67 Church Street, Mt Ayliff, 4735
Tel: +27 (0)39 254 6000
Fax: +27 (0) 39 255 0167
Web : www.umzimvubu.gov.za

UMZIMVUBU
LOCAL MUNICIPALITY

813 Main Street , Mount Frere
P/ Bag 9020, M t Frere , 5090
Tel: +27 (0)39 255 8500 /166
Fax: +27 (0) 39 255 0167

ICT CYBERSECURITY STRATEGY

Cybersecurity Strategy

1. Introduction

The Umzimvubu Local Municipality acknowledges the critical importance of cybersecurity in safeguarding its digital assets, infrastructure, and sensitive information. This strategy provides a structured approach to managing cybersecurity risks, ensuring regulatory compliance, and maintaining a secure operational environment for the municipality's digital ecosystem.

This document is aligned with global best practices, including COBIT 5, ISO 27001, and the NIST Cybersecurity Framework, and aims to establish a resilient and proactive cybersecurity posture.

2. Objectives

The primary objectives of this cybersecurity strategy are:

- To establish a robust cybersecurity governance framework.
- To protect municipal data, IT infrastructure, and services from cyber threats.
- To ensure compliance with relevant cybersecurity regulations and frameworks.
- To define clear roles and responsibilities for cybersecurity management.
- To implement proactive risk management and incident response mechanisms.
- To enhance cybersecurity awareness and training among all employees.
- To build resilience against emerging cyber threats through continuous improvement.

3. Cybersecurity Governance and Responsibilities

3.1 Governance Structure

Effective cybersecurity governance is essential to maintaining a secure municipal environment. The governance structure is as follows:

- **Municipal Council:** Provides oversight and strategic direction for cybersecurity policies.

- **Executive Management:** Ensures cybersecurity initiatives align with organizational goals and provides the necessary resources.
- **ICT Section:** Leads cybersecurity implementation, monitors threats, and coordinates response efforts.
- **ICT Manager:** Ensures compliance with regulatory requirements such as POPIA.
- **Departmental Heads:** Ensure adherence to cybersecurity policies within their respective units.
- **All Employees:** Play a critical role in maintaining cybersecurity hygiene and reporting incidents.

3.2 Policies and Procedures

The municipality shall establish and enforce cybersecurity policies and procedures, covering:

- Data Protection and Privacy Policy
- Incident Response and Recovery Policy
- Network Security Policy
- Access Control and Identity Management Policy
- Cybersecurity Awareness and Training Policy

4. Cyber Risk Management Framework

4.1 Risk Assessment Process

To proactively address cyber threats, the municipality will adopt a structured risk assessment approach:

- Conduct bi-annual risk assessments to identify vulnerabilities.
- Prioritize risks based on potential impact and likelihood.
- Implement mitigation measures for identified risks.
- Regularly update risk registers and conduct internal audits.

4.2 Threat Intