or password resets.

6.6 Recovery

- Restore affected systems from backups.
- Monitor for recurrence for at least 72 hours post-recovery.
- Notify system owner or affected department.

6.7 Post-Incident Review (PIR)

- Conduct a review within **5 working days** of incident closure.
- PIR must identify:
    - Root cause
    - Mitigation measures taken
    - Lessons learned
    - Recommendations for future prevention

7. Communication and Escalation

Incident Severity	Initial Responder	Escalate to	Notify
Low	Helpdesk	ISO (if repeated)	Not required
Medium	Helpdesk + ISO	ICT Manager	Department Head
High/Critical	ISO	ICT Manager + EXCO	Council, Compliance Authorities (e.g., Information Regulator under POPIA)

Note: Any **data breach involving personal information** must be reported to the Information Regulator under POPIA within 72 hours.

8. Forensics and Evidence Preservation

- Preserve affected devices or system logs in original state.
- All evidence must be collected and handled under **chain of custody** rules.
- Engage external forensic experts if required (subject to legal or regulatory actions).

9. Documentation and Audit Trail

- Maintain full incident logs, evidence, communications, and recovery actions for audit.
- Incident reports shall be retained for **5 years**.
- Monthly summary reports submitted to ICT Steering Committee.

10. Training and Awareness

- Annual cybersecurity awareness training for all employees.
- ICT personnel to receive specific training on threat detection and incident handling.

11. Policy Compliance

- Failure to report or respond to incidents in a timely and accurate manner may result in disciplinary action.
- All incidents will be used to inform future risk assessments and control improvements.

12. Policy Review

- This policy shall be reviewed annually by the ISO and ICT Manager or after any significant incident.

13. User Acknowledgment

I acknowledge that I have read and understood the ICT Security Incident Management Policy and will comply with the responsibilities outlined.

Name:_____
Signature:_____
Date: _____

Policy Approvals:

Information Security Officer: _____
ICT Manager: _____

Senior ICT Manager: _____

Municipal Manager: _____

ICT Server Room Management Policy

Matjhabeng Local Municipality
Policy Version: 1.0
Date: [Insert Date]
Next Review Date: [Insert Review Date]

1. Introduction

1.1 Purpose

The purpose of this policy is to define the security, environmental, and operational requirements for managing the ICT Server Room facilities of Matjhabeng Local Municipality (MLM). The policy ensures the protection of critical ICT infrastructure from unauthorized access, environmental threats, and operational risks.

1.2 Scope

This policy applies to all server room environments, data centers, communication closets, and similar ICT-controlled infrastructure within MLM's buildings and satellite offices. It covers:

- Physical access
- Environmental controls
- Security monitoring
- Equipment standards
- Incident response procedures

2. Policy Principles

- **Availability:** Ensure continuous availability of ICT infrastructure.
- **Security:** Prevent unauthorized physical and network access.
- **Safety:** Maintain a safe working environment.
- **Resilience:** Protect infrastructure against environmental and operational threats.

3. Roles and Responsibilities

Role	Responsibility
ICT Department	Daily operations and maintenance of server room infrastructure
ICT Manager	Enforce compliance with server room access and operations
Facilities Management	Maintain environmental systems (power, cooling, fire protection)
Security Personnel	Monitor physical access and surveillance
Authorized Technicians	Install and maintain equipment under ICT supervision

4. Physical Access Control

4.1 Access Restrictions

- Server Rooms are designated as **Restricted Areas**.
- Only **authorized ICT personnel** and **escorted technicians** may access server rooms.
- Visitors must:
    - Sign an access log
    - Present ID
    - Be accompanied by an authorized staff member at all times

4.2 Access Mechanisms

- Access control via card, biometric scanner, or secure lock.
- Access records must be retained for **12 months** and reviewed monthly.
- CCTV monitoring must be installed and footage retained for a minimum of **30 days**.

5. Environmental Controls

5.1 Power Supply

- All server rooms must:
    - Be equipped with an **Uninterruptible Power Supply (UPS)**

    - Use **automatic generator backup** during prolonged outages
- Power infrastructure must be inspected **quarterly**.

5.2 Cooling and Ventilation

- Air conditioning systems must maintain room temperatures between **18°C and 27°C**.
- Environmental monitors must alert ICT staff of any deviations.

5.3 Fire Suppression

- Install fire detection and suppression systems (e.g., gas-based systems like FM200 or Novec 1230).
- Fire extinguishers must be ICT-appropriate (e.g., CO_2 for electronics).
- Annual inspection and testing required.

6. Equipment Management

6.1 Equipment Standards

- Only **rack-mounted and labelled** devices shall be installed.
- All equipment must be:
    - Tagged in the ICT Asset Register
    - Maintained according to manufacturer guidelines
    - Connected to UPS and surge-protected plugs

6.2 Cabling

- Cabling must be organized using proper trunking, labelled, and color-coded.
- No loose or unsecured cables allowed.

6.3 Housekeeping

- Server rooms must be **free from clutter**, storage items, or combustible materials.
- Floors must be clean and anti-static.

6.4 Disposal and Decommissioning

- Assets of approved and industry-recognised guidelines must be established for the physical removal of decommissioned equipment from the server room, ensuring it is done safely and without disrupting other operations.
- The practice of securely erasing or destroying data stored on decommissioned equipment must be adhered to protect sensitive information.
- The disposal and decommissioning practices must be comply with relevant laws and regulations, such as e-waste laws, data protection regulations, and environmental standards.

7. Incident Response in Server Room

- Any abnormal events (e.g., water leaks, fire, overheating, equipment alarms) must be reported **immediately** to ICT and Facilities.
- Evacuation procedures must be documented and communicated to ICT staff.
- A **Server Room Incident Log** must be maintained for all events.

8. Monitoring and Logging

- All server room access must be logged manually and/or via access control systems.
- Environmental monitoring tools must log temperature, humidity, and power alerts.
- Monthly reports must be submitted to the ICT Manager.

9. Audits and Inspections

- **Quarterly internal inspections** to verify:
    - Environmental compliance
    - Access control compliance
    - Cable management
    - Housekeeping
- **Annual external audit** of physical and environmental controls.

10. Maintenance and Vendor Visits

- All maintenance work must be:
    - Scheduled and approved by the ICT Manager
    - Documented in a **Maintenance Logbook**

- Vendors must:
    - Sign a confidentiality agreement if accessing sensitive systems
    - Be escorted at all times
    - Log work performed and submit post-visit reports

11. Policy Enforcement

- Unauthorized access or failure to comply with this policy will result in disciplinary actions.
- Any compromise in physical security must be escalated to the Senior ICT Manager and Security Services.

12. Review and Updates

- This policy must be reviewed annually or after any infrastructure change, security incident, or audit finding.

13. User Acknowledgment

I acknowledge that I have read and understood the ICT Server Room Management Policy and agree to comply accordingly.

Name: _____
Signature: _____
Date: _____

Policy Approvals **ICT Manager:**

_____
Senior ICT Manager: _____
Municipal Manager: _____

ICT Firewall Management Policy

1. Introduction

1.1 Purpose

This policy outlines the standards and responsibilities for managing and securing firewall infrastructure within Matjhabeng Local Municipality (MLM). It ensures the confidentiality, integrity, and availability of municipal networks through structured control of inbound and outbound traffic using firewalls.

1.2 Scope

This policy applies to all firewalls deployed in MLM's ICT environment, including:

- **Palo Alto Networks Firewalls (physical and virtual)**
- **Cisco Meraki Firewall Features**
- Firewalls integrated within VPN solutions (e.g. GlobalProtect)
- Any other security appliances enforcing perimeter or internal segmentation

2. Policy Principles

- **Defence-in-Depth:** Firewalls are a critical perimeter defense mechanism.
- **Least Privilege:** Access rules must follow a minimum necessary access model.
- **Change Control:** Firewall rule changes must follow formal change management.
- **Logging & Monitoring:** Firewall activities must be logged and reviewed regularly.

3. Roles and Responsibilities

Role	Responsibility
ICT Security Team	Configure, review, and monitor firewalls
ICT Manager	Authorize major configuration or rule-set changes
System Owners	Approve access to applications and services relevant to their function
Information Security Officer (ISO)	Audit firewall activities and enforce compliance
Vendors (under SLA)	Perform approved maintenance under ICT supervision

4. Firewall Configuration Standards

- Firewalls must operate in a **default-deny** mode; only explicitly allowed traffic is permitted.
- Rule sets must:
  - Use source/destination IPs, ports, and protocols
  - Include description, business justification, and approval
  - Be reviewed and updated every **90 days**
- **Admin interfaces** must:
  - Be accessible only from authorized management subnets
  - Enforce MFA and role-based access control
- **Firmware and signatures** must be updated in line with the Patch Management Policy.

5. Access Request and Rule Change Procedures

- All access requests must:
  - Be submitted via the **Firewall Change Request Form**
  - Include risk impact, business justification, and required duration
- Rule changes must follow the **ICT Change Management Policy**, including testing and rollback plans.
- Emergency changes may be authorized by the ICT Manager but must be reviewed post-implementation within **24 hours**.

6. Monitoring and Logging

- All firewall activity logs must include:
  - Source and destination IP
  - Port and protocol
  - Action (allow/deny)
  - Timestamp
  - Receive Time
  - Source User/Host Name
- Logs must be:
  - Collected centrally (e.g., SIEM or secure syslog server)
  - Retained for **12 months**

- Reviewed **monthly** by the ISO for anomalies

7. Rule Review and Clean-Up

- Every **quarter**, ICT must:
  - Review all firewall rules for relevance and compliance
  - Remove obsolete or unused rules
  - Document changes and submit to the ICT Steering Committee
- Rules that haven't been used in **90 days** must be marked for review or removal.

8. Firewall Types and Use Cases

Firewall	**Purpose**
Palo Alto NGFW	Perimeter security, VPN access, threat prevention, application control
Cisco Meraki	Branch-level perimeter protection, VLAN isolation, site-to-site VPN
Internal Host Firewall (Windows Defender, etc.)	Device-level security and endpoint hardening

9. Incident Response and Breach Handling

- If suspicious activity or intrusion attempts are detected:

- Immediate containment procedures must be initiated
- Incident logged and escalated to the ISO
- Firewall access logs reviewed as part of forensic investigation
- Response follows the **Security Incident Management Policy**

10. Backup and Recovery

- Firewall configurations must be:
  - Backed up weekly and after any rule change
  - Encrypted and stored in the secure backup repository
  - Validated quarterly through configuration restore simulations

11. Physical and Logical Access Control

- Only authorized personnel may access firewall consoles.
- Management interfaces must be restricted to secure VLANs or jump servers.
- Remote access to firewalls must require VPN, MFA, and administrative approval.

12. Training and Awareness

- ICT personnel responsible for firewall management must undergo annual training on:
  - Palo Alto and Cisco Meraki configuration
  - Threat detection and policy enforcement
  - Incident handling and logging best practices

13. Compliance and Auditing

- Internal audits of firewall controls shall be conducted every **12 months**.
- Audit trails, change history, and access logs must be maintained for compliance with MFMA, POPIA, and ISO/IEC 27001.

14. Policy Review

- This policy must be reviewed annually or when significant changes occur in firewall technology or architecture.

15. User Acknowledgment

I acknowledge that I have read and understood the ICT Firewall Management Policy and agree to comply with its terms.

Name: _____
Signature: _____
Date: _____

Policy Approvals:

ICT Manager: _____
Senior ICT Manager: _____
Information Security Officer: _____
Municipal Manager: _____

ICT Operating System Security Control Policy

1. Introduction

1.1 Purpose

This policy establishes security requirements and controls for the secure configuration, maintenance, and management of all operating systems (OS) within Matjhabeng Local Municipality (MLM). The goal is to reduce the risk of unauthorized access, system compromise, and data loss.

1.2 Scope

This policy applies to all municipal devices running operating systems, including but not limited to:

- Microsoft Windows Server and Client OS
- Linux-based servers (e.g., Ubuntu, CentOS, Red Hat)
- Microsoft Azure and cloud-hosted environments

- Virtual machines (Hyper-V/VMware)
- Mobile operating systems (e.g., Android, iOS) used in municipal work

2. Policy Principles

- **System Hardening:** Minimize attack surfaces through controlled and secure configurations.
- **Standardization:** Use standardized images and configurations across devices.
- **Patch Compliance:** Ensure timely OS updates to address vulnerabilities.
- **Access Control:** Implement strong authentication and authorization mechanisms.
- **Auditability:** Ensure system activities are logged and monitored.
-

3. Roles and Responsibilities

Role	Responsibility
ICT Infrastructure Team	Implement OS controls and enforce compliance
ICT Manager	Review and approve OS baselines and configurations
Information Security Officer (ISO)	Audit OS security controls and risk posture
End Users	Use systems responsibly and report anomalies

4. Operating System Security Standards

4.1 Secure Installation

- All OS deployments must use **approved base images** that are:
    - Pre-hardened using CIS Benchmarks or Microsoft Security Baselines
    - Free from unnecessary default services or software
    - Updated to the latest patches before deployment
- New operating systems must be reviewed by ICT before production use.

4.2 Hardening Requirements

- Disable unused services, ports, and features
- Rename or disable default admin/root accounts
- Enforce password complexity, lockout, and expiry policies
- Enable host-based firewalls (e.g., Windows Defender Firewall)
- Block remote desktop access by default unless explicitly approved

5. Patch and Update Management

- Apply critical security patches **within 48 hours** of release.
- Non-critical patches must be installed within the **monthly patch cycle**.
- Patch compliance must follow the **ICT Patch Management Policy**.
- All updates must be tested in a staging environment before deployment to production systems.

6. Authentication and Access Control

- Enforce **Active Directory Group Policy** on all domain-joined Windows systems.
- Implement **role-based access control (RBAC)** with minimal privilege principles.
- Local admin access must be tightly controlled and logged.
- Use **multi-factor authentication (MFA)** on servers, administrative accounts, and remote access endpoints.

7. Malware and Threat Protection

- All endpoints must run approved **anti-malware software** (e.g., Microsoft Defender or equivalent).
- Real-time protection, automatic definition updates, and scheduled scans must be enabled.
- Security alerts must be integrated into the centralized monitoring system (e.g., Microsoft Sentinel or SIEM).

8. Logging and Monitoring

- Enable audit logging for:

    - Login attempts (successful/failed)
    - Privileged account usage
    - System modifications
    - File access on protected directories
- Logs must be:
    - Sent to a central log management system
    - Retained for **12 months**
    - Reviewed by ISO **monthly**

9. Mobile and Portable Device Controls

- Mobile devices accessing municipal systems must:
    - Be enrolled in **Mobile Device Management (MDM)**
    - Use encryption (e.g., BitLocker for Windows, FileVault for macOS)
    - Enforce PIN/password and remote wipe functionality
- Rooted or jailbroken devices are strictly prohibited.

10. Remote Access Security

- Remote OS access (e.g., RDP, SSH, management consoles) must:
    - Require VPN with MFA (GlobalProtect)
    - Be logged and monitored for abnormal access
    - Be reviewed quarterly by the ISO

11. Backup and Recovery

- System state and critical OS files must be included in backup scope.
- Recovery procedures must be documented and tested biannually.

12. Decommissioning and Disposal

- Before disposal or repurposing, OS drives must be:
    - Sanitized using secure wipe utilities
    - Certified by the ICT Department

- Systems must be removed from Active Directory and asset registers.

13. Compliance and Auditing

- Random compliance checks must be performed **quarterly**.
- Non-compliant systems may be quarantined or disconnected from the network.
- Audit findings must be reported to ICT Steering Committee and remediated within **14 days**.

14. Policy Review

- Reviewed annually or upon significant changes to OS environments, vendor recommendations, or threat landscape.

15. User Acknowledgment

I acknowledge that I have read and understood the ICT Operating System Security Control Policy and agree to comply with its provisions.

Name: _____
Signature: _____
Date: _____

ICT Fraud Prevention and Management Policy

1. Introduction

1.1 Purpose

This policy establishes the framework for preventing, detecting, and managing fraud involving the use of Information and Communication Technology (ICT) systems within Matjhabeng Local Municipality (MLM). It aims to protect municipal digital assets, services, and data from exploitation and unethical practices.

1.2 Scope

This policy applies to all ICT users, including employees, contractors, consultants, and third-party service providers who access MLM's ICT systems, including but not limited to:

- Solar ERP System
- Payday Payroll System
- Cashdrawer Paypoint System
- Active Directory and Azure AD
- Email and Collaboration Tools
- Firewalls, VPN, Network Systems
- End-user devices and mobile systems

2. Policy Principles

- **Zero Tolerance:** MLM enforces a zero-tolerance approach to ICT fraud.
- **Prevention-Oriented:** Strong internal controls and monitoring reduce the opportunity for fraud.
- **Accountability:** Users are accountable for their actions and access rights.
- **Transparency:** All incidents of suspected or confirmed ICT fraud must be reported, investigated, and addressed.

