# MANDENI MUNICIPALITY


# ICT SECURITY POLICY & PROCEDURES FRAMEWORK 2026-2027

Table of Contents

## LIST OF TABLES

## APPROVAL AND REVISION HISTORY

| APPROVAL SIGNATURES RECORD | | | |
|---|---|---|---|
| **APPROVALS** | **NAME** | **SIGNATURE** | **DATE** |
| | | | |
| | | | |
| | | | |

| REVISION NUMBER | PAGE NUMBER/S | CHANGES EFFECTED | DATE OF CHANGE |
|---|---|---|---|
| 0.1 | 1-102 | First draft created | 24-07-2026 |
| 0.2 | 1-62 | Second draft created | 06-08-2026 |
| 0.3 | 1-115 | Third draft created | 27-08-2026 |

## GLOSSARY OF TERMS AND ABBREVIATIONS

### Table 1: Terms and Abbreviations

| # | Abbreviation | Term |
|---|---|---|
| 1. | ACLs | Access Control Lists |
| 2. | APTs | Advanced Persistent Threats |
| 3. | BCP | Business Continuity Plan |
| 4. | BIA | Business Impact Analysis |
| 5. | BIOS | Basic Input/Output System |
| 6. | BYOD | Bring Your Own Device |
| 7. | CASB | Cloud Access Security Broker |
| 8. | CI/CD | Continuous Integration / Continuous Deployment (or Delivery) |
| 9. | CMDB | Configuration Management Database |
| 10. | CMT | Crisis Management Team |
| 11. | COBIT 2019 | Control Objectives for Information and Related Technologies 2019 |
| 12. | CPU | Central Processing Unit |
| 13. | CRUD | Create, Read, Update, Delete |
| 14. | CSIRT | Cybersecurity Incident Response Team |
| 15. | DHCP | Dynamic Host Configuration Protocol |
| 16. | DLP | Data Loss Prevention |
| 17. | DMZ | Demilitarised Zone |

| # | Abbreviation | Term |
|---|---|---|
| 18. | DNS | Domain Name System |
| 19. | DRP | Disaster Recovery Plan |
| 20. | EDR | Endpoint Detection and Response |
| 21. | EXCO | Executive Committee |
| 22. | FTP | File Transfer Protocol |
| 23. | HIPS | Host-based Intrusion Prevention Systems |
| 24. | HR | Human Resources |
| 25. | HTTP | Hypertext Transfer Protocol |
| 26. | I&T | Information and Technology |
| 27. | IC | Incident Commander |
| 28. | ICT | Information and Communication Technology |
| 29. | IdP | Identity Provider |
| 30. | IDS | Intrusion Detection System |
| 31. | IMT | Incident Management Team |
| 32. | IP | Internet Protocol |
| 33. | IPS | Intrusion Prevention System |
| 34. | IR | Incident Response |
| 35. | IRP | Incident Response Plan |
| 36. | ISO/IEC | ISO/IEC (International Organization for Standardization / International Electrotechnical Commission) |

| # | Abbreviation | Term |
|---|---|---|
| 37. | IT | Information Technology |
| 38. | ITSM | IT Service Management |
| 39. | KPIs | Key Performance Indicators |
| 40. | LAN | Local Area Network |
| 41. | LMS | Log Management System |
| 42. | MDM | Mobile Device Management |
| 43. | MFA | Multi-Factor Authentication |
| 44. | MFDs | Multi-Function Devices |
| 45. | MM | Municipal Manager |
| 46. | MTTC | Mean Time to Contain |
| 47. | MTTD | Mean Time to Detect |
| 48. | MTTR | Mean Time to Recover |
| 49. | NIST | National Institute of Standards and Technology |
| 50. | NIST CSF | National Institute of Standards and Technology Cybersecurity Framework |
| 51. | NLA | Network Level Authentication |
| 52. | NTP | Network Time Protocol |
| 53. | ODBC | Open Database Connectivity |
| 54. | OPA | Open Policy Agent |
| 55. | OS | Operating System |

| # | Abbreviation | Term |
|---|---|---|
| 56. | PAM | Privileged Access Management |
| 57. | PIN | Personal Identification Number |
| 58. | POPIA | Protection of Personal Information Act |
| 59. | PPE | Personal Protective Equipment |
| 60. | RACI | Responsible, Accountable, Consulted, Informed |
| 61. | RAS | Remote Access Service |
| 62. | RBAC | Role-Based Access Control |
| 63. | RCA | Root Cause Analysis |
| 64. | RDP | Remote Desktop Protocol |
| 65. | RPOs | Recovery Point Objectives |
| 66. | RTOs | Recovery Time Objectives |
| 67. | SCCM | System Centre Configuration Manager |
| 68. | SCIM | System for Cross-domain Identity Management |
| 69. | SIEM | Security Information and Event Management |
| 70. | SLA | Service Level Agreement |
| 71. | SMTP | Simple Mail Transfer Protocol |
| 72. | SSH | Secure Shell |
| 73. | SSL | Secure Sockets Layer |
| 74. | TLS/SSL | Transport Layer Security / Secure Sockets Layer |

| # | Abbreviation | Term |
|---|---|---|
| 75. | UAC | User Account Control |
| 76. | UAT | User Acceptance Testing |
| 77. | UEFI | Unified Extensible Firmware Interface. |
| 78. | UPS | Uninterruptible Power Supply |
| 79. | VDI | Virtual Desktop Infrastructure |
| 80. | VLAN | Virtual Local Area Network |
| 81. | VM | Virtual Machine |
| 82. | VPN | Virtual Private Network |
| 83. | WLAN | Wireless Local-Area Network |

# 1. INTRODUCTION

Mandeni Local Municipality is committed to strengthening information security and cybersecurity governance through the establishment and implementation of comprehensive ICT security policies, standards, plans, and procedures that support the secure management of information assets, Information and Communication Technology (ICT) resources, and municipal services.

To improve administrative efficiency and streamline the Municipal Council approval process, the Municipality has brought together key ICT security governance and operational documents into a single framework for submission and review. This document contains the **Access Management Policy, Incident Response Plan, Configuration Standards (including Antivirus and Firewall Procedures), Patch Management Procedure, IT Operating Procedure (for data backup and retention, website management, and server room management).** The documents have been presented together to facilitate a coordinated review and approval process and to provide a consolidated view of the Municipality's key ICT security requirements and controls.

The inclusion of these documents within a single framework does not replace or alter the purpose, scope, authority, or requirements of the individual documents. Each document remains independently applicable and retains its own objectives, scope, roles and responsibilities, requirements, and implementation provisions. Following approval, each document will continue to be implemented, maintained, monitored, and reviewed in accordance with the Municipality's established governance and document management processes.

Collectively, the documents contained within this framework establish the security requirements, controls, standards, and operational practices necessary to strengthen the Municipality's cybersecurity posture. They provide guidance for managing user access, responding to cybersecurity incidents, maintaining secure ICT configurations, and protecting the Municipality's ICT environment through appropriate antivirus and firewall controls.

This framework therefore supports the Municipality's efforts to strengthen cybersecurity governance, improve the protection of municipal information and ICT assets, enhance regulatory and governance compliance, and promote the secure and reliable delivery of municipal services.

## 2. ICT SECURITY DOCUMENTS COVERED BY THE FRAMEWORK

This document contains the following ICT security governance and operational documents, which have been consolidated exclusively for the purpose of Municipal Council review and approval:

- Access Management Policy
- Incident Response Plan
- Configuration Standards (including Antivirus and Firewall Procedures)
- Patch Management Procedure
- IT Operating Procedure (for data backup and retention, website management, and server room management)

Each document addresses a specific area of ICT security governance or operational security and has been developed to establish the relevant requirements, responsibilities, controls, and procedures applicable to its respective area. While the documents are presented together within this framework for purposes of coordinated Municipal Council review and approval, each document retains its individual purpose, scope, authority, and governance status and should not be interpreted as a single integrated policy or document.

The inclusion of these documents within a single framework provides the Municipal Council with a structured and coordinated submission, thereby facilitating an efficient review and approval process. Following approval, each document will continue to be implemented, communicated, monitored, maintained, and reviewed according to its specific requirements and in accordance with the Municipality's ICT governance framework and established document management processes.

# ACCESS MANAGEMENT POLICY

## 2.1. INTRODUCTION

Access management is an integral part of good information security practices and having a robust policy and processes in place help protect the Municipality network and data sets from potential cyber-attacks and reputational damage.

The Mandeni Local Municipality (also hereinafter referred to as "the Municipality") saw a need to develop this Access Management Policy that will assist the Municipality to prevent unauthorised access to the Municipality's information systems. The Information and Communications Technology (ICT) security is becoming increasingly important to the Municipality, driven in part by changes in the regulatory environment and advances in technology. Information security ensures that ICT systems, data and infrastructure are protected from risks such as unauthorised access, manipulation, destruction or loss of data, as well as unauthorised disclosure or incorrect processing of data.

The King IV Report places accountability on the Council to make arrangements for the continual monitoring of security of information. This policy will assist the Council and Executive Management exercise such accountability

## 2.2. OBJECTIVE OF THE POLICY

This policy defines the user access management control measures for the Municipality's ICT systems, information and infrastructure where it would apply to both the Municipal users and Service Providers. This policy seeks to further ensure that it protects the privacy, security and confidentiality of the Municipality's information.

## 2.3. LEGISLATIVE FRAMEWORK

The policy was developed with the legislative environment in mind. The following legislation, amongst others, were considered in the drafting of this policy:

- Municipal Finance Management Act, Act No. 56 of 2003;
- Municipal Structures Act, Act No. 117 of 1998;
- Municipal Systems Act, Act No. 32, of 2000;
- National Archives and Record Service of South Africa Act, Act No. 43 of 1996;
- Promotion of Access to Information Act, Act No. 2 of 2000;

- Protection of Personal Information Act, Act No. 4 of 2013;
- Regulation of Interception of Communications Act, Act No. 70 of 2002; and
- Treasury Regulations for departments, trading entities, constitutional institutions and public entities, Regulation 17 of 2005.

The following ICT standards and frameworks were leveraged in the development of this policy:

- Control Objectives for Information Technology (COBIT);
- ISO 27002:2013 Information technology — Security techniques — Code of practice for information security controls;
- National Institute of Standards and Technology Cybersecurity Framework (NIST CSF); and
- King Code of Governance Principles.

## 2.4. SCOPE

The policy applies to everyone in Mandeni Local Municipality, including its service providers / vendors. This policy is regarded as being crucial to the operation and security of ICT systems of the Municipality. The policy covers the following elements of user access management:

- New user registration;
- Terminated user removal;
- User permission / role change request;
- User access rights assignment for networks, operating systems, databases and applications;
- Reviewing user access permissions; and
- User and administrator activity monitoring.

## 2.5. POLICY ADMINISTRATION

The ICT Manager or delegated authority within the Municipality is responsible for maintaining this policy. The policy must be reviewed by the ICT Steering Committee on an annual basis and recommended changes must be approved by Council.

## 2.6. POLICY PRINCIPLES

**2.6.1.** Employees shall challenge and/or report any visitors found unsupervised or acting suspiciously at any site where sensitive data is processed or maintained.

**2.6.2.** Remote access to networks shall be appropriately authorised on a least privilege basis, with access only granted to systems and resources where there is an explicit business requirement.

**2.6.3.** Third Party Access to information assets shall be granted in increments according to business need and identified risks. Information asset owners shall specify access timeframes and be prepared to offer justification for such access.

**2.6.4.** Users who have satisfied all necessary criteria may be granted access to information assets only on the basis that they have a specific need to know, or to "have-access to", those information assets.

**2.6.5.** Administrator accounts shall only be granted to those users who require such access to perform their job function. Administrator accounts shall be strictly controlled and their use shall be logged, monitored and regularly reviewed.

## 2.7. NEW USER REGISTRATION

**2.7.1.** A formalised user registration process must be implemented and followed in order to assign access rights.

**2.7.2.** All user access requests must be formally documented, along with the access requirements, and approved by authorised person by making use of the user access request form.

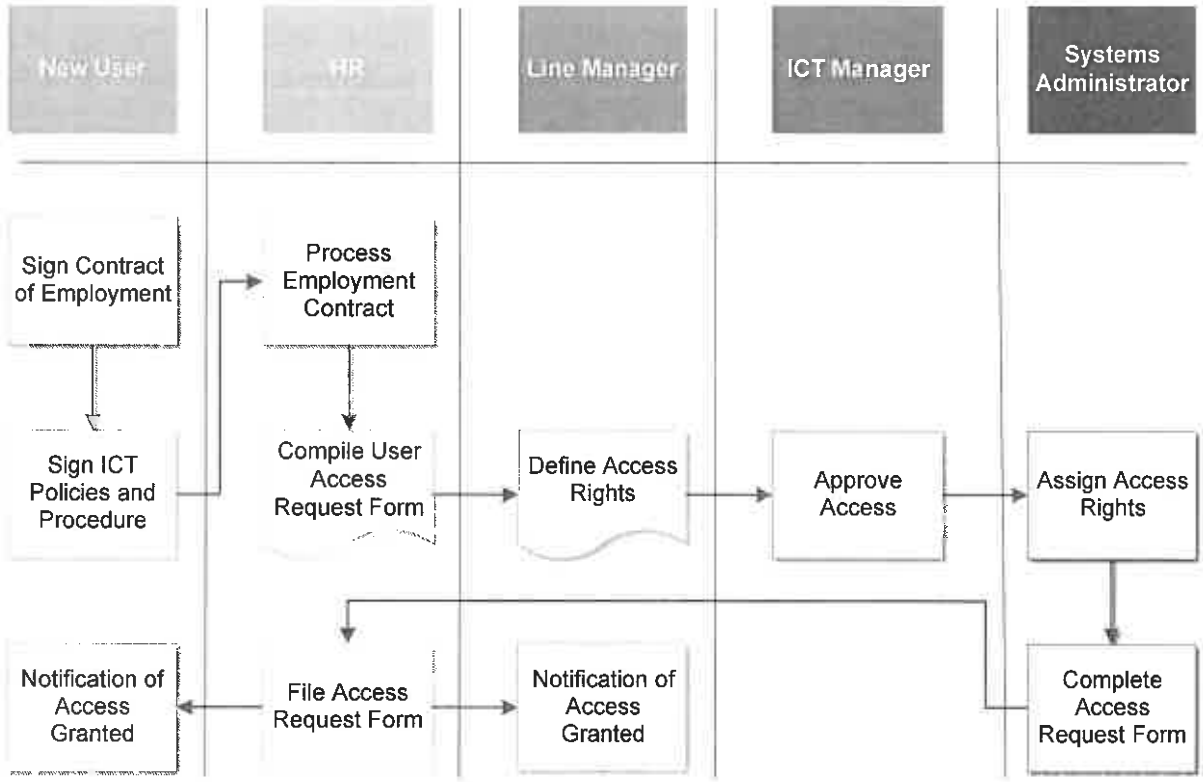
**2.7.3.** User access requests must be obtained from HR on registration of a new employee. The form must be sent to the line manager for access requirements to be requested. Once the requirements have been requested and signed off by the line manager, the form must be sent to the ICT division for approval following which the activation of the employee based on the specified requirements will be completed. The form must then be sent back to HR for record keeping purposes.

**2.7.4.** User access must only be granted once approval has been obtained.

**2.7.5.** All users must be assigned unique user IDs in order to ensure accountability for actions performed. Should shared accounts be required to fulfil a business function, this account must be approved and documented by the ICT Manager.

**2.7.6.** Figure 1 below depicts the formal new user registration process to be followed.

**Figure 1: New User Registration Process**




## 2.8. TERMINATED USER REMOVAL

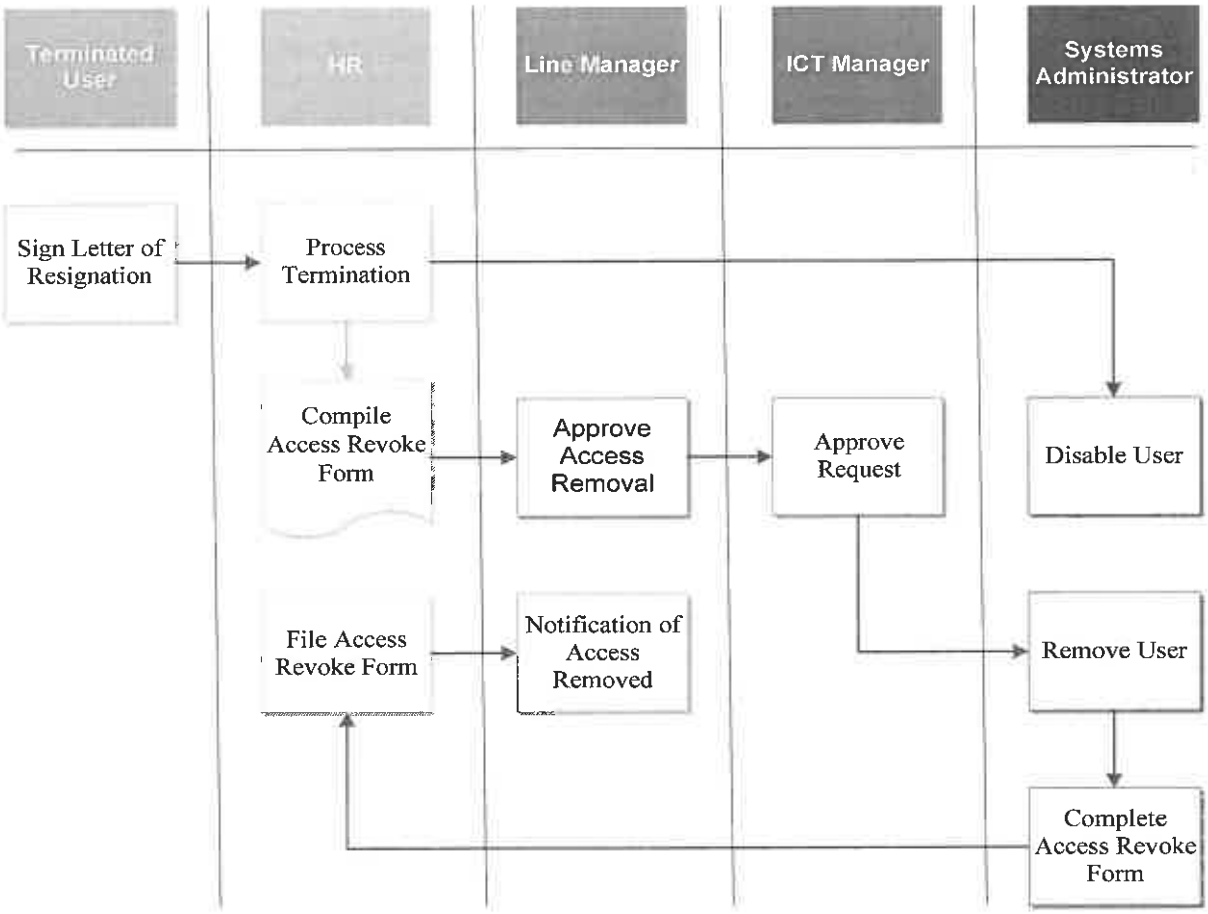
**2.8.1.** A formalised user termination process must be implemented and followed in order to revoke access rights.

**2.8.2.** All user termination requests must be formally documented and approved by duly authorised personnel. Access must be disabled immediately, with accounts being removed after 6 months once authorisation has been obtained by line manager.

**2.8.3.** Terminated user requests must be obtained from HR on the termination of an employee. The form must be sent to the line manager for access revocation to be signed off. Once access revocation has been signed off, the form must be sent to the ICT division for approval and deactivation of employee based on specified requirements. The form must then be sent back to HR for record keeping purposes.

**2.8.4.** Figure 2 below depicts the formal user termination process to be followed.

**Figure 2: User Termination Process**




## 2.9. USER PERMISSION / ROLE CHANGE REQUEST

**2.9.1.** A formalised user access management process must be implemented and followed in order to adjust user access rights.

**2.9.2.** All user access change requests must be formally documented, along with their access requirements, and approved by duly authorised personnel.

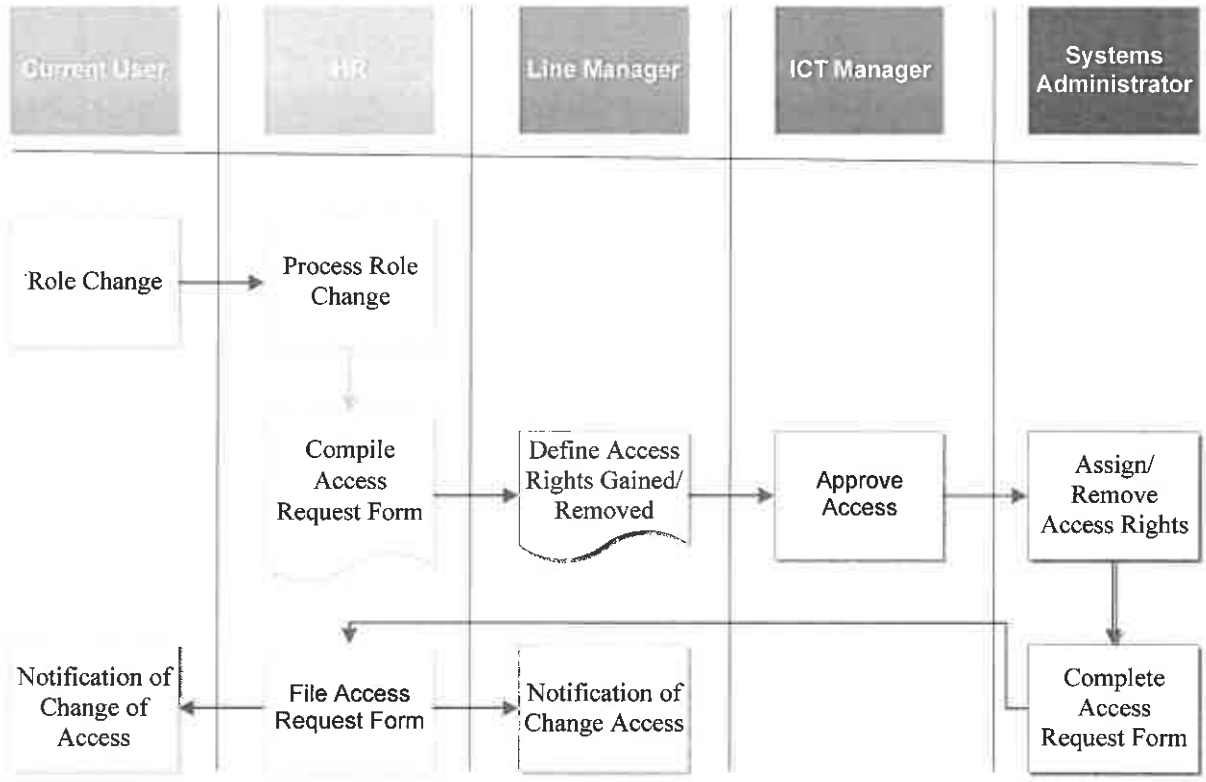
**2.9.3.** Access must only be granted once approval has been obtained by the respective line manager.

**2.9.4.** User access change requests must be obtained from HR on change of an employee's role or permissions. The form must be sent to the line manager for access requirements to be signed off. Once the access requirements have been signed off, the form must then be sent to the ICT division for approval and adjustment of employee's access rights based on specified requirements. The form must then be sent back to HR for record keeping purposes.

**2.9.5.** User access rights that are no longer required must be removed immediately.

**2.9.6.** A figure below depicts the formal user permission/role change request process to be followed.

**Figure 3: User Permission/Role Change Process**



## 2.10. NETWORK USER ACCESS RIGHTS ASSIGNMENT

**2.10.1.** Access to the Municipality's network must only be allowed once a formal user registration process has been followed.

**2.10.2.** Access to Wi-Fi must only be provided to users who require access to the network throughout the Municipality, to fulfil their business function.

**2.10.3.** RAS/VPN access must only be granted to users who require the service to fulfil their business function.

**2.10.4.** RAS access must only be granted to employees who require remote access to a system in order to administer the environment or work remotely (not at the office), and work overtime, or not within regular office hours.

**2.10.5.** RAS/VPN access must be monitored and audit logs reviewed every quarter (3 months) by system administrators.

**2.10.6.** All reviews must be formally documented and signed off by the ICT Manager. Documentation must be kept for record keeping purposes.

**2.10.7.** The ICT Manager must approve all hardware and software, owned by Municipal employees and service providers/vendors, if it is to be used for official purposes (BYOD).

## 2.11. OPERATING SYSTEM ACCESS RIGHTS ASSIGNMENT

**2.11.1.** Each system administrator must be given their own accounts within the administrator group. Should shared accounts be required to fulfil a business function, then this account must be approved and documented by the Audit and Risk Committee.

**2.11.2.** The default administrator account must be renamed and a password must be randomly generated and sealed in an envelope and kept in a safe.

**2.11.3.** The default guest account must be removed or renamed and disabled.

## 2.12. APPLICATION USER ACCESS RIGHTS ASSIGNMENT

**2.12.1.** Segregation of duties must be practiced, in such a way that application administrators cannot perform general user tasks on an application.

**2.12.2.** Applications administrators must remain independent of the department utilising the application.

## 2.13. DATABASE USER ACCESS RIGHTS ASSIGNMENT

**2.13.1.** The ICT Manager must limit full access to databases to ICT staff who need this access.

**2.13.2.** The ICT Manager must ensure that Municipal employees who access databases directly from Open Database Connectivity (ODBC) only have read access.

**2.13.3.** The ICT Steering Committee must approve all instances where Municipal employees have edit or execute access to databases.

**2.13.4.** The ICT Manager must review database rights and permissions on a quarterly basis (every 3 months). Excessive rights and permissions must be removed.

## 2.14. REVIEWING USER ACCESS AND PERMISSIONS

**2.14.1.** User access and user permissions must be reviewed every quarter (3 months) by system administrators.

**2.14.2.** On a monthly basis, HR must send a list of all terminated employees for that month to the ICT division. This list must be used to ensure that all terminated users have had their access revoked.

**2.14.3.** On a monthly basis, the ICT Manager must review all users with administrative access to the environment and assess their rights for appropriateness. Should a user be found with excessive rights, a user access change request must be performed.

**2.14.4.** All reviews must be formally documented and signed off by the ICT Manager. Documentation must be kept for record keeping purposes

## 2.15. USER AND ADMINISTRATOR ACTIVITY MONITORING

User and administrator activity must be monitored through audit and event logging.

Logs must be reviewed once a month for suspicious and malicious activities by system administrators.

All reviews must be formally documented and signed off by the ICT Manager. Documentation must be kept for record keeping purposes.

## 2.16. POLICY ENFORCEMENT

A user account should have the least privilege that is sufficient for the user to perform their role within the Municipality.

Access to information and information systems and services must be driven by business requirements. Changes in the privilege of an account must be authorised by the user's line manager and the Information Asset Owner of the information system to which the account affects.

Users' privilege rights will be periodically reviewed and is the responsibility of the relevant Information Asset Owner.

## 2.17. NON-COMPLIANCE

Any person, subject to this policy, who fails to comply with the provisions as set out above or any amendment thereto, shall be subjected to appropriate disciplinary action in accordance with the Municipality's Disciplinary Code.

# INCIDENT RESPONSE PLAN

## 2.18. SCOPE

This Incident Response Plan (IRP) applies to all Mandeni Local Municipality (hereinafter referred to as "the Municipality") operations, facilities, information systems, networks, applications, data, and personnel (employees, contractors, volunteers) and all parties that interact with the information and systems of Mandeni Local Municipality.

The IRP governs the procedures for identifying, assessing, responding to, and recovering from incidents that may impact the Municipality's ICT environment, operations, or service delivery.

This plan is strategically aligned with two internationally recognised frameworks:

- **COBIT 2019**: Provides the overarching governance and management framework, ensuring that incident response activities are integrated into the Municipality's overall governance of information and technology (I&T) and enterprise risk management.
- **NIST Cybersecurity Framework (CSF)**: Offers a risk-based approach specifically for cybersecurity incidents, guiding the Municipality in identifying, protecting against, detecting, responding to, and recovering from cyber threats.

It encompasses a broad spectrum of incident categories, acknowledging the diverse risks the Municipality faces:

- **Cybersecurity Incidents:** Malware (e.g., ransomware impacting municipal services), phishing, unauthorised access to citizen data, data breaches, Denial of Service (DoS/DDoS) attacks on municipal websites/portals, insider threats, website defacement.
- **Natural Disasters:** Floods, severe storms, droughts, fires (e.g., affecting municipal buildings, infrastructure, or critical areas within the Municipality).
- **Operational Disruptions:** Major power outages, critical equipment failures (e.g., water treatment plant equipment, waste management vehicles), supply chain disruptions (e.g., affecting municipal procurement), significant infrastructure failures (e.g., road collapse, bridge damage), severe accidents involving municipal assets or personnel.
- **Health and Safety Incidents:** Major workplace accidents, public health emergencies (e.g., pandemics impacting municipal service delivery or personnel availability).
- **Civil Unrest/Public Disturbances:** Events impacting municipal operations or safety.

### 2.18.1. Exclusions

This plan primarily focuses on the Municipality's internal response to incidents. While it outlines communication with external entities, it does not detail their internal response protocols.

## 2.19. PURPOSE AND OBJECTIVES

The purpose of this IRP is to establish a structured and systematic approach for identifying, managing, and mitigating incidents that may impact the Municipality's information systems, data, and critical operations. This plan ensures a timely and effective response to cybersecurity threats, natural disasters, system failures, and other disruptive events, thereby supporting business continuity, public service delivery, and stakeholder trust.

The IRP is designed to achieve the following key objectives:

- To establish a clear, flexible, and comprehensive framework for incident response across all incident types.
- To define roles, responsibilities, and communication channels for incident handling, ensuring effective coordination and accountability.
- To provide guidance for effective containment, resolution, and recovery of municipal services and assets.
- To ensure timely restoration of affected operations, systems, and data, minimising disruption to public services.
- To facilitate effective post-incident review and continuous improvement of response capabilities.
- To ensure compliance with relevant South African legal, regulatory, and ethical obligations. (e.g., POPIA, Disaster Management Act).

## 2.20. INCIDENT RESPONSE MANAGEMENT ROLES AND RESPONSIBILITIES

### 2.20.1. Roles and Responsibilities

The Incident Management Team (IMT) serves as the core response body, supported by specialised teams. This structure ensures clear accountability, and it aligns with COBIT 2019's emphasis on defined roles and responsibilities.

**Table 2: Roles and Responsibilities**

| Structures | | Roles | Responsibilities |
|---|---|---|---|
| **Incident Management Team (IMT) / Crisis management Team (CMT)** | Incident Commander (IC) / Crisis Lead | Municipal Manager | • Responsible for strategic direction, resource allocation, and overall management of significant incidents.<br>• Overall authority and responsibility for incident management.<br>• Primary liaison with the EXCO and external high-level stakeholders. |
| | Incident Coordinator | ICT Manager | • Receives initial incident reports, performs preliminary assessment and logging, and activates the IMT/escalates to relevant tier based on established criteria. |
| | Operations Lead | Corporates Service | • Manages the execution of tactical response actions for the specific incident type, coordinating all operational efforts. |
| | Planning Lead | Manager: Legal, Labour Relations & Risk Management | • Gathers and analyses information, maintains incident status, develops detailed action plans, and forecasts potential future impacts. |

| Structures | | Roles | Responsibilities |
|---|---|---|---|
| | | | • Engaged by Logistics/Legal Lead e.g., Forensic investigators, disaster recovery specialists, environmental consultants.<br>• Provides legal advice, ensures adherence to relevant legislation (e.g., POPIA; Disaster Management Act), manages litigation risks, and advises on regulatory reporting. |
| | Logistics Lead | Facility Management | • Manages resources (personnel, equipment, facilities, supplies), procurement, and ensures the well-being of responders.<br>• Manages municipal buildings, utilities, physical security, and infrastructure.<br>• On-site security personnel, access control. |
| | Communications Lead | Communications Officer | • Manages all internal and external communications, public relations, and media engagement.<br>• (Emergency Services Liaison) – Dedicated points of contact for the |

| Structures | | Roles | Responsibilities |
|---|---|---|---|
| | | | Municipality's SAPS, KwaDukuza Fire Department (serving the Municipality), Provincial Ambulance Services, etc. |
| | Finance/Admin Lead | Chief Financial Officer | • Manages financial aspects, emergency procurement, documentation of expenses, and administrative support during the incident. |
| | Human Resources (HR) Lead | HR Manager | • Manages personnel impacts (safety, support, deployment), employee well-being, and internal staffing needs. |
| | | | |
| **Support Teams (engaged as needed based on incident type)** | Cybersecurity Incident Response Team (CSIRT) | ICT Team | • For cybersecurity-specific incidents. Composed of municipal IT security specialists.<br>• Network, systems, database administrators responsible for municipal IT infrastructure. |
| | IT Operations Team | | |
| | Health and Safety Officer | Community Services & Public Safety | • For workplace injuries, public health advisories, environmental hazards within municipal operations. |

| Structures | | Roles | Responsibilities |
|---|---|---|---|
| | Business Unit Representatives | Managers / Heads | • From affected municipal departments (e.g., Water, Electricity, Planning, Social Development) for operational impact assessment, service continuity, and recovery prioritisation. |

**Delegation of Authority:** While specific roles are assigned responsibilities, delegation of tasks is permissible, provided that the delegating party retains accountability and ensures the delegate is appropriately trained and authorised.

### 2.20.2. Incident Declaration and Escalation Matrix

#### 2.20.2.1. Criteria for IMT Activation

Clear criteria ensure timely and appropriate IMT activation, aligning with COBIT 2019's focus on structured decision-making.

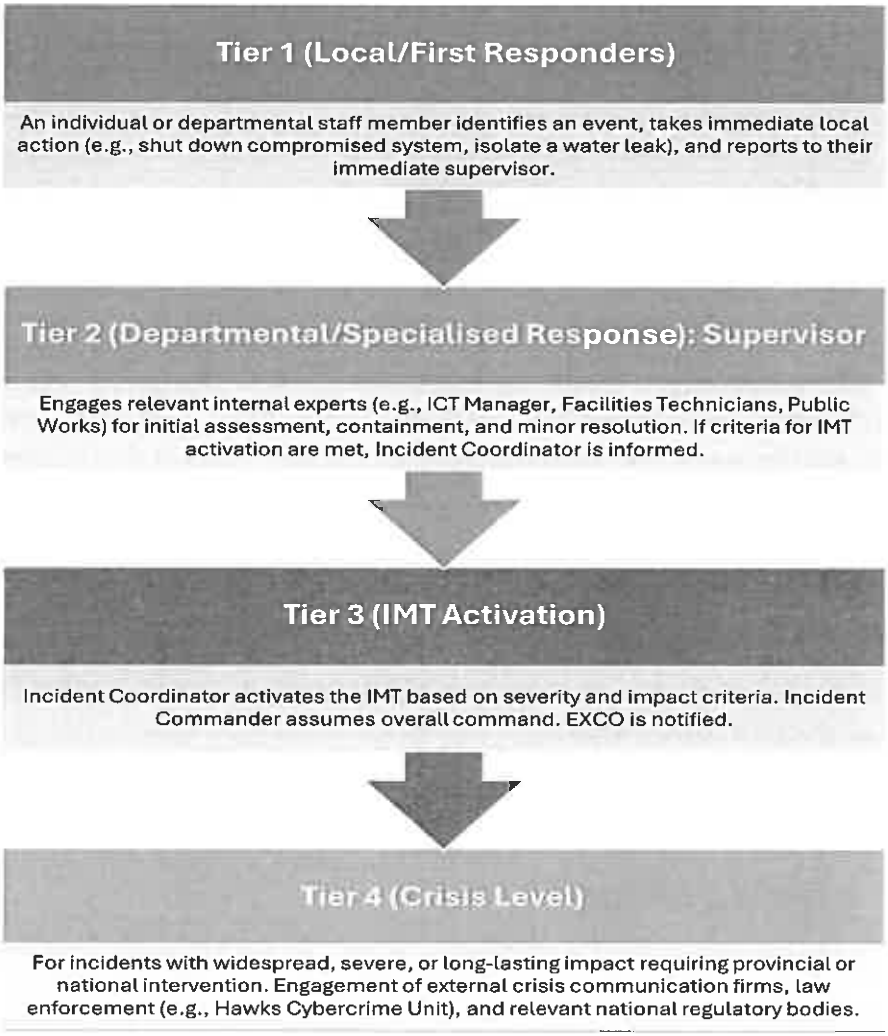
An incident is escalated to the IMT if it meets one or more of the following:

- Significant disruption or degradation of critical municipal services (e.g., water supply, electricity, emergency services).
- Loss or compromise of sensitive citizen data or critical municipal records.
- Direct threat to the life or safety of municipal personnel or citizens.
- Major financial impact or significant reputational damage to the Municipality.
- Activation of legal or regulatory reporting obligations (e.g., POPIA breach, environmental incident).
- Requires resources beyond normal departmental capabilities.
- High-profile media attention or public concern.
- Inability to contain the incident at lower tiers within a defined timeframe (e.g., 2 hours).
- Detection of advanced persistent threats (APTs) or highly sophisticated attacks.

#### 2.20.2.2. Escalation Tiers

Figure 4 below outlines the respective escalation tiers to escalate an incident.

**Figure 4 : Escalation Tiers**

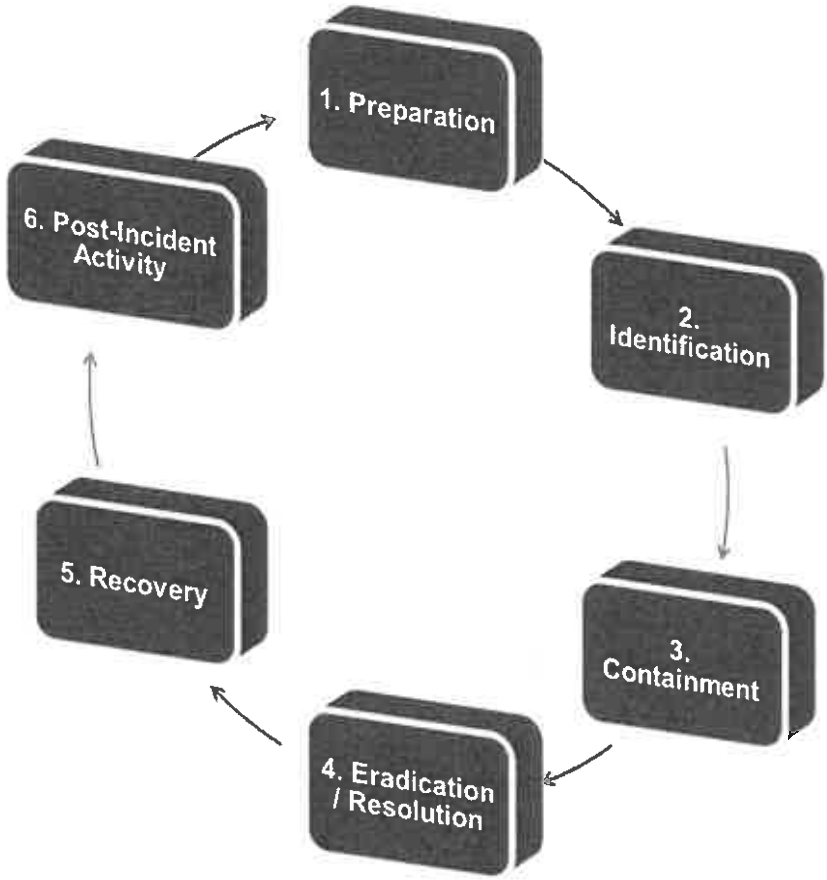


## 2.21. INCIDENT RESPONSE LIFECYCLE (PHASES)

This plan adopts a six-phase incident response lifecycle, with explicit integration of COBIT 2019 objectives/management practices and NIST CSF functions.

Figure 5 below illustrates a summary of the six phases in the Incident Response Plan Lifecycle.

**Figure 5 : Incident Response Lifecycle**




### Phase 1: Preparation

The objective of this phase is to establish a state of continuous readiness to handle incidents effectively across all categories, ensuring the Municipality's resilience which include but not limited to:

- Identify (Asset Management, Risk Assessment), Protect (Security Awareness, Access Control, Data Security, Maintenance).

- Proactive identification and assessment of municipal risks.
- Establishing a robust information security management system.
- Developing and testing business continuity plans.
- Ensuring skilled and trained personnel.

**Activities:**

- **Plan Development & Review:** Develop, review, and formally approve this IRP, BCPs, DRPs, and related policies (e.g., POPIA Compliance) annually or after significant changes.
- **Team Formation & Training:** Establish IMT/CMT and support teams, conduct regular, realistic training, workshops, and tabletop exercises covering diverse scenarios relevant to the Municipality (e.g., simulated ransomware attack, mass casualty incident, prolonged power outage).
- **Risk Assessment Mitigation:** Conduct comprehensive, multi-disciplinary risk assessments (cyber, physical, operational, environmental, health) to identify vulnerabilities and potential incident sources. Implement preventative and detective controls.
- **Business Impact Analysis (BIA):** Identify all critical municipal functions, their interdependencies, Recovery Time Objectives (RTOs), and Recovery Point Objectives (RPOs).
- **Communication Infrastructure:** Establish redundant and resilient communication channels for emergency use (e.g., satellite phones, dedicated emergency lines, backup internet, Municipality-wide emergency notification systems like SMS/WhatsApp groups).
- **Emergency Supplies & Equipment:** Maintain and regularly check stocks of essential supplies for various scenarios (e.g., first aid kits, safety equipment, emergency lighting, portable power generators, potable water, fuel reserves for critical vehicles).
- **Legal & Regulatory Preparedness:** Proactively understand all reporting obligations (e.g., POPIA, National Disaster Management Act), legal requirements for evidence preservation, and potential liabilities.
- **Vendor & Partner Agreements:** Establish clear incident response expectations, roles, and communication protocols with all key suppliers and service providers to the Municipality.
- **Tooling and Resources Acquisition:** Procure and maintain necessary incident response tools (e.g., forensic software, secure communication platforms, spare hardware, PPE for physical incidents).
- **Threat Intelligence Integration:** Establish processes for continuously receiving and integrating relevant threat intelligence (cyber, environmental, public safety) to anticipate potential incidents.

- **Security Architecture Review:** Regularly review the Municipality's security architecture to ensure it supports effective incident detection and containment capabilities.

### Phase 2: Identification (Detection and Assessment)

The objective of this phase is to effectively detect security incidents and other events, confirm their occurrence, and assess their nature, scope, and initial impact on municipal operations and assets which include but not limited to:

- Detect (Anomalies and Events, Security Continuous Monitoring, Detection Processes).
- Define Classification Schemes for Incidents and Service Requests: For consistent categorisation.
- Record, Classify, and Prioritise Requests and Incidents: Ensuring all events are formally handled.
- Investigate and Diagnose: Understanding the root cause and impact.
- Manage Security Monitoring: Utilising security monitoring tools for early detection.

#### Activities:

**Detection Sources:**

- **Cyber:** Automated alerts from SIEM, EDR, IDS/IPS, Antivirus. User reports (e.g., municipal staff reporting phishing emails, suspicious system behaviour). External notifications (e.g., from community members reporting website issues, threat intelligence feeds, SAPS Cybercrime Unit). Audit logs and municipal IT system monitoring.
- **Natural/Operational:** Environmental monitoring systems (e.g., flood sensors, fire alarms), building management systems, direct observation by municipal personnel (e.g., Roads & Stormwater, Electrical Services), emergency service notifications, weather alerts, public tip-offs, news reports.

**Initial Triage & Verification:**

- Confirm whether the reported event is a genuine incident requiring response.

- Gather preliminary information (what happened, where, when, who is affected, how it was discovered).
- Assign a unique incident ID and meticulously log the start time and initial details.
- Assign an initial severity level based on predefined criteria.

**Impact Assessment:**

- Determine immediate impact on people (safety, injuries), municipal property (damage), operations (service disruption to citizens), data (compromise of citizen/municipal records), and reputation.
- Identify affected systems, physical areas/facilities, personnel, and critical public service functions.
- Assess potential escalation.

**Incident Notification & Activation:**

- Promptly notify the Incident Coordinator/IMT Commander based on initial assessment and severity.
- Activate the IMT/CMT if the incident meets predefined escalation criteria (Section 2.20.2.2).
- Initiate preliminary communication to immediate internal stakeholders and relevant municipal departments.

**False Positive Management:**

- Develop a process for managing false positives to avoid alert fatigue and ensure legitimate incidents are not overlooked.

**Data Collection for Analysis:**

- Define specific data points to be collected during initial identification (e.g., logs, network traffic, system configurations, physical observations) to support subsequent analysis phases.

**Phase 3: Containment**

The objective of this phase is to limit the scope and impact of the incident, prevent further damage, and localise the threat which include but not limited to:

- Respond (Response Planning, Mitigation, Analysis).
- Investigate and Diagnose: Actions are part of the broader resolution.
- Respond to Risk: Implementing immediate risk response actions.
- Manage Network Security: Implementing network-level containment.

**Activities:**

**Short-Term Containment:**

- **Cyber:** Isolate compromised systems/networks (e.g., disconnect affected municipal servers from the network, block malicious IP addresses at the municipal firewall, disable compromised user accounts, revoke access tokens).
- **Natural/Operational:** Initiate immediate evacuation procedures (if unsafe), shut down affected utilities (e.g., municipal power lines, water mains, gas lines), secure physical access points to damaged areas, reroute traffic, divert affected services to alternate sites/methods (e.g., manual processes).
- Prioritise life safety and evidence preservation as paramount actions before further containment.

**Long-Term Containment Strategy:**

- Develop a strategic plan to prevent recurrence or limit long-term damage (e.g., rebuild compromised IT systems, reinforce damaged physical infrastructure, implement revised operational processes).
- Balance containment efforts with potential business disruption, always prioritising critical public services.

**Evidence Preservation:**

- **Cyber:** Take forensic images of affected municipal systems, collect memory dumps, preserve all relevant logs and network traffic captures.
- **Physical:** Document physical damage meticulously with photos/videos, secure affected physical areas to prevent tampering, collect relevant operational data (e.g., equipment logs, sensor readings).
- Maintain a strict chain of custody for all evidence collected, ensuring its integrity for potential legal action or insurance claims.

**Legal Hold:**

- Implement a legal hold on relevant data and systems as soon as an incident with potential legal implications is identified.

**Communication during Containment:**

- Maintain regular, controlled communication internally about containment progress to manage expectations and provide updates to affected personnel.

**Phase 4: Eradication / Resolution**

The objective of this phase is to eliminate the root cause of the incident, remove all traces of the threat, and fully resolve the immediate issue which include but not limited to:

- Respond (Mitigation, Analysis).
- Investigate and Diagnose: Identifying and resolving the root cause.
- Protect Against Malware: Direct malware removal.
- Implementing necessary changes in a controlled manner.

**Activities:**

- **Root Cause Analysis:** Conduct a thorough investigation to identify the underlying cause of the incident (e.g., exploited software vulnerability, structural weakness in a municipal building, a critical process failure, human error).
- **Cyber:** Fully remove malware, apply all necessary security patches, harden municipal IT systems (e.g., servers, workstations, network devices), force password resets for all potentially compromised accounts, remove any lingering backdoors or unauthorised access mechanisms.
- **Natural/Operational:** Repair damaged municipal infrastructure (e.g., roads, bridges, public buildings), clear debris, address environmental hazards (e.g., chemical spills), rectify faulty operational processes, repair or replace damaged critical equipment.
- **Verification:** Conduct rigorous checks to ensure the threat is completely removed or the root cause is fully resolved, and no lingering issues remain that could cause recurrence.
- **Vulnerability Scanning Post-Eradication:** Perform targeted vulnerability scans (for cyber incidents) after eradication to confirm no new vulnerabilities were introduced and existing ones are patched.
- **Threat Intelligence Update:** Integrate newly identified threat indicators into security tools to enhance future detection capabilities.

**Phase 5: Recovery**

The objective of this phase is to restore affected municipal operations, systems, and services to normal, secure, and resilient functionality, minimising downtime for citizens which include but not limited to:

- Recover (Recovery Planning, Improvements, Communications).
- Investigate and Diagnose: The final steps of incident resolution.
- Restore BCP/DRP: Restoring I&T capabilities and services following disruption.
- Ensuring smooth operational resumption.

**Activities:**

**Restoration:**

- **Cyber:** Restore affected municipal IT systems and citizen data from clean, verified backups. Reconfigure networks and applications to their secure operational state.
- **Natural/Operational:** Reoccupy municipal facilities (after safety clearance), restore all affected utilities (water, electricity, sanitation), reactivate equipment, resume affected municipal business processes and public services (e.g., licensing, billing, community services).

**Validation & Testing:**

- Thoroughly test all restored systems, services, and operational functions for full functionality, performance, and security.
- Verify data integrity and consistency.
- Perform post-recovery vulnerability scans (for cyber) or safety and operational readiness checks (for physical/operational).
- **Phased Rollout:** Bring municipal operations/systems back online in a controlled, phased manner, prioritising critical public services identified in the BIA.
- **Enhanced Monitoring:** Implement increased monitoring for a defined period after recovery to detect any recurrence or new issues.
- **Communication:** Inform stakeholders (internal and external) of recovery progress and completion of service restoration.

**Public Announcements of Service Resumption:**

- Clearly communicate to citizens when services are fully restored, acknowledging any inconvenience.

**Service Level Agreement (SLA) Review:**

- Review compliance with SLAs for critical services during the recovery period and assess any penalties or credits.

**Phase 6: Post-Incident Activity (Lessons Learned and Improvement)**

The objective of this phase is to identify weaknesses, and implement changes for continuous improvement in resilience, prevention, detection, and response capabilities which include but not limited to:

- Identify (Improvements), Recover (Improvements, Communications)
- Close Requests and Incidents: Formal closure after all actions are complete.
- Report on Incidents: Provide comprehensive reports.
- Monitor and Report Performance and Conformance: Collect and analyse performance data.
- Evaluate Performance and Conformance: Review the effectiveness of processes and controls.
- Respond to Risk: Review risk response effectiveness and update risk treatment plans.
- Maintain the Governance Framework: Incorporating lessons learned into the overall governance system.

**Activities:**

- **Post-Incident Review Meeting (Hotwash/Debrief):** Conduct a comprehensive "lessons learned" meeting with the IMT/CMT, all involved teams, and relevant stakeholders.
    - **Key questions:** What happened? How was it detected? How effective was the response? What worked well? What could be improved? What was the actual impact (financial, reputational, operational, human, public service delivery)?
- **Incident Report:** Create a detailed incident report documenting the entire incident, including timeline, nature and root cause, actions taken during each

phase, resources utilised, comprehensive impact assessment, and clear recommendations for improvement.

- **Action Plan for Improvements:** Develop specific, actionable recommendations for:
  - Updating municipal policies, procedures, and plans (IRP, BCP, DRP, safety plans, IT security policies).
  - Enhancing preventative controls and security measures (e.g., new cybersecurity solutions, infrastructure upgrades, revised safety protocols).
  - Addressing underlying infrastructure or operational weaknesses.
  - Identifying additional training requirements for personnel.
  - This directly feeds into strategic improvements

- **Communication with External Parties:** Fulfil any required regulatory reporting (e.g., POPIA breach notifications to the Information Regulator, incident reports to Department of Labour, environmental agencies). Communicate with affected citizens, partners, and the public as required by law and policy.
- **Knowledge Base Update:** Update internal municipal knowledge bases, operational playbooks, and training materials with new insights, revised procedures, and threat intelligence.
- **Compliance Audit:** Engage internal audit or an independent third party to audit the incident response process for compliance with this IRP and relevant regulations.
- **Sharing Lessons Learned (Internal):** Disseminate lessons learned and updated best practices to all relevant staff through various communication channels.

## 2.22. COMMUNICATION PLAN

### Internal Communication

- **Primary Audience:** IMT/CMT members, Municipal Manager and Executive Committee, affected departmental staff, all municipal employees.
- **Key Information:** Incident status, safety instructions, operational changes, recovery timelines, "all clear" notifications.
- **Methods:** Dedicated secure communication channels (e.g., crisis communication platform, emergency messaging system, municipal-wide SMS/WhatsApp, out-of-band communication via satellite phones), dedicated conference call bridges, internal email (if uncompromised), municipal intranet portal.

- **Communication Templates:** Pre-drafted internal notifications for various incident types and severity levels, ensuring rapid and consistent messaging.

**External Communication**

- **Primary Audience:** Citizens of Mandeni Local Municipality, Customers/Clients (e.g., service users), Regulators (e.g., Information Regulator of South Africa, Department of Labour, Provincial Disaster Management Centre), Law Enforcement (SAPS, Hawks), Media/Public, Key Vendors/Partners, Emergency Services.
- **Key Information:** General incident overview (avoiding sensitive details initially), impact on municipal services/public, actions being taken, recovery status, safety advisories, official statements.
- **Methods:** Official statements, press releases, dedicated municipal website page for updates, direct email (for registered users/stakeholders), municipal call centre support, social media updates (controlled by Communications Lead), public service announcements (local radio).
- **Ownership:** All external communications must be managed by the Communications Lead, approved by the Incident Commander/Crisis Lead, and examined by Legal Officer.
- **Communication Templates:** Pre-drafted external notifications and holding statements for various scenarios, ensuring legal compliance and public trust.