3. Definition of ICT Fraud

ICT fraud includes but is not limited to:

- Unauthorized access or manipulation of data or systems (e.g., modifying billing records)
- Creation or use of fake accounts, users, or transactions
- Misuse of privileged access for personal gain or malicious purposes
- Alteration or deletion of logs to conceal activity
- Unauthorized use of municipal digital assets (e.g., payroll, vendor payment systems)
- Phishing, identity spoofing, or impersonation within MLM systems
- Suppression of critical alerts or security controls
- Collusion with external parties to defraud the municipality using ICT systems

4. Roles and Responsibilities

Role	Responsibility
All Users	Abide by ICT policies and report suspected fraud
ICT Department	Implement fraud deterrent controls (e.g., access logs, system monitoring)
Information Security Officer (ISO)	Lead investigations and maintain fraud incident registry
Internal Audit & Risk Management	Conduct audits and fraud risk assessments
Municipal Management	Enforce disciplinary or legal actions as needed

5. Fraud Prevention Controls

5.1 Access Management

- Enforce **role-based access** (RBAC) for all critical systems.
- Segregation of Duties (SoD) in sensitive systems like Payroll and Billing:
  - Initiation ≠ Approval ≠ Payment
- Periodic access reviews and approval by department heads.

5.2 Audit Logging

- Maintain detailed logs of:
  - Logins, file access, administrative changes
  - Transactions within Solar ERP, Payday, and Cashdrawer
  - VPN connections and firewall modifications
- Logs retained for **minimum 12 months**, reviewed monthly.

5.3 System and Network Monitoring

- Deploy SIEM or log correlation tools to identify anomalies (e.g., after-hours access, volume-based thresholds).
- Use alerting on:
    - Multiple failed login attempts
    - Unusual data exports or access patterns
    - Privileged account escalation attempts

6. Fraud Detection and Reporting

6.1 Reporting Mechanisms

- Users must report suspected ICT fraud to:
    - ICT Manager
    - ISO
    - Internal Audit Office
    - Fraud Hotline (if applicable)

6.2 Anonymous Reporting

- MLM shall provide secure and anonymous channels for whistleblower reporting in accordance with the Protected Disclosures Act.

6.3 Indicators of ICT Fraud

- Unexplained changes in financial or billing records
- Disabling of security controls (e.g., audit logs, antivirus)
- Duplicate payments or transactions
- System access outside of business hours without justification

7. Fraud Response and Investigation

7.1 Incident Handling

- ICT and ISO will:
    - Secure affected systems
    - Preserve digital evidence
    - Launch a forensic investigation in collaboration with Internal Audit
    - Notify Municipal Management and Legal (if applicable)

7.2 Disciplinary and Legal Action

- If fraud is confirmed, MLM may initiate:
    - Disciplinary hearings
    - Suspension or termination of contracts
    - Civil or criminal prosecution

7.3 Post-Incident Review

- Conduct a **lessons-learned session** and update controls to prevent recurrence.

8. Awareness and Training

- Annual ICT fraud awareness sessions for all employees.
- Specialized training for:
    - Payroll and finance staff
    - ERP administrators
    - ICT security personnel
- Posters and reminders on secure system use, password policies, and whistleblower rights.

9. Continuous Improvement

- Perform **annual fraud risk assessments** across all critical systems.
- Update internal controls based on emerging fraud trends and audit recommendations.

10. Policy Enforcement and Compliance

- Failure to comply with this policy or concealment of ICT fraud is grounds for disciplinary action, including dismissal.

- Regular internal and external audits will evaluate adherence to fraud controls.

11. Review and Maintenance

- This policy shall be reviewed annually by the ISO and Internal Audit or upon detection of a significant incident.

12. User Acknowledgment

I acknowledge that I have read and understood the ICT Fraud Prevention and Management Policy and agree to comply fully with its requirements.

Name: _____
Signature: _____
Date: _____