Below is the list of internal and external contacts:

**Table 3: Contacts List**

| Roles | Name /Title | Contact Info |
|---|---|---|
| INTERNAL | | |
| Incident Response Lead | Mr. S Khuzwayo (Municipal Manager) | 032 456 8200 queries@mandeni.gov.za |
| ICT Manager / Technical Lead | Mr. P Ntanzi | 032 456 8200 |
| Executive Mayor | Cllr. T. Mdlalose | 032 456 8200 |
| Head of Communications | Mr. M Manzi | 032 456 8200 |
| Information Officer (PAIA) | Mr. S Khuzwayo | 032 456 8200 |
| Manager: Legal, Labour Relations & Risk Management | Ms. B Masinga | 032 456 8200 |

| Roles | Name /Title | Contact Info |
|---|---|---|
| Emergency Services | — | 087 285 1153 |
| **EXTERNAL** | | |
| iLembe District Municipality | Regional coordination | ilembe.gov.za |
| KwaZulu-Natal Office of the Premier | Provincial escalation & oversight | kznpremier.gov.za |
| South African Police Service (SAPS) | Criminal investigation support | 10111 (Emergency) |
| State Information Technology Agency (SITA) | National ICT support & escalation | sita.co.za |
| Department of Cooperative Governance (COGTA) | Disaster management & compliance | cogta.gov.za |
| Information Regulator (POPIA) | Data breach reporting & compliance | inforegulator.org.za |

**Dedicated Communication Hub:**

- Designate a specific physical or virtual location (e.g., a shared drive, collaboration platform) for all incident-related communications, templates, and contact lists.

**Public Information Officer (PIO):**

- Explicitly assign a primary Public Information Officer role (likely the Communications Lead) who is the sole authorised spokesperson for external communications.

**Social Media Monitoring:**

- Implement tools or processes to monitor social media for public sentiment and misinformation during an incident, allowing for timely and accurate responses.

## 2.23. TOOLS AND RESOURCES

The availability and readiness of tools and resources are critical and align with NIST CSF's Protect and Detect functions, and COBIT 2019's DSS (Deliver, Service, and Support) domain.

### Communication Tools

- Emergency contact lists (internal & external, readily available in hard copy and secure digital formats).
- Secure and resilient communication platforms (e.g., encrypted messaging, dedicated crisis communication software).
- Designated incident management communication centre/room with backup power.

### Technical Tools (for Cybersecurity Incidents)

- Forensic workstations and software for data analysis.
- Malware analysis tools (sandboxes, threat intelligence platforms).
- Packet sniffers and network analysis tools.
- Robust Backup and Recovery systems for municipal data and systems.
- Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), Intrusion Detection/Prevention Systems (IDS/IPS), Antivirus.
- Secure external storage for evidence collection and preservation.
- Vulnerability scanners and penetration testing tools.

### Physical Resources (for Natural / Operational Incidents)

- Emergency power generators and sufficient fuel reserves.
- Comprehensive first aid kits, medical supplies, and designated medical personnel/liaisons.
- Safety equipment (Personal Protective Equipment (PPE), fire extinguishers, emergency lighting).
- Access to pre-identified emergency shelters or alternate work locations for municipal staff.
- Physical security measures (barricades, alarms, access control systems).

- Up-to-date municipal building schematics, utility shut-off locations.
- Emergency vehicle fleet (e.g., public works, emergency services).

### Documentation & Reference

- Current IRP, BCP, DRP documents (accessible off-site).
- Up-to-date network diagrams, system architecture diagrams.
- Comprehensive asset inventory (including critical IT and physical municipal assets).
- Key vendors contact information and Service Level Agreements (SLAs).
- Relevant municipal policies (Data Breach Policy, Health & Safety Manuals, Environmental Policies).
- Threat intelligence feeds (cyber and environmental data).
- Contact details for external emergency services (e.g., Mandeni SAPS, KwaDukuza Fire Department, Provincial Ambulance Services).

### Dedicated Incident Response Kit

Develop and maintain physical "go-bags" for the IMT/CSIRT with essential supplies (e.g., chargers, secure laptops, portable hard drives, basic first aid, contact lists).

### Third-Party Expertise List

Maintain a list of pre-vetted external experts (e.g., forensic investigators, PR firms, legal counsel specializing in data privacy) with whom the Municipality can engage quickly if needed.

## 2.24. TESTING AND MAINTENANCE

Continuous testing and maintenance are crucial for ensuring the IRP's effectiveness, aligning with NIST CSF's emphasis on continuous improvement and COBIT 2019's MEA (Monitor, Evaluate, and Assess) domain.

### Regular Review

This IRP will be reviewed and updated at least annually, or after any significant organisational, technological, or environmental changes (e.g., new municipal services, major IT system upgrades, significant local climate shifts, changes in SA legislation).

### Training

All IMT/CMT members and relevant municipal staff will undergo regular, role-specific training on incident response procedures, including practical drills and simulations.

### Exercises

Conduct a variety of exercises at least annually to test the effectiveness of the IRP and identify areas for improvement:

- **Tabletop Exercises:** Discuss hypothetical scenarios (e.g., a major data breach, a localised flood) to test understanding of the plan and communication protocols.
- **Simulation Exercises:** Simulate elements of an incident (e.g., a ransomware attack drill on non-production systems, a fire evacuation drill for a municipal building, a system failover test).
- **Full-Scale Exercises:** Comprehensive, realistic simulations involving multiple municipal departments and external parties (e.g., SAPS, local disaster management) if feasible, to test full operational response.

## 2.25. LEGAL AND REGULATORY

Compliance with laws and regulations is paramount for Mandeni Local Municipality.

- Protection of Personal Information Act (POPIA), Act No. 4 of 2013:
- National Disaster Management Act, Act No. 57 of 2002:
- Occupational Health and Safety Act (OHSA), Act No. 85 of 1993:
- National Environmental Management Act (NEMA), Act No. 107 of 1998:
- Municipal Finance Management Act (MFMA), Act No. 56 of 2003:
- National Institute of Standards and Technology Cybersecurity Framework (NIST CSF):
- Control Objectives for Information and Related Technologies (COBIT 2019):

- ISO 27001:
- Department of Public Service and Administration
- KING IV

**Evidence Handling:** All evidence collected during an incident (digital or physical) must be handled in a legally admissible manner to support potential legal action, forensic analysis, insurance claims, or regulatory investigations.

## 2.26. Performance Metrics

The Municipality must track key performance indicators (KPIs) for incident response across all categories, ensuring alignment with municipal objectives:

- Mean Time to Detect (MTTD)
- Mean Time to Respond (MTTR)
- Mean Time to Contain/Resolve (MTTC/R)
- Mean Time to Recover (MTTR)
- Number of incidents by type and severity.
- Cost per incident (direct and indirect, e.g., lost productivity, repair costs, potential fines).
- Effectiveness of communication (internal and external).
- Lessons learned implementation rate and closure.

Below is a table outlining Performance Metrics for the Incident Response Plan of Mandeni Local Municipality, designed to measure the effectiveness and efficiency of the Municipality's Cybersecurity and IT incident response efforts.

**Table 4: Performance Metrics**

| Metric | Performance Indicator (KPI) | Target / Benchmark | Measurement Criteria |
|---|---|---|---|
| 1 **Incident Detection Time** | Average time to detect incidents | ≤ 30 minutes for critical incidents | Time between incident occurrence and detection logged in SIEM or ticketing system |
| 2 **Incident Response Initiation** | Time to initiate response after detection | ≤ 1 hour for critical incidents | Time from detection to first documented response action |

| Metric | Performance Indicator (KPI) | Target / Benchmark | Measurement Criteria |
|---|---|---|---|
| 3 **Time to Contain Incident** | Duration from detection to full containment | ≤ 4 hours (high), ≤ 24 hours (medium) | Time from incident detection to isolation or containment confirmation |
| 4 **Time to Resolve Incident** | Time to fully resolve the incident | ≤ 48 hours (standard), ≤ 5 days (complex cases) | Time from detection to resolution (system restored, threat removed) |
| 5 **Time to Close Incident** | Time from resolution to case closure | ≤ 5 working days | Includes documentation, RCA, and communication completed |
| 6 **Incident Documentation Rate** | % of incidents fully documented in incident register | 100% | Incident records completed with date, type, severity, and resolution steps |
| 7 **Repeat Incident Rate** | % of repeated incidents (same root cause) | ≤ 5% per quarter | Number of incidents with identical or related root causes |
| 8 **Post-Incident Review Completion** | % of major incidents reviewed post-resolution | 100% within 5 working days | Lessons learned and preventive actions recorded and communicated |
| 9 **Staff Awareness Training** | % of staff trained in incident reporting annually | ≥ 90% | Training attendance logs and annual awareness test results |
| 10 **IR Plan Test Frequency** | Number of simulations or tabletop exercises per year | ≥ 2 per year | Test logs, reports, and outcomes from IR simulation exercises |
| 11 **Incident Escalation Accuracy** | % of incidents correctly escalated to appropriate support levels | ≥ 95% | Cross-check incident category vs. responsible team/escalation matrix |
| 12 **User-Reported Acknowledgement** | % of user-reported incidents acknowledged within SLA | ≥ 80% within 2 hours | Helpdesk/ticket system response time tracking |

| Metric | Performance Indicator (KPI) | Target / Benchmark | Measurement Criteria |
|---|---|---|---|
| 13 **Regulatory Notification Time** | Time taken to notify regulatory body of notifiable breach | Within 72 hours (per POPIA & NEMISA guidelines) | Email, letter, or online submission timestamp vs. discovery time |

# CONFIGURATION STANDARDS (INC FIREWALL AND ANTIVIRUS)

## 2.27. SCOPE

These standards apply to all hardware and software configurations of:

- **Servers:** All servers hosting municipal applications, databases, file shares, and infrastructure services.
- **Computer Workstations:** All desktop and laptop computers used by municipal employees, contractors, and authorised third parties, whether municipality-owned or approved BYOD.
- **Printers:** All network-connected and locally attached printers, multi-function devices (MFDs), and imaging systems.

This includes all operating systems, applications, and network settings on these devices.

These standards are strategically aligned with these internationally recognised-frameworks:

- **COBIT 2019:**
  - **BAI10 (Managed Configuration):** Directly addresses the need to define and maintain descriptions and relationships among key resources and capabilities required to deliver I&T-enabled services. This includes collecting configuration information, establishing baselines, verifying, auditing, and updating configuration repositories.
  - **APO13 (Managed Security):** Ensures that the municipality has a comprehensive approach to information security, of which secure configurations are a fundamental component.
  - **DSS05 (Managed Security Services):** Covers the operational aspects of security services, including vulnerability management and security testing, which rely on well-defined configurations.
  - **BAI06 (Managed IT Changes):** Configuration changes must be managed as part of a robust change management process.

- **ISO/IEC 27001:2022:**
  - **Configuration Management:** This control directly mandates that "Configurations, including security configurations, of hardware, software,

services and networks should be established, documented, implemented, monitored and reviewed." This document provides the framework for achieving this.

- **Change Management:** All configuration changes must adhere to a formal change management process to minimise risks to information security.
- **Control of Operational Software:** Procedures should be implemented to control the installation of software on operational systems, ensuring integrity and authorised changes.
- **Access Control & Identity Management**: Secure configurations are fundamental to implementing effective access controls.
- **Clear Desk and Clear Screen:** While not direct configuration, it relates to the physical security implications of printers and workstations.
- **Equipment Siting and Protection:** Physical security of servers and critical printers.
- **Installation of Software on Operational Systems:** Covered under workstation and server software configuration.

The Firewall and Antivirus Management Procedures are also incorporated into this document as appendix A & B.

## 2.28. PURPOSE AND OBJECTIVES

The purpose of these Configuration Standards is to establish a consistent, secure, and well-managed ICT environment that supports reliable service delivery to citizens and internal departments. These standards serve as a foundational layer for operational efficiency, compliance, and protection of the Municipality's data.

These Configuration Standards define the minimum secure baseline configurations for all servers, computer workstations, and printers within the Mandeni Local Municipality. The key objectives include:

- Ensure the security, integrity, and availability of municipal information and IT assets.
- Mitigate risks associated with misconfigurations and vulnerabilities.
- Provide a consistent and repeatable process for system deployment and management.
- Support compliance with regulatory requirements and internal policies.
- Align with the principles of the Mandeni Local Municipality's ICT Governance Framework, COBIT 2019, and ISO/IEC 27001.
- To ensure compliance with relevant South African legal, regulatory, and ethical obligations. (e.g., POPIA, Disaster Management Act).

## 2.29. CONFIGURATION PRINCIPLES

These principles apply across all device types covered within these standards.

**Table 5: Principles**

| # | Principle | Description |
|---|---|---|
| 1. | Principle of Least Privilege | • All systems, applications, and user accounts shall be configured with the minimum necessary rights, privileges, and access required to perform their intended function. |
| 2. | Documentation | • All configurations, baselines, and deviations shall be thoroughly documented, maintained, and version-controlled within a Configuration Management Database (CMDB) or similar repository. |
| 3. | Default Deny | • Unless explicitly permitted, all network traffic, services, and features shall be denied by default. |
| 4. | Security by Design | • Security considerations shall be embedded from the initial planning and design phases of any new system or service deployment. |
| 5. | Standardisation | • Utilise standardised templates and images for consistent deployment and maintenance |
| 6. | Regular Review and Update | • Configuration standards shall be reviewed and updated at least annually, or more frequently in response to changes in threat landscape, technology, or regulatory requirements. |
| 7. | Change Management: | • All changes to baseline configurations must follow the municipality's formal Change Management Policy and Procedures. |
| 8. | Monitoring and Auditing | • Configurations shall be continuously monitored for deviations from baselines and audited regularly for compliance. |
| 9. | Patch Management | • Implement a robust and timely patch management process for operating systems, applications, and firmware across all devices. |
| 10. | Data Classification | • Configurations shall consider the classification of data being processed, stored, or transmitted, applying stricter controls for highly sensitive information. |
| 11. | Vulnerability Management | • Systems shall undergo regular vulnerability scanning and penetration testing, with findings promptly remediated according to risk. |
| 12. | Backup and Recovery | • Critical system configurations and data shall be regularly backed up, and recovery procedures tested to ensure business continuity. |

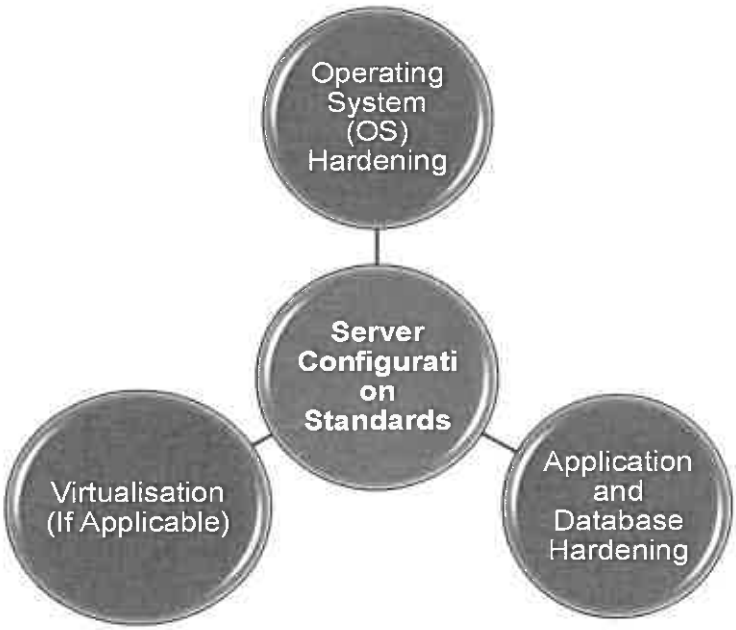
## 2.30. CONFIGURATION STANDARDS

### 2.30.1. Server Configuration Standards

Servers are critical assets; their configurations must be highly secure.

The following diagram provides an overview of the Server configuration standards.

**Figure 6: Server Configuration Standards**




#### 2.30.1.1. Operating System (OS) Hardening:

- **Minimal Installation:** Install only essential operating system components, services, and roles required for the server's function. Remove or disable all unnecessary services and features
- **Latest Patches:** Ensure all OS security patches and updates are applied promptly as per the Patch Management Policy.
- **Strong Authentication:**
    - Enforce strong password policies for all local and domain accounts, meeting complexity, length (minimum 8 characters recommended), and history requirements.

- Implement account lockout policies (e.g., 5 failed attempts, 30-minute lockout).
- Disable default administrator accounts and rename them.
- Implement Multi-Factor Authentication (MFA) for administrative access where technically feasible.

- **Access Control:**
  - Implement Role-Based Access Control (RBAC).
  - Restrict interactive logins (e.g., RDP, SSH) to authorised personnel only.
  - Use secure protocols (SSH, RDP with NLA) and disable insecure ones (Telnet, FTP, HTTP for management).
- **Firewall:** Enable and configure the host-based firewall to deny all incoming and outgoing connections by default, allowing only explicitly required ports and protocols for the server's function.
- **Logging and Auditing:**
  - Enable comprehensive security logging (e.g., successful/failed logins, privilege escalation, file access, system changes).
  - Configure logs to be securely stored on a centralised log management system (SIEM) with sufficient retention periods.
  - Synchronise server clocks using an authoritative time source (NTP).
- **Antivirus/Anti-Malware:** Install and maintain centrally managed antivirus/anti-malware software with real-time protection and regular updates.
- **PowerShell/Scripting Security:** Implement PowerShell logging, constrained language mode, and restrict script execution to signed scripts where possible.

#### 2.30.1.2. Application and Database Hardening:

- **Dedicated Instances:** Where possible, deploy applications and databases on dedicated server instances to limit the blast radius of a compromise.
- **Default Passwords:** Change all default passwords for application and database accounts immediately.
- **Least Privilege:** Configure application and database accounts with the minimum necessary permissions to perform their functions.

- **Secure Configuration Guides:** Follow vendor-specific security hardening guides for all applications and databases (e.g., SQL Server, IIS, Apache, specific municipal software).
- **Encryption:**
    - Encrypt sensitive data at rest (e.g., database encryption, file system encryption).
    - Encrypt data in transit using TLS/SSL for all sensitive communications.
- **Error Handling:** Configure applications and databases to provide generic error messages, avoiding detailed error information that could aid attackers.
- **Database Auditing:** Enable comprehensive auditing of database activities (e.g., DDL, DML, failed logins) and send logs to the centralised SIEM.
- **Secure Development Practices:** For internally developed applications, adhere to secure coding guidelines and perform regular security testing (e.g., penetration testing, vulnerability scanning).

#### 2.30.1.3. Virtualisation (if applicable):

- **Hypervisor Hardening:** Secure the hypervisor itself (e.g., VMware ESXi, Microsoft Hyper-V) with strong authentication, regular patching, and restricted administrative access.
- **VM Isolation:** Ensure proper network and resource isolation between virtual machines.
- **Guest OS Hardening:** Apply all server OS hardening standards to guest virtual machines.

**Physical Security:**

- Servers must be housed in secure, access-controlled environments with appropriate environmental controls (temperature, humidity), and fire suppression.

**Network Segmentation:**

- Implement network segmentation to isolate critical server roles and sensitive data, limiting lateral movement in case of compromise.

**Automated Configuration Management:**

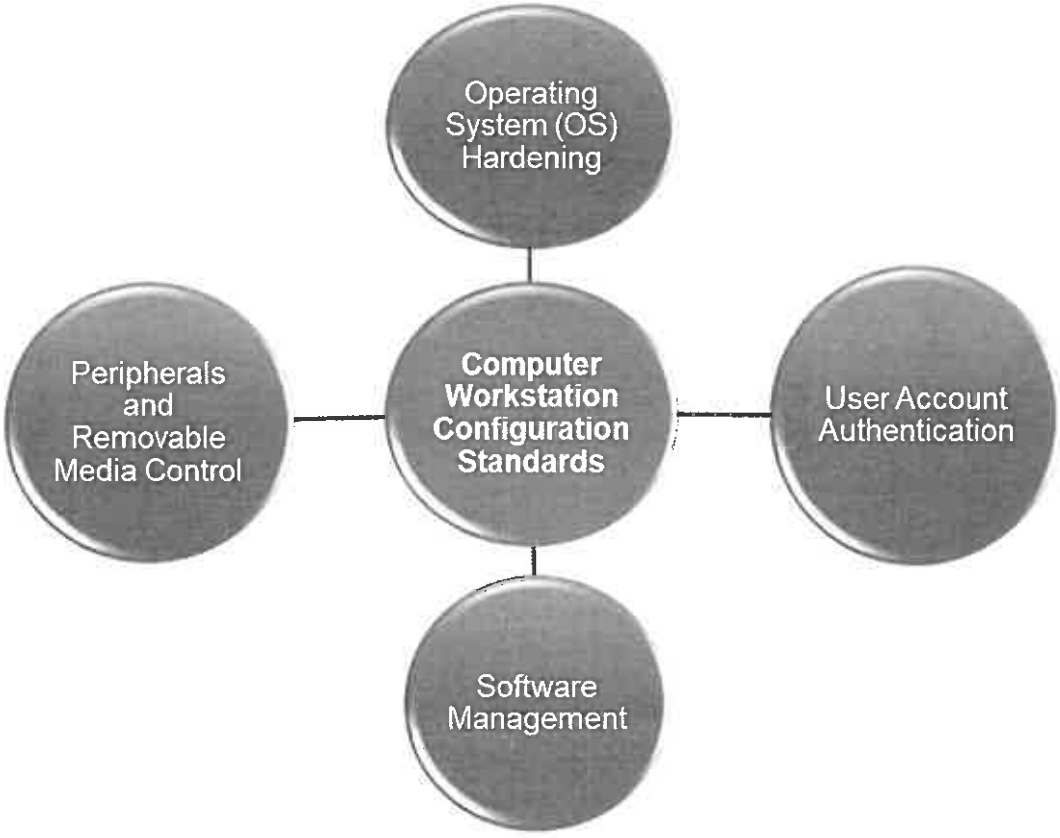
- Utilise automated tools to deploy, maintain, and monitor server configurations against defined baselines, minimizing manual errors and ensuring consistency.

### 2.30.2. Computer Workstation Configuration Standards

Workstations are often the initial point of compromise; therefore, strong configurations are essential.

The following diagram provides an overview of the Computer Workstation configuration standards.

**Figure 7: Computer Configuration Standards**




#### 2.30.2.1. Operating System (OS) Hardening:

- **Standardised Images:** Deploy all workstations using a standardised, pre-hardened operating system image approved by the ICT Unit.
- **Latest Patches:** Implement automated patch management for OS and installed applications, ensuring updates are applied promptly.

- **Antivirus/Anti-Malware:** Install and maintain centrally managed antivirus/anti-malware software with real-time protection and regular scans, and endpoint detection and response (EDR) capabilities where feasible.
- **Firewall:** Enable and properly configure the operating system's built-in firewall to block unnecessary incoming connections.
- **User Account Control (UAC):** Ensure UAC or equivalent privilege elevation mechanisms are enabled and configured to prompt for administrative credentials for administrative tasks.
- **Disable Autorun:** Disable the Autorun/AutoPlay feature for all removable media.
- **Disk Encryption:** Encrypt all workstation hard drives (e.g., BitLocker for Windows, FileVault for macOS) to protect data at rest in case of loss or theft.

#### 2.30.2.2. User Account Authentication:

- **Standard User Accounts:** All end-users shall operate with standard user privileges for daily tasks. Administrator accounts shall only be used for elevated privileges and for administrative purposes, using separate credentials.
- **Strong Passwords:** Enforce strong password policies for all user accounts, aligned with the ICT Network Security Policy (minimum 12 characters, complexity, history).
- **Account Lockout:** Configure account lockout thresholds (e.g., 5 failed attempts, 15-minute lockout).
- **Screen Lock:** Configure automatic screen locking after 5-10 minutes of inactivity, requiring re-authentication.
- **Multi-Factor Authentication (MFA):** Implement MFA for remote access (VPN, VDI) and access to critical municipal applications.

#### 2.30.2.3. Software Management:

- **Approved Software List:** Only approved and licensed software from the Municipality's approved software list shall be installed.
- **Prohibited Software:** Prohibit the installation of unauthorised software, peer-to-peer applications, personal cloud storage sync clients, and unnecessary tools.
- **Browser Security:** Configure web browsers with appropriate security settings (e.g., pop-up blockers, enhanced tracking protection, disable unnecessary plugins, restrict untrusted sites).
- **Application Whitelisting/Blacklisting:** Implement application whitelisting for critical systems or, at minimum, application blacklisting to prevent execution of known malicious software.
- **Privilege Elevation:** Control and monitor the use of privilege elevation tools (e.g., sudo on Linux, "Run as administrator" on Windows).
- **Third-Party Application Updates:** Ensure a robust process for timely patching and updating of all third-party applications installed on workstations.

- **Secure Boot/UEFI:** Enable Secure Boot and configure UEFI firmware securely to prevent unauthorised software from loading during startup.

#### 2.30.2.4. Peripherals and Removable Media Control

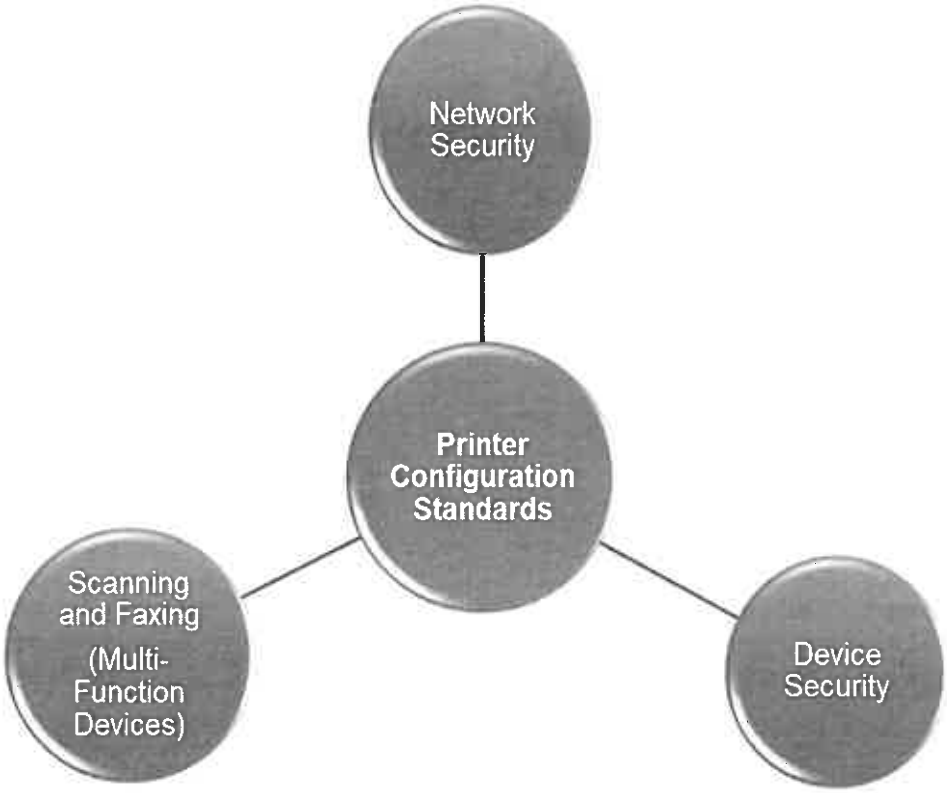
- **USB Device Control:** Implement controls to prevent unauthorised USB device usage (e.g., blocking, whitelisting specific devices).
- **Removable Media Encryption:** All removable media (USB drives, external hard drives) used for municipal data must be encrypted.
- **Port Disabling:** Disable unused physical ports (e.g., USB, FireWire) in the BIOS/UEFI or via Group Policy/MDM.

### 2.30.3. Printer Configuration Standards

Printers, especially network-connected ones, can pose significant security risks.

The following diagram provides an overview of the Printer configuration standards.

**Figure 8: Printer Configuration Standards**



### 2.30.3.1. Network Security:

- **Dedicated VLAN/Network Segment:** Where possible, place network printers on a dedicated VLAN or network segment, isolated from sensitive data networks, with strict firewall rules.
- **Disable Unnecessary Services:** Disable all unnecessary network services (e.g., FTP, Telnet, SNMP v1/v2c, Bonjour, UPnP, Wi-Fi Direct). Only enable services essential for print/scan/copy functionality (e.g., LPR, IPP, SMB where necessary).
- **Firmware Updates:** Regularly update printer firmware to patch known vulnerabilities.
- **Strong Passwords:** Change all default administrator passwords immediately upon deployment. Use strong, unique passwords for all administrative interfaces.
- **Secure Protocols:** Enable and enforce HTTPS for web administration interfaces. Disable HTTP.
- **Port Access:** Restrict access to printer management ports to authorised IP addresses/ranges.

### 2.30.3.2. Device Security:

- **Physical Security:** Place printers in secure locations, especially those handling sensitive documents. Consider physical locks where appropriate.
- **Sensitive Document Handling:** Implement clear policies and procedures for handling and disposing of sensitive documents printed, copied, or scanned, aligned with the Clear Desk Policy.
- **Secure Print/Pull Print:** Implement "Secure Print" or "Pull Print" functionality requiring user authentication (e.g., PIN, card reader) at the device to release print jobs, preventing unauthorised access to printed documents.
- **Hard Drive Overwriting/Encryption:**
    - Configure printers with internal hard drives to automatically overwrite temporary job data after printing.
    - Where possible, enable encryption for the printer's internal hard drive.
    - For end-of-life printers, ensure data on internal storage is securely wiped or physically destroyed.
- **Logging and Auditing:** Enable logging of print jobs, access attempts, and configuration changes. Integrate with the centralised log management system where possible.
- **Disable Guest Access:** Disable any guest or anonymous access features.
- **Out-of-Band Management:** Consider managing printers via a separate, secure management network if supported by the device.

#### 2.30.3.3. Scanning and Faxing (Multi-Function Devices – MDFs):

- **Secure Scan Destinations:** Restrict scan-to-email/folder destinations to approved internal municipal addresses/shares.
- **Email Security:** Ensure scan-to-email functions use secure SMTP (STARTTLS/SSL) with authentication.
- **Fax Security:** If faxing is enabled, ensure a dedicated fax line is used and that faxes are handled securely.

## 2.31. IMPLEMENTATION AND ENFORCEMENT

### 2.31.1. Roles and Responsibilities

**Table 6: Roles and Responsibilities**

| Roles | Responsibility |
|---|---|
| **ICT Unit** | Responsible for developing, implementing, maintaining, and enforcing these standards. |
| **ICT Manager** | Overall responsibility for the security posture and compliance with these standards. |
| **System Administrators** | Responsible for configuring and maintaining systems according to these standards. |
| **End-Users** | Responsible for adhering to policies that impact configurations (e.g., strong passwords, secure screen lock). |
| **Internal Audit** | Will perform independent audits of configuration compliance. |

### 2.31.2. Configuration Management Process

- **Baseline Definition:** Define and document baseline configurations for all asset types covered.
- **Automated Deployment:** Utilise tools (e.g., Group Policy, SCCM, MDM, configuration management platforms like Ansible, Puppet, Chef) to automate the deployment of baseline configurations where feasible.
- **Version Control:** Maintain version control for all configuration templates and scripts.
- **Deviation Management:** Establish a process for identifying, documenting, and approving or remediating deviations from baseline configurations.
- **Configuration Audits:** Regularly audit configurations against established baselines.

### 2.31.3. Change Management

All changes to these baseline configurations must follow the Municipality's formal Change Management Policy, including:

- Change Request Submission and Documentation.
- Impact Assessment (including security impact).
- Risk Assessment.
- Approval by relevant stakeholders (e.g., Change Advisory Board).
- Testing in a non-production environment.
- Implementation plan with rollback procedures.
- Post-implementation review.
- Documentation of the change.

### 2.31.4. Monitoring and Reporting

- Implement tools such as Configuration Management Databases (CMDB), Security Information and Event Management (SIEM) systems, or dedicated compliance monitoring software tools to continuously monitor configurations for unauthorised changes or deviations from baselines.
- Regularly generate reports on configuration compliance.
- Integrate configuration monitoring systems with the municipality's incident response procedures to facilitate rapid detection and response to security incidents originating from misconfigurations.
- Deviations from these Configuration Standards without approved exceptions may result in disciplinary action or restrictions on system access, as outlined in relevant municipal policies.

### 2.31.5. Training and Awareness

- Provide regular information security awareness training to all staff on the importance of secure configurations and their role in maintaining security.
- Provide specialised training for IT personnel responsible for system configuration and management.

## 2.32. REVIEW AND CONTINUOUS IMPROVEMENT

These Configuration Standards shall be formally reviewed and updated by the ICT Unit, in consultation with relevant stakeholders (e.g., ICT Steering Committee, Internal Audit), on an annual basis or as necessitated by:

- Changes in technology.

- Emergence of new threats or vulnerabilities.
- Changes in regulatory requirements.
- Results of internal or external audits and security assessments.
- Lessons learned from security incidents.

## 2.33. PERFORMANCE METRICS

To ensure the effectiveness of configuration standards and alignment with the Municipality's operational goals, the following key performance indicators (KPIs) and metrics are used to measure and monitor compliance, efficiency, and security.

**Table 7: Performance and Metrics**

| Metric | Performance Indicator (KPI) | Target / Benchmark | Measurement Criteria |
|---|---|---|---|
| 1 **Compliance Rate** | % of devices compliant with configuration standards | Servers: ≥ 98%<br>Laptops: ≥ 95%<br>Printers: ≥ 90% | Configuration audits vs. approved baseline checklist |
| 2 **Configuration Drift Incidents** | Number of deviations from approved configuration baseline | Servers: ≤ 1 / quarter<br>Laptops: ≤ 3<br>Printers: ≤ 2 | Logged incidents of non-compliance |
| 3 **Patch Management Compliance** | % of devices with latest security patches | Servers: ≥ 98% within 7 days<br>Laptops: ≥ 95% within 14 | Patch deployment reports from update management tools |
| 4 **Time to Remediate Non-Compliance** | Average time to fix a non-compliant configuration | Servers: ≤ 24 hrs<br>Laptops/Printers: ≤ 48 hrs | Time from detection to remediation logged in ITSM system |
| 5 **Configuration Audit Frequency** | Number of audits conducted per year | Servers: Monthly<br>Laptops: Quarterly<br>Printers: Bi-annual | Audit calendar and reports |
| 6 **Automated Configuration Rate** | % of configurations deployed using automation tools | Servers: ≥ 90%<br>Laptops: ≥ 80%<br>Printers: ≥ 60% | Device setup logs from tools |
| 7 **Standard Build Image Accuracy** | % of deployments using approved configuration images | Laptops: ≥ 95% | Imaging logs, device management platform reports |

| Metric | Performance Indicator (KPI) | Target / Benchmark | Measurement Criteria |
|---|---|---|---|
| 8 **Printer Network Compliance** | % of networked printers correctly configured | ≥ 90% | Verification against IP schema, naming, and access controls |
| 9 **Configuration-Related Downtime** | % of system outages caused by misconfigurations | ≤ 5% of total incidents | Incident root cause analysis logs |
| 10 **User Satisfaction (Config Stability)** | % of users satisfied with standard device setup | Laptops/Printers: ≥ 85% satisfaction | Annual user satisfaction survey results |
| 11 **Change Success Rate** | % of configuration changes implemented without causing incidents | ≥ 98% | Change management logs |
| 12 **Backup Configuration Verification** | % of servers verified for backup and recovery configuration | ≥ 100% of critical servers | Monthly verification logs and backup test results |

# APPENDIX A: FIREWALL PROCEDURE

This appendix provides detailed procedures on firewall management.

## 2.34. SCOPE

This procedure applies to all firewalls (hardware, software, cloud-based, next-generation) deployed across Mandeni Local Municipality's networks, including:

- Perimeter firewalls securing the connection to the internet.
- Internal network segmenting firewalls.
- Firewalls protecting critical servers and applications.
- Firewalls on endpoints (e.g., desktops, laptops, servers).
- Any third-party or cloud services that include firewall functionalities.
- All municipal employees, contractors, and any third parties with access to Municipality's network infrastructure.

This Firewall Procedure incorporates principles and practices from the following:

- COBIT 2019:
  - APO12: Managed Security.
  - BAI06: Managed IT Changes.
  - DSS05: Managed Security Services.
  - MEA01: Monitored, Evaluated and Assessed Performance and Conformance.
- NIST Cybersecurity Framework (CSF).
- ISO 27001.

## 2.35. PURPOSE AND OBJECTIVES

The purpose of this Firewall Procedure is to establish comprehensive guidelines and controls for the selection, configuration, deployment, maintenance, and monitoring of all firewalls within Mandeni Local Municipality's information technology (IT) infrastructure. This procedure aims to:

- Protect Municipality's network and information assets from unauthorised access, misuse, disclosure, modification, or destruction.
- Ensure the confidentiality, integrity, and availability of critical municipal data and services.

- Comply with relevant national regulations, internal policies, and international best practices for cybersecurity.
- Support a secure and resilient IT environment for all municipal operations and citizen services.

## 2.36. ROLES AND RESPONSIBILITY

**Table 8: Roles and Responsibilities**

| Roles | Responsibility |
|---|---|
| **Corporate Services** | Overall accountability for the firewall policy and procedure, ensuring alignment with strategic municipal objectives and risk appetite. |
| **ICT Manager** | Responsible for the implementation, oversight, and enforcement of this procedure. Approves significant firewall changes.<br>Advises on security risks, reviews firewall rules, conducts audits, and ensures compliance with security policies and standards. |
| **Network Administrators / Firewall Administrators** | Responsible for the day-to-day configuration, monitoring, maintenance, and troubleshooting of firewalls. They execute approved changes. |
| **Application/System Owners** | Provide requirements for network access for their applications/systems and review rules affecting their resources. |
| **Internal Audit** | Periodically reviews the effectiveness and compliance of firewall procedures and controls. |

## 2.37. FIREWALL GUIDELINES

### 2.37.1. Firewall Procedure Guidelines

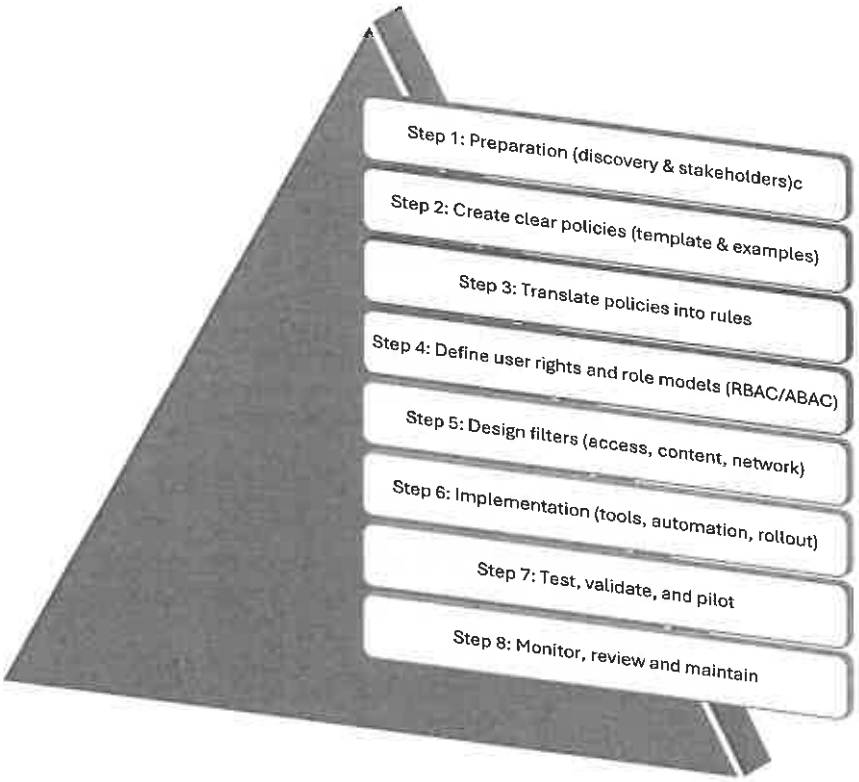
- **Default Deny Principle:** All firewalls shall operate on a "deny-all" by default principle. This means all network traffic is blocked unless explicitly permitted by a specific, approved firewall rule.
- **Network Segmentation:** The municipal network shall be segmented into logical security zones (e.g., DMZ for public-facing services, Internal LAN, Server Farm, Guest Wi-Fi, Administrative Network). Firewalls shall control traffic flow between these zones based on the principle of least privilege.

- **Dedicated Firewalls:** For critical network segments and perimeter defense, firewalls should run on dedicated hardware or virtual appliances. No other non-firewall related software should be installed on these devices.
- **High Availability:** Critical firewalls (e.g., perimeter firewalls) shall be deployed in a high-availability (HA) configuration to ensure continuous service in case of a device failure.
- **Centralised Management:** Where feasible, firewall management should be centralised to ensure consistent policy application and simplified administration.
- **Secure Configuration:**
    - All default credentials must be changed immediately upon installation.
    - Management interfaces must be secured and accessible only from authorised management networks/IPs using strong authentication (e.g., multi-factor authentication where supported).
    - Unnecessary services on the firewall itself (e.g., HTTP, Telnet, FTP) must be disabled.
    - Network Time Protocol (NTP) should be configured for accurate time synchronisation.
- **No Direct Internet Access:** No internal host or network segment, apart from the DMZ, shall have direct, unfiltered access to the internet. All internets bound traffic must pass through the perimeter firewall.

### 2.37.2. Firewall Procedure Configurations

The following figure illustrates the step-by-step firewall configuration standards.

**Figure 9: Firewall Configuration Steps**




**STEP 1: Preparation (discovery & stakeholders)**

- **Identify stakeholders:** Security, HR, IT operations, application owners, legal/compliance, business unit leads.
- **Inventory accounts & systems:** List identity providers, directories, privileged accounts, service accounts and the systems they access.
- **Map sensitive resources & data:** Which systems and data sets are high risk or regulated?
- **Regulatory & legal requirements:** Note password retention, data residency, audit/reporting needs.
- **Define objectives & success metrics:** e.g., 100% MFA for admin roles within 60 days; reduce orphaned accounts by 90%.
- **Risk assessment:** Rank account types by impact (compromise, data exfiltration, admin takeover).

**STEP 2: Create clear policies (template & examples)**

**Policy writing best practices:** use clear language, keep short and actionable, assign owners, include enforcement and exceptions process, set a review cadence.

**Policy template (use this for each account-related policy):**

- **Title:** e.g., Account Management Policy
- **Purpose:** Short statement of intent
- **Scope:** Systems, users, account types covered
- **Definitions:** Key terms used in this policy
- **Policy statements:** Numbered rules (specific high-level requirements)
- **Roles & responsibilities:** Who does what (IT, managers, HR)
- **Enforcement & exceptions:** How violations are handled and how to request exceptions
- **Review cycle & revision history**

**Sample high-level policy statements:**

- All user accounts must be uniquely assigned and linked to a real person or approved service identity. Shared accounts are prohibited except where documented and approved.
- All privileged accounts must use MFA and be recorded in the privileged account inventory.
- Account provisioning and deprovisioning must follow the HR-triggered lifecycle and be automated where possible.
- Passwords must meet complexity and rotation requirements or be replaced by strong authentication methods.
- Access reviews for privileged roles must occur at least quarterly.

**STEP 3: Translate policies into rules**

Turn each policy statement into one or more enforceable rules.

**Rule-writing checklist:**

- Make rules specific and testable (who, what, when, where, how)
- Prefer deny-by-default rules with explicit allow lists
- Encode exceptions in a controlled workflow

Rule examples (plain language → pseudo-rule):

- Policy: All privileged accounts require MFA.
  - Rule (pseudo): IF user.role IN privileged THEN require (MFA) AND disallow (auth_method='SMS')
- Policy: External contractors have limited access.
  - Rule (pseudo): IF user.employment_type=='contractor' THEN allow_access(resource in contractor_catalog) AND deny (resource in sensitive_catalog)
- Policy: No unmanaged device may download sensitive files.

- Rule (pseudo): IF device.managed==false AND file.sensitivity=='high' THEN deny(action=='download')

**Translating to platform controls:**

- Use conditional access policies (IdP or CASB) to implement time/location/device conditions.
- Use group membership or roles to scope permissions.
- Use policy-as-code (OPA, Terraform, Azure Policy) to manage rules in source control.

**STEP 4: Define user rights and role model (RBAC/ABAC)**

**Steps to build roles & rights:**

- **Identify job functions** and the sets of resources they require.
- **Create role archetypes** (Admin, Manager, Power User, Standard User, Read-only, Service Account).
- **Map least privilege**: assign only the permissions necessary for the role.
- **Use groups for assignment** (avoid assigning permissions directly to users).
- **Apply constraints** (time-of-day, network segment, device posture) — this is ABAC style.
- **Privileged Access Management (PAM)**: require just-in-time elevation, session recording, approval workflows for critical tasks.
- **Document role definitions** and owners.

Role matrix sample (short):

**Table 9: Role Matrix**

| Role | Primary responsibilities | Example permissions |
|---|---|---|
| Admin | Manage systems & users | User CRUD, Role assignment, Config |
| Manager | Approve access for team | Approve requests, view reports |
| User | Day-to-day tasks | Read/write own data, use apps |
| Service Account | App-to-app access | API access scoped to service |

**Periodic reviews**: schedule access reviews and orphan account detection.

**STEP 5: Design filters (access, content, network)**

Filters implement fine-grained blocking and inspection.

**Filter categories & where to apply:**

- **Identity / Conditional Access filters:** based on user attributes, group membership, device posture, IP, location, time.
- **Network / Firewall filters:** IP allow/deny, port restrictions, VPN segmentation.
- **Application filters / ACLs:** application-level permission checks and scopes.
- **Content filters / DLP:** detect sensitive data exfiltration in email, file transfer, uploads.
- **Email filters:** spam, phishing, attachment type inspection, external forwarding controls.

**Steps to design filters:**

- Determine what you want to block or monitor (sensitive file upload, access from foreign IPs, unmanaged devices).
- Specify attributes and conditions to match.
- Define actions (block, prompt for step-up auth, quarantine, log-only for tuning).
- Pilot in log-only mode for tuning, then move to enforce.
- Maintain exception process and logging.

**Filter pseudo-example:**

Filter: Block external file-sharing of PII

When user.group != 'AllowedExternalSharing' AND file.tag == 'PII' THEN action = block_upload; notify_security = true

**STEP 6: Implementation (tools, automation, rollout)**

**Implementation steps:**

- **Choose enforcement points**: IdP (Okta, Azure AD), PAM, CASB, firewall, application gateways.
- **Use automation & source control**: store policy/rules as code and deploy via CI/CD.
- **Provisioning workflow**: integrate HR system with IdP (SCIM) for onboarding/offboarding.
- **Logging & SIEM**: forward auth logs, access decisions, and filter events to a central log and alerting system.
- **Change control & approval**: all policy changes should follow change management.

- **Communication & training**: publicize changes to users and provide helpdesk scripts.

**STEP 7: Test, validate and pilot**

- **Pilot group:** test policies with a small representative user set.
- **Log-only mode:** run filters/rules in monitoring mode to collect false positives.
- **Use policy simulation tools** where available (policy simulators, AD group policy modeling).
- **User acceptance testing (UAT):** capture business function owners' sign-off.
- **Rollout plan:** staged rollout (by org unit → by region → global).

**STEP 8: Monitor, review and maintain**

Ongoing operations:

- **Continuous monitoring**: failed logins, MFA failures, anomalous privileged actions.
- **Periodic access reviews**: quarterly for privileged roles, annually for broad access.
- **Policy review cycle**: review policies at least annually or after major incidents.
- **Metrics & KPIs**: MFA coverage, orphaned accounts, average time to deprovision, number of high-severity access incidents.
- **Incident response**: ensure policies map to IR runbooks (who to contact, how to revoke access quickly).

## 2.38. FIREWALL RULE MANAGEMENT PROCEDURE

### 2.38.1. Rule Request and Justification

- All requests for new firewall rules or modifications to existing rules must be formally submitted using a designated change request form/system.
- The request must clearly state:
  - Source IP address(es) or network(s).
  - Destination IP address(es) or network(s).
  - Service(s) and port(s) (e.g., TCP 443 for HTTPS).
  - Direction (Inbound/Outbound).
  - Business justification for the rule (why it is needed).
  - Anticipated duration of the rule (temporary/permanent).
  - Contact person/owner of the application/service.

### 2.38.2. Review and Approval

- All firewall rule requests shall be reviewed by at least two (2) Network/Firewall Administrators.
- Security impact assessment shall be conducted by the ICT Manager (or delegate).
- Approval by the ICT Manager is required for all significant rule changes (e.g., opening new ports to the internet, creating new VPN tunnels).
- For highly sensitive changes, approval from the Corporate Services may be required.

### 2.38.3. Implementation

- Approved rules shall be implemented by authorised Firewall Administrators.
- Changes should ideally be implemented during off-peak hours to minimise disruption.
- Detailed documentation of the change (including date, time, implementer, and reason) must be recorded in the change management system.
- The principle of least privilege must always be applied when creating rules, granting only the necessary access and no more.
- Rules for insecure services (e.g., Telnet, FTP without encryption) are generally prohibited unless exceptional business justification and compensating controls are in place.
- All firewall changes must adhere to the Municipality's overarching IT Change Management policy and procedures.

### 2.38.4. Testing and Verification

- After implementation, the new or modified rule must be immediately tested to verify its functionality and to ensure no unintended side effects (e.g., legitimate traffic being blocked, security gaps created).
- Testing shall be documented.

### 2.38.5. Rule Documentation

- Each firewall rule must have a clear description, including its purpose, associated application/service, and approval reference.
- Rules should be logically grouped (e.g., by application, by network segment) for easier management.

### 2.38.6. Regular Rule Review and Optimisation

- Firewall rulesets shall be reviewed at least quarterly (or more frequently for highly dynamic environments) by Firewall Administrators and the ICT Manager.
  - The review process shall identify and remove:
    - Expired temporary rules.
    - Unused or redundant rules (e.g., rules that have no hits in logs).
    - Overlapping rules.
    - Rules that no longer serve a business purpose.
- The review should also assess the effectiveness of rule ordering.

### 2.38.7. Backups and Version Control

- Firewall configurations (including rulesets) must be backed up regularly (e.g., daily) and stored securely off-device.
- Multiple versions of configurations should be retained to allow for rollbacks if necessary.

## 2.39. MONITORING AND LOGGING

- All firewalls must have logging enabled for both allowed and denied traffic.
- Firewall logs shall be retained for a minimum of 90 days online and archived for at least 1 year (or longer as per legal/compliance requirements).
- Firewall logs shall be sent to a centralised Log Management System (LMS) or Security Information and Event Management (SIEM) system for aggregation, analysis, and correlation.
- Firewall logs shall be reviewed daily by Firewall Administrators for unusual or suspicious activity (e.g., repeated denied connections from external sources, attempts to access unauthorised resources, high volume of traffic from unexpected sources).
- Automated alerts shall be configured within the SIEM/LMS for critical security events detected in firewall logs (e.g., signs of intrusion attempts, Denial of Service attacks).
- Any detected security incidents based on firewall logs shall trigger the municipal Incident Response Plan.
- In the event of a critical firewall failure, suspected compromise, or major Denial of Service (DoS) attack specifically targeting firewall infrastructure, the following immediate steps shall be taken:
  - **Isolate:** Immediately isolate affected segments or devices if safe to do so without causing wider service disruption.
  - **Notify:** Alert the ICT Manager immediately.

- **Assess:** Rapidly assess the scope and impact of the incident.
- **Restore:** Initiate recovery procedures using verified backups or failover systems as per the Incident Response Plan.
- **Document:** All emergency actions and observations must be meticulously documented.

## 2.40. MAINTENANCE AND UPDATE

- Firewall operating systems and firmware must be kept up to date with the latest security patches and updates as released by the vendor. Updates should be tested in a non-production environment before deployment to production firewalls.
- Regular vulnerability scans and penetration tests (at least annually) shall be conducted against the external and internal interfaces of firewalls to identify and address any weaknesses.
- Firewall performance (CPU, memory, throughput) shall be monitored to ensure optimal operation and capacity planning.
- When a firewall appliance or virtual instance is no longer required (e.g., end-of-life, replacement, service discontinuation), a formal decommissioning process shall be followed:
  - **Data Backup:** All configurations, logs, and relevant data must be backed up and archived according to retention policies.
  - **Rule Removal:** All firewall rules associated with the device must be reviewed and removed from other active firewalls if applicable.
  - **Secure Erasure:** For hardware appliances, all sensitive data on storage components must be securely wiped or physically destroyed. For virtual instances, ensure the virtual disk is securely deleted.
  - **Asset Management Update:** The firewall's status must be updated in the asset management system as decommissioned.

## 2.41. PHYSICAL SECURITY AND ENVIRONMENTAL CONTROL

Firewalls, especially hardware appliances, shall be located in secure data centres or server rooms with restricted physical access, appropriate environmental controls (temperature, humidity), and uninterruptible power supply (UPS).

## 2.42. TRAINING AND AWARENESS

All ICT personnel involved in firewall management shall receive appropriate training on firewall technologies, security best practices, and this procedure.

General cybersecurity awareness training for all municipal employees shall include the importance of firewalls in protecting the municipal network.

## 2.43. ENDORSEMENT AND COMPLIANCE

Adherence to this Firewall Management Procedure is mandatory for all Mandeni Local Municipality employees, contractors, and third parties with access to the municipal network infrastructure.

- Compliance with this procedure will be regularly monitored through internal audits, log reviews, and performance assessments.
- Any instances of non-compliance with this procedure may result in disciplinary action, up to and including termination of employment or contract, and potential legal action, depending on the severity and impact of the non-compliance.
- Employees are encouraged to report any suspected violations of this procedure to the ICT Manager.

## 2.44. PERFORMANCE METRICS

Below are performance metrics for Mandeni Local Municipality's Firewall Procedure. This ensures alignment with governance and operational best practices.

**Table 10: Firewall Performance Metrics**

| Metric | Performance Indicator (KPI) | Target / Benchmark | Measurement Criteria |
|---|---|---|---|
| 1 **Firewall Configuration Compliance** | % of firewall rules compliant with approved baseline policy | ≥ 98% | Configuration audit reports against the documented firewall standards |
| 2 **Change Request Turnaround Time** | Average time to review and implement approved firewall rule changes | ≤ 48 hours | Time from request submission to implementation logged |

| Metric | Performance Indicator (KPI) | Target / Benchmark | Measurement Criteria |
|---|---|---|---|
| | | | in change control system |
| 3 **Unauthorised Rule Detection Rate** | Number of firewall rules not approved or undocumented | 0 (Zero tolerance) | Monthly configuration reviews and audit trail analysis |
| 4 **Firewall Rule Review Frequency** | Frequency of firewall rule base review and cleanup | Quarterly | Documented review logs and rule change history |
| 5 **Intrusion Prevention Efficacy** | % of intrusion attempts blocked by the firewall | ≥ 99% | Firewall logs showing detected and blocked intrusion attempts |
| 6 **Firewall Uptime / Availability** | Percentage of time the firewall is operational and available | ≥ 99.9% uptime | Monitoring system availability reports |
| 7 **Log Retention Compliance** | % of firewall logs retained according to policy (e.g., 90 days minimum) | 100% | Log retention policy vs actual log storage confirmation |
| 8 **Incident Response Integration** | % of detected firewall events escalated to the incident response team | ≥ 95% of critical events | Cross-reference of firewall alerts and incident management system |
| 9 **Penetration Test Findings Resolved** | % of firewall-related vulnerabilities fixed from external/internal tests | 100% within 30 days | Remediation logs and test report follow-ups |
| 10 **Staff Access to Firewall System** | % of staff with firewall access authorised and documented | 100% | Access control list review against approved user roles |
| 11 **Change Success Rate** | % of firewall changes executed without causing unplanned downtime | ≥ 98% | Post-change reviews and system availability metrics post-implementation |
| 12 **Configuration Backup Frequency** | Frequency of automatic or manual firewall configuration backups | Daily (at minimum) | Backup logs and verification of backup recovery success |

# APPENDIX B: ANTIVIRUS PROCEDURE

This appendix provides detailed procedures on antivirus management.

## 2.45. SCOPE

This procedure applies to all IT assets owned or managed by Mandeni Local Municipality, including but not limited to:

- All desktop computers, laptops, and tablets.
- All servers.
- Mobile devices (smartphones, tablets) connected to the municipal network or used for municipal business.
- Network devices capable of hosting antivirus software (e.g., some next-generation firewalls, intrusion prevention systems, where applicable).
- All removable media (USB drives, external hard drives) used within the municipal environment.
- Cloud-based services and platforms that handle municipal data, where endpoint protection is applicable and managed by Mandeni Local Municipality.

This antivirus procedure incorporates principles and practices from the following:

a. COBIT 2019:

- APO12: Managed Security.
- BAI03: Managed Identification and Build.
- BAI06: Managed IT Changes.
- DSS02: Managed Service Requests and Incidents.
- DSS05: Managed Security Services.
- MEA01: Monitored, Evaluated and Assessed Performance and Conformance.

b. NIST Cybersecurity Framework (CSF).
c. ISO 27001.

This procedure applies to all municipal employees, contractors, third-party vendors, and any other individuals with access to Municipality's IT systems.

## 2.46. PURPOSE AND OBJECTIVES

The purpose of this Antivirus Procedure is to establish comprehensive guidelines and controls for the selection, deployment, configuration, management, monitoring, and response to malicious software (malware) threats across Mandeni Local Municipality's information technology (IT) environment. This procedure aims to:

- Protect Municipality's IT infrastructure, data, and services from viruses, worms, Trojans, ransomware, and other forms of malware.
- Minimise the risk of data breaches, system downtime, and reputational damage due to malware infections.
- Ensure the confidentiality, integrity, and availability of critical municipal data, including personal information as required by Protection of Personal Information Act (POPIA).
- Maintain a secure and resilient computing environment for all municipal employees and operations.
- Comply with relevant national regulations, internal policies, and international cybersecurity best practices.

## 2.47. ROLES AND RESPONSIBILITY

**Table 11: Roles and Responsibilities**

| Roles | Responsibility |
|---|---|
| Corporate Services | Overall accountability for the Antivirus Policy and Procedure, ensuring strategic alignment with municipal objectives and risk appetite. Endorses the selection of antivirus solutions. |
| ICT Manager | Responsible for the implementation, oversight, and enforcement of this procedure. Approves significant changes to antivirus solutions, deployment strategies, and high-level policy configurations.<br>Advises on malware threats and trends, reviews antivirus effectiveness, conducts regular audits of compliance with this procedure, and ensures alignment with broader security policies and standards (especially POPIA). Involved in defining exclusions. |
| Systems Administrators / Endpoint Protection Administrators | Responsible for the day-to-day deployment, configuration, monitoring, maintenance, and |

| Roles | Responsibility |
|---|---|
| | troubleshooting of antivirus software, including signature updates, policy enforcement, and initial incident response for malware detections. |
| End-Users (All Employees) | Responsible for adhering to this procedure, promptly reporting suspected malware infections to the IT Helpdesk, and not attempting to disable or interfere with antivirus software. |
| Internal Audit | Periodically reviews the effectiveness and compliance of antivirus procedures and controls, reporting findings to senior management. |

## 2.48. ANTIVIRUS GUIDELINES

### 2.48.1. Antivirus Procedure Guidelines Configurations

- **Mandatory Deployment**: Approved antivirus/endpoint protection software must be installed, enabled, and actively running on all applicable IT assets. No exceptions are permitted without explicit, documented approval from the ICT Manager, with clear compensating controls in place.
- **Centralised Management:** A centralised antivirus/endpoint protection management console shall be used to deploy, configure, monitor, and update antivirus software across the municipal network. This ensures consistent policy application and efficient administration.
- **Real-time Protection:** All antivirus software must be configured for real-time (on-access) scanning to detect and block malware as it attempts to access or execute on a system.
- **Automatic Updates:** Antivirus definition files (signatures) and software components must be automatically updated at least hourly, or more frequently if critical threats emerge and vendor updates are available. Automated alerts will be configured to notify administrators if updates fail or clients are out-of-date.
- **Scheduled Scans:** Full system scans must be scheduled to run regularly (e.g., daily for workstations when not in heavy use, weekly for servers during off-peak hours) on all devices. Quick scans may be run more frequently to ensure rapid detection.
- **Quarantine and Remediation:** Antivirus software must be configured to automatically quarantine or block detected malware. Infected files or systems must be isolated promptly, and automated remediation actions (e.g., deletion, cleaning) configured according to policy.

- **Mobile Device Protection:** All municipal-issued mobile devices accessing municipal resources or handling municipal data must have approved mobile endpoint protection solutions installed and configured. Personal devices accessing municipal resources should comply with relevant Bring Your Own Device (BYOD) security policies, which should include antivirus requirements.
- **Removable Media Scans:** All removable media (USB drives, external hard drives) must be scanned automatically upon connection to any municipal device before access is granted. If the device does not support automatic scanning, it must be manually scanned before use.
- **Prohibition of Unauthorised Software:** Users are strictly prohibited from installing or running unauthorised software on municipal devices, as this can bypass antivirus controls and introduce vulnerabilities.
- **Regular Assessment:** The effectiveness of the chosen antivirus solution should be regularly assessed against new threats, benchmarked against industry standards, and alternative solutions investigated based on emerging threat landscapes and vendor performance. This includes reviewing False Positives and False Negatives.

### 2.48.2. Antivirus Procedure Configurations

#### Step 1: Plan & inventory

- List interfaces (LAN, DMZ, WAN), subnets, critical servers and apps, and which user groups (employees, contractors, contractors-vpn, admins) need access.
- Decide the order of policies (FortiGate evaluates policies top→down per interface pair — ordering matters).

#### Step 2: Configure authentication sources (LDAP / RADIUS / local)

**Why**: you'll bind user/groups from your identity system to firewall policies (user-based access). Typical choices:

- **LDAP** (Active Directory) for domain users.
- **RADIUS** for MFA integrations or other RADIUS servers / FortiAuthenticator.
- **Local** for stand-alone accounts.

**GUI flows (examples)**

- LDAP: User & Authentication → LDAP Servers → Create New. Configure server IP, DN, CN identifier, secure connection, bind account.

- RADIUS: User & Authentication → RADIUS Servers → Create New. Fill server, secret, service (PAP/CHAP etc.).

**CLI examples (LDAP + RADIUS)**

(Replace names/IPs/credentials with your values.)

```
config user ldap
        edit "CorpLDAP"
                set server "10.10.10.10"
                set cnid "sAMAccountName"
                set dn "dc=example,dc=com"
                set type regular set username "binduser"
                set password ********
        next
end
config user radius
        edit "DuoRadius"
                set server "10.10.20.20"
                set secret "radsecret"
                set auth-type pap
        next
end
```

### Step 3: Create user objects & user groups

GUI: User & Authentication → User Groups → Create New. Choose type (Firewall, LDAP, RADIUS, FSSO, etc.) and add members/remote group mappings.

**CLI example**

```
config user group
  edit "Employees"
    set member "CorpLDAP"        # for LDAP remote server
```

```
    set group-type ldap
  next
end
```

(You can also create local users under config user local and add them to groups.)

**Tip**: use group naming that reflects access (e.g., HR_readonly, Dev_admins).

### Step 4: Create address & service objects/groups

Use address objects (not raw IPs) so policies are readable and reusable. GUI: Policy & Objects → Addresses → Create New. CLI config firewall address is used for address objects.

**CLI example**

```
config firewall address
 edit "WebServer-Prod"
   set subnet 10.20.30.40 255.255.255.255
next
end
config firewall addrgrp
 edit "WebServers"
   set member "WebServer-Prod" "WebServer-Admin"
  next
end
```

### Step 5: Build security profiles (filters): Web Filter, App Control, IPS, AV, DLP, SSL Inspection

**Overview**: FortiGate security profiles are attached to firewall policies to add content-level protections. Create profiles first, then attach them to policies.

**Web Filter**

- GUI: Security Profiles → Web Filter → Create New — define URL categories, static URL filters, safe search, block/monitor actions. You can set "monitor" to log-only while tuning.

**Application Control**

- GUI: Security Profiles → Application Control → Create New — create application sensors that block or monitor application categories. Apply to policies.

**IPS (Intrusion Prevention)**

- GUI: Security Profiles → Intrusion Prevention → Create New — choose signatures, filters and default actions (detect/block). Keep signatures updated.

**DLP**

- GUI: Security Profiles → Data Loss Prevention → Create New — add rules (keywords, file types, regex, fingerprints) and actions (monitor, block, quarantine). Start in monitor mode.

**SSL / SSH inspection (required for HTTPS content inspection)**

- If you intend to inspect HTTPS (webfilter/IPS/DLP deep inspection), create an SSL inspection profile and configure deep inspection; clients will need the FortiGate CA in trusted stores.

**CLI example — (attach profiles later to a policy)**

```
# create an application list (sensor)
config application list
 edit "Updates_Only"
  config entries
   edit 1
    set category 17
      set action pass
  next
end
```

next

end

(Profiles are usually created in GUI; CLI names/keys come from the profile names.)

**Step 6: Create the user-aware firewall policy (tie users → policy → filters)**

**GUI path**: Policy & Objects → IPv4 Policy (or Policy & Objects → Firewall Policy) → Create New.

Key fields to set:

- **Incoming interface (srcintf)** and **Outgoing interface (dstintf)**
- **Source address** and **Destination address** (use objects)
- **Service** (TCP/UDP/ALL or specific)
- **Source user/group** — select the user group you created (e.g., Employees). This is the user-binding that makes the policy account aware. Fortinet Documentation
- **Security Profiles**: enable Web Filter, App Control, IPS, Antivirus, DLP, and SSL Inspection profile as needed. Fortinet Documentation+2Fortinet Documentation+2
- **Logging**: set logtraffic all (or as appropriate) to record matches for tuning.

**CLI example (full sample policy)**

config firewall policy

edit 100

set name "LAN_to_WAN_UserBased"

set srcintf "lan"

set dstintf "wan1"

set srcaddr "LAN_NET"

set dstaddr "all"

set action accept

set schedule "always"

set service "ALL"

set groups "Employees" # user group binding (user-aware

```
policy)
        set utm-status enable
        set webfilter-profile "WF-Default"
        set av-profile "AV-Default"
        set ips-sensor "IPS-Protect"
        set application-list "Updates_Only"
        set ssl-ssh-profile "DeepInspect" # if you created an SSL inspection
profile
        set nat enable
        set logtraffic all
 next
end
```

(UTM/profile CLI options such as set webfilter-profile, set av-profile, set ips sensor, set application-list, and set utm-status enable are supported — see the firewall policy CLI reference.)

**Important**: if you apply deep SSL inspection for web filtering/IPS/DLP, ensure proper certificate deployment to avoid client errors.

**Step 7: Tuning & testing (monitor mode first)**

- Put new web/app/IPS/DLP profiles in monitor/log mode where possible to collect matches without blocking (many profiles support "monitor"/"detect" vs "block"). Tune signatures and exceptions. Fortinet Documentation+1
- Use the policy log (Log & Report → Forward Traffic) and the policy hit counters to verify which rules matched. FortiGate evaluates policies top→down so check ordering if a rule never matches. Fortinet Documentation+1
- Test with representative users and devices; check for false positives (exempt/monitor lists, static URL exceptions). Yuri's IT Security Blog

**Step 8: Deployment & operations**

- Roll out staged: pilot group → department → global. Use change control. Configure central logging (FortiAnalyzer or SIEM) to collect logs for alerting and periodic audits. (Fortinet documentation/administration guides cover FortiAnalyzer integration.)
- Schedule periodic access reviews and signature updates (IPS, AV, FortiGuard updates).

## 2.49. ANTIVIRUS DEPLOYMENT AND CONFIGURATION PROCEDURE

- **Solution Selection:** The selection of antivirus/endpoint protection software shall involve a thorough evaluation process, considering:
  - Vendor reputation and market standing.
  - Detection capabilities (signature-based, heuristic, behavioural, AI/ML-driven).
  - Performance impact on endpoints and servers.
  - Management capabilities (centralised console, reporting, alerting).
  - Compatibility with existing IT infrastructure.
  - Cost-effectiveness.
  - South African vendor support and local presence, if applicable.

- **Standardised Deployment:**
  - A standard antivirus client package will be used across the Municipality where feasible, often integrated with device provisioning.
  - Deployment to new devices (desktops, laptops, servers) must occur as part of the standard IT asset provisioning process before the device is put into production.
  - For existing devices, a phased deployment or verification process will ensure full coverage.

- **Policy Configuration (Centralised Console):**
  - Policies for real-time scanning, scheduled scans, update frequency, and remediation actions will be configured via the centralised management console.
  - Policies will differentiate between workstation and server environments based on performance and security requirements (e.g., specific exclusions for server applications).
  - Exclusions (e.g., for legitimate applications or specific directories) must be strictly managed, documented, justified, and periodically reviewed (at least quarterly) and approved by the ICT Manager to minimise risk.

- **Signature and Engine Updates:**
  - The antivirus management server(s) must be configured to automatically download updates from the vendor and distribute them to client machines.
  - A fallback mechanism (e.g., direct internet update for roaming laptops, cloud-based updates) should be in place for devices not regularly connected to the internal network.
  - Automated alerts will be configured to notify administrators if update distribution fails or clients are consistently out-of-date.

- **Advanced Endpoint Protection Features:**
  - Where available, advanced endpoint protection features such as Host-based Intrusion Prevention Systems (HIPS), web filtering, application control, device control, ransomware protection, and Endpoint Detection and Response (EDR) capabilities should be configured and leveraged to enhance protection. These capabilities provide deeper insights into endpoint activity and enable faster response to sophisticated threats. These features must be carefully tested before full deployment.

## 2.50. MONITORING AND REPORTING

- **Centralised Logging:** All antivirus events (detections, clean-ups, blocks, updates, errors, policy violations) must be logged and sent to the centralised management console. Critical events should also be forwarded to the municipal SIEM (Security Information and Event Management) system for aggregation, analysis, and correlation with other security data.
- **Regular Review of Reports:** Systems/Endpoint Protection Administrators shall daily review reports from the antivirus management console and SIEM for:
  - Detected and quarantined malware, especially new or unusual strains.
  - Unresolved infections or persistent threats.
  - Devices with out-of-date clients or failed updates.
  - Unauthorised attempts to disable antivirus software.
  - Trends in malware activity and common infection vectors.
- **Alerting:** Automated alerts shall be configured within the SIEM/LMS for critical security events, such as:
  - New or widespread malware outbreaks.
  - Critical systems (e.g., financial servers, database servers) reporting infections.
  - Antivirus service stoppages or unauthorised disabling on critical devices.

- Repeated failed attempts to update signatures or communicate with the management server.

- **Incident Response for Malware:**
  - Upon detection of a confirmed malware infection, the responsible Systems/Endpoint Protection Administrator shall immediately isolate the affected device(s) from the network (e.g., disconnect network cable, quarantine via endpoint solution) to prevent further spread.
  - The incident must be immediately reported to the ICT Manager.
  - The municipal Incident Response Plan shall be activated.
  - Remediation steps include but are not limited to:
    - Detailed analysis of the infection (type of malware, entry point, scope of compromise).
    - Full system scan and cleanup using updated definitions and potentially supplementary tools.
    - Reimaging or rebuilding the affected device(s) if necessary to ensure complete eradication.
    - Password resets for affected user accounts.
    - Communication with affected users.
    - Post-incident review to identify root causes, improve controls, and update this procedure as needed.
    - For personal information breaches caused by malware, relevant sections of POPIA must be adhered to. Legal counsel should be consulted if personal information is compromised.

## 2.51. MAINTENANCE AND UPDATE

- Antivirus software versions (client and server components) must be kept current. Major version upgrades will be planned and executed in a controlled manner, with testing in a non-production environment before widespread deployment, to take advantage of new features and improved protection capabilities.
- Regular monitoring of system performance on devices running antivirus software will be conducted to identify and address any resource conflicts or degradation. Configuration adjustments may be made based on these observations.
- Centralised antivirus management console configurations and policies must be regularly backed up to enable rapid recovery in case of system failure.
- When antivirus software or a management system component is no longer required (e.g., end-of-life, replacement, service discontinuation), a formal decommissioning process shall be followed:

- **Data Backup:** All configurations, logs, and relevant data must be backed up and archived according to retention policies.
- **Software Uninstallation:** Antivirus client software must be properly uninstalled from all affected endpoints and servers.
- **Management System Removal:** If a centralised management server is being decommissioned, ensure all associated databases and configurations are securely removed or archived.
- **Asset Management Update:** The status of the antivirus software/system must be updated in the asset management system as decommissioned.

## 2.52. TRAINING AND AWARENESS

All municipal employees shall receive mandatory cybersecurity awareness training at least annually, and upon onboarding. This training will specifically cover:

- The critical importance of antivirus protection for municipal operations and data (including POPIA compliance).
- Common malware vectors (e.g., phishing emails, suspicious attachments, malicious websites, infected removable media).
- How to identify potential malware threats (e.g., unusual pop-ups, system slowdowns, unexpected emails).
- The procedure for reporting suspected malware infections to the IT Helpdesk immediately.
- The strict prohibition against disabling, uninstalling, or tampering with antivirus software.
- Secure handling of removable media.

Regular communications (e.g., emails, intranet announcements, posters) will reinforce antivirus best practices and general cybersecurity hygiene.

## 2.53. ENFORCEMENT AND COMPLIANCE

Adherence to this Antivirus Procedure is mandatory for all Mandeni Local Municipality employees, contractors, and third parties with access to the municipal IT systems.

- Compliance with this procedure will be regularly monitored through internal audits, system reports, and performance assessments.
- Any instances of non-compliance with this procedure may result in disciplinary action, up to and including termination of employment or contract, and potential legal action, depending on the severity and impact of the non-compliance.

- Employees are encouraged to report any suspected violations of this procedure to the ICT Manager.

## 2.54. PERFORMANCE METRICS

Below are performance metrics for Mandeni Local Municipality's Antivirus Procedure referencing governance components, which ensures proper protection against malware, viruses, and other malicious software across the Municipality's IT infrastructure.

**Table 12:Antivirus Performance Metric**

| Metric | Performance Indicator (KPI) | Target / Benchmark | Measurement Criteria |
|---|---|---|---|
| 1 **Antivirus Installation Coverage** | % of endpoints (servers, laptops) with antivirus installed | 100% | Endpoint management reports vs. asset inventory |
| 2 **Real-Time Protection Enabled** | % of antivirus agents with real-time protection turned on | ≥ 98% | Antivirus management console reports |
| 3 **Signature Update Compliance** | % of devices with up-to-date virus definitions | ≥ 98% updated within 24 hours of release | Update logs from antivirus software |
| 4 **Scheduled Scan Completion Rate** | % of devices completing scheduled scans | ≥ 95% weekly scan completion | Antivirus platform scan logs |
| 5 **Threat Detection Rate** | % of known malware successfully detected during scans | ≥ 99% | Antivirus test logs or third-party validation results |
| 6 **Time to Quarantine or Remove Threat** | Average time from detection to threat isolation/removal | ≤ 4 hours | Threat incident logs with timestamps |
| 7 **False Positive Rate** | % of benign files incorrectly flagged as threats | ≤ 1% | Analysis of alert logs and user-reported issues |
| 8 **Antivirus Policy Compliance** | % of systems adhering to antivirus policy (e.g., no exclusions) | 100% | Policy audit reports vs. current antivirus settings |

| Metric | Performance Indicator (KPI) | Target / Benchmark | Measurement Criteria |
|---|---|---|---|
| 9 **Incident Response Escalation Rate** | % of critical antivirus alerts escalated to security team | ≥ 95% | Antivirus logs vs. incident ticketing system records |
| 10 **Antivirus License Compliance** | % of devices covered by valid antivirus licenses | 100% | Licensing inventory vs. number of active installations |
| 11 **User Awareness and Training** | % of users trained on malware prevention and antivirus reporting | ≥ 90% annually | Training records, attendance logs, and phishing test results |
| 12 **Antivirus System Uptime** | Availability of central antivirus server or management console | ≥ 99.9% | Uptime reports from monitoring tools |

# PATCH MANAGEMENT PROCEDURE

## 2.55. SCOPE

This procedure applies to:

- All servers, desktops, laptops, mobile devices, and network equipment owned and managed by Mandeni Local Municipality.
- Third-party applications, operating systems, and firmware.
- Cloud and hosted solutions under municipal control.
- Systems supporting critical services such as finance, public records, and municipal service delivery.

This procedure is strategically aligned with two internationally recognised frameworks (i.e. COBIT 2019, NIST Cybersecurity Framework (CSF) and ISO 27001).

## 2.56. PURPOSE AND OBJECTIVES

This procedure outlines a structured, step-by-step approach for identifying, testing, deploying, and documenting patches across all information systems within Mandeni Local Municipality. The aim of the Patch Management Procedure is to ensure that all systems, applications, and devices are safeguarded against known vulnerabilities through timely, consistent, and well-controlled patching. This ensures timely remediation of vulnerabilities and reduces the risk of cyber incidents.

This procedure supports compliance with COBIT 2019 (DSS05 - Manage Security Services & APO12 - Manage Risk), ISO/IEC 27001 (Technical Vulnerability Management), and NIST CSF (Vulnerability Management).

The Patch Management procedure is designed to achieve the following key objectives:

- Reduce exposure to security vulnerabilities and threats by applying patches promptly.
- Ensure uniform and documented processes for acquiring, testing, approving, and deploying patches.
- Minimise downtime and service disruptions during patching.
- Maintain compliance with relevant security and governance standards.
- Establish accountability and monitoring for patch management activities.

## 2.57. ROLES AND RESPONSIBILITIES

### 2.57.1. Roles and Responsibilities

**Table 13: Roles and Responsibility**

| Role | Responsibility |
|---|---|
| ICT Manager | • Oversees patch management<br>• Approves exceptions<br>• Ensures compliance with policy |
| System Administrators | • Identify patches, perform testing, deploy patches on assigned systems<br>• Update the Patch Register<br>• Monitors patch compliance<br>• Evaluate Risks |
| Helpdesk/ ICT Support | • Communicates patching impact to end-users<br>• Escalates patch-related incidents |
| Vendors / Third Parties | • Apply patches to outsourced services or systems as per SLA |
| End Users | • Ensure devices are available for patching<br>• Report any post-patch issues |

## 2.58. PATCH MANAGEMENT LIFECYCLE

The Patch Management Lifecycle involves seven key steps: identifying vulnerabilities and patches, assessing and prioritising them based on risk, testing in a staging environment, deploying in production during controlled windows, and then verifying installation through scans and reports. All activities are documented and reported, with exceptions formally managed and approved. This cycle ensures patches are applied consistently, securely, and with minimal disruption to municipal services.

**Figure 10** below illustrates a summary of the seven phases in the Patch Management Lifecycle

**Figure 10 : Patch Management Lifecycle**


### Step 1 – Vulnerability and Patch Identification

- Monitor sources (vendor advisories, threat intelligence, CVE database, MSRC, etc.).
- System Administrators reviews new patches bi-weekly.

### Step 2 – Patch Assessment and Prioritisation

- Classify patches based on severity:
  - Critical – Exploited in the wild / high business impact (deploy within 48–72 hours).
  - High – Security vulnerabilities with significant risk (deploy within 7 days).
  - Medium/Low – General bug fixes or enhancements (deploy within 30 days).

### Step 3 – Testing

- Test patches in a staging environment before production deployment.

- Validate compatibility with critical applications (financial systems, HR systems, municipal service apps).
- Rollback plans documented before deployment.

**Step 4 – Deployment**

- Schedule patching during non-business hours where possible.
- Deploy critical patches immediately if risk is high.
- Automate patch deployment using centralised tools (e.g., WSUS, SCCM, or open-source equivalents).
- Maintain audit trails.

**Step 5 – Verification and Validation**

- Confirm successful patch installation via reports or endpoint checks.
- Perform vulnerability scans post-deployment.
- Update asset inventory with patch status.

**Step 6 – Documentation and Reporting**

- Maintain records of:
    - Patch ID, system patched, date/time, responsible person.
    - Testing outcomes and approval evidence.
- Monthly reports submitted to ICT Manager.

**Step 7 – Exception Handling**

- Where patching cannot be applied (legacy systems, application conflicts):
    - Document risk acceptance and compensating controls (e.g., firewall restrictions, network segmentation).
    - Review exceptions quarterly.

## 2.59. TOOLS AND TECHNOLOGIES

This section describes the software, systems, and technical solutions that support the entire patch management process. Its purpose is to ensure that patching is not done manually and inconsistently, but instead through automated, controlled, and verifiable methods.

- Automated patch deployment tools (Microsoft WSUS, SCCM, or open-source alternatives).
- Vulnerability scanners (OpenVAS, Nessus, Qualys).
- Centralised logging (SIEM).

## 2.60. LEGAL AND REGULATORY

Compliance with laws and regulations is paramount for Mandeni Local Municipality.

- Protection of Personal Information Act (POPIA), 2013 (Act No. 4 of 2013)
- Municipal Finance Management Act (MFMA), 2003 (Act No. 56 of 2003)
- Municipal Systems Act, 2000 (Act No. 32 of 2000)
- Electronic Communications and Transactions Act (ECTA), 2002
- ISO/IEC 27001:2022
- NIST Cybersecurity Framework (CSF)
- Control Objectives for Information and Related Technology (COBIT) 2019.

## 2.61. PERFORMANCE METRICS

Below is a table outlining Performance Metrics for the Patch Management procedure of Mandeni Local Municipality.

**Table 14: Key Performance Metrics**

| Metric | Performance Indicator (KPI) | Target / Benchmark | Measurement Criteria |
|---|---|---|---|
| **Patch Deployment Timelines** | % of critical patches deployed within required timeframe | 95% of critical patches applied within 72 hours | Review system patch logs, deployment reports, and change management records |
| **Overall Patch Compliance** | % of systems fully patched (OS, | 100% compliance for supported systems | Vulnerability scan reports and patch compliance dashboards |

| Metric | Performance Indicator (KPI) | Target / Benchmark | Measurement Criteria |
|---|---|---|---|
| | applications, firmware) | | |
| **Testing Effectiveness** | % of patches tested before deployment | 100% of patches tested in staging environment | Testing logs, approval records, rollback documentation |
| **Patch Failure Rate** | % of failed or rolled-back patches | Less than 5% | Post-deployment verification, system error logs, helpdesk incident reports |
| **Exception Management** | % of patch exceptions formally documented and approved | 100% of exceptions documented and reviewed quarterly | Exception logs, ICT Manager approval records |
| **Vulnerability Reduction** | % decrease in known vulnerabilities after patching | 90% reduction in detected vulnerabilities post-patch | Pre- and post-patch vulnerability scan comparisons |
| **Reporting & Audit Readiness** | % of patching reports submitted on time to ICT Manager | 100% monthly reporting compliance | Patch management reports, submission timestamps |
| **User Impact** | Number of unplanned service outages due to patching | 0 major outages | Incident management records, downtime reports |

## 2.62. REVIEW CYCLE

This procedure shall be reviewed annually or when significant changes in IT infrastructure occur or major security incidents arise.

# IT OPERATIONS PROCEDURE

## 2.63. SCOPE

The scope of this IT Operations Procedure Document is to define a unified and standardised set of operational procedures for the management of key Information and Communication Technology (ICT) functions within Mandeni Local Municipality. The document focuses on ensuring secure, reliable, and consistent ICT operations that support service delivery, governance, and business continuity.

This procedure specifically covers the end-to-end operational requirements for **data backup and retention**, **website management**, and **server room management** as integrated components of ICT operations. It establishes controls for data protection, system availability, infrastructure security, and operational efficiency.

This procedure applies to:

- All municipal ICT systems.
- Municipal servers and storage infrastructure.
- Municipal websites and web applications.
- All ICT personnel, service providers, and authorized users.
- Municipal server room facilities.

All procedures within this document are benchmarked against the principles and control objectives of COBIT 2019 to ensure strong governance, risk management, compliance, and continuous improvement of ICT services within the Municipality.

## 2.64. PURPOSE AND OBJECTIVES

The purpose of this IT Operations Procedure is to establish standardised processes for the management of ICT operational activities within Mandeni Local Municipality. This procedure provides guidance for Data Backup and Retention, Website Management, and Server Room Management to ensure confidentiality, integrity, availability, and recoverability of municipal information assets.

This Procedure is designed to achieve the following key objectives:

- Protect municipal information assets.
- Ensure business continuity and disaster recovery readiness.
- Maintain secure and reliable website services.
- Safeguard ICT infrastructure located within server rooms.

- Ensure compliance with applicable legislation, standards, and governance frameworks.

## 2.65. IT OPERATIONS PROCEDURE MANAGEMENT ROLES AND RESPONSIBILITIES

### 2.65.1. Roles and Responsibilities

**Table 15: Roles and Responsibilities**

| Role | Responsibilities |
|---|---|
| **ICT Manager** | • Approves operational procedures.<br>• Ensures implementation and compliance.<br>• Reviews operational performance. |
| **System and Web Administrator** | • Executes backups.<br>• Maintains servers and storage systems.<br>• Monitors server room conditions.<br>• Maintains website content and functionality.<br>• Ensures website security and availability. |
| **Network Administrator** | • Manages LAN/WAN connectivity and network devices.<br>• Maintains server room physical infrastructure (cabling, racks, UPS).<br>• Supports installation and configuration of ICT equipment.<br>• Monitors network performance and resolve connectivity issues.<br>• Ensures environmental controls in the server room. |
| **IT Technician & helpdesk** | • Supports municipal applications (financial systems, HR systems, etc.).<br>• Troubleshoots application-related issues.<br>• Coordinates system upgrades and vendor support.<br>• Ensures application availability and user support. |
| **End Users** | • Adhere to ICT policies and procedures.<br>• Report incidents and operational issues. |

| Role | Responsibilities |
|---|---|
| Service Providers | • Deliver services according to approved agreements and security requirements. |

**Delegation of Authority:** While specific roles are assigned responsibilities, delegation of tasks is permissible, provided that the delegating party retains accountability and ensures the delegate is appropriately trained and authorised.

## 2.66. DATA BACKUP AND RETENTION PROCEDURE

### 2.66.1. Purpose

To ensure municipal information and systems can be recovered in the event of accidental deletion, corruption, cyber incidents, hardware failure, or disasters.

### 2.66.2. Backup Requirements

The municipality shall maintain backups for:

- Application servers.
- Databases.
- File servers.
- Virtual machines.
- Configuration files.
- Critical municipal records.

### 2.66.3. Backup Schedule

**Table 16: Backup Schedule**

| Backup Type | Frequency |
|---|---|
| Incremental Backup | Daily |
| Full Backup | Weekly |
| Archive Backup | Monthly |

### 2.66.4. Backup Storage

Backups shall be stored:

- On designated backup storage systems.
- At an offsite location or cloud repository where approved.
- In encrypted format where technically feasible.

### 2.66.5. Backup Retention

**Table 17: Backup Retention**

| Backup Type | Retention Period |
|---|---|
| Daily Backups | 30 Days |
| Weekly Backups | 3 Months |
| Monthly Backups | 12 Months |
| Annual Archives | 5 Years or as required by legislation |

### 2.66.6. Backup Testing

- Backup restoration testing shall be conducted at least quarterly.
- Results shall be documented and retained for audit purposes.

### 2.66.7. Monitoring

ICT personnel shall review backup logs daily and investigate backup failures promptly.

## 2.67. WEBSITE MANAGEMENT PROCEDURE

### 2.67.1. Purpose

To ensure the municipal website remains secure, accurate, accessible, and available to stakeholders.

### 2.67.2. Website Governance

The municipal website shall:

- Support service delivery objectives.
- Provide accurate and current information.
- Comply with applicable legislative requirements.

### 2.67.3. Content Management

- Content updates shall be authorized by the department responsible.
- Content shall be reviewed before publication.
- Outdated content shall be removed or updated promptly.

### 2.67.4. Website Security

ICT shall ensure:

- Secure hosting environments.
- Timely application of security patches.
- SSL/TLS certificates remain valid.
- Administrative accounts are protected using strong passwords and MFA where possible.

### 2.67.5. Website Monitoring

The ICT Department shall monitor:

- Website availability.
- Website performance.
- Security incidents.
- Unauthorized changes.

### 2.67.6. Website Backup

Website files and databases shall be backed up according to the municipal backup schedule.

### 2.67.7. Incident Management

Website incidents shall be:

- Logged.
- Investigated.
- Resolved according to ICT incident management processes.

## 2.68. SERVER ROOM MANAGEMENT PROCEDURE

### 2.68.1. Purpose

To ensure the security, reliability, and proper management of the municipal server room environment.

### 2.68.2. Physical Security

The server room shall:

- Remain locked at all times.

- Be accessible only to authorized personnel.
- Maintain an access register for visitors.

### 2.68.3. Environmental Controls

The server room shall maintain:

- Adequate cooling and ventilation.
- Fire detection and suppression systems where available.
- Protection against water damage.
- Appropriate humidity and temperature levels.

### 2.68.4. Power Management

The municipality shall maintain:

- Uninterruptible Power Supply (UPS) systems.
- Surge protection devices.
- Backup power arrangements where available.

### 2.68.5. Equipment Management

ICT personnel shall:

- Maintain an inventory of server room assets.
- Label equipment appropriately.
- Remove obsolete equipment according to approved disposal procedures.

### 2.68.6. Housekeeping

The server room shall:

- Remain clean and free from clutter.
- Not to be used for storage of non-ICT items.
- Be inspected regularly.

### 2.68.7. Monitoring

The ICT Department shall periodically inspect:

- Physical security controls.
- Environmental conditions.
- Power infrastructure.

## 2.69. INCIDENT REPORTING

All operational incidents involving backups, websites, servers, or the server room shall be reported to the ICT Department and recorded in the municipal incident register.

## 2.70. COMPLIANCE

Failure to comply with this procedure may result in disciplinary action and corrective measures in accordance with municipal policies and applicable legislation.

## 2.71. REVIEW

This procedure shall be reviewed annually by the ICT Department and submitted to the appropriate municipal governance structures for approval.

# 3. DOCUMENT APPROVAL

This document becomes effective upon approval by the Municipal Manager and Council as required.

**PREPARED BY: P.E. NTANZI**

**DATE OF ADOPTION BY COUNCIL: 30 JULY 2026**

**COUNCIL RESOLUTION NO: C22**

**MUNICIPAL MANAGER**

**S.G. KHUZWAYO**

30/07/2026

**DATE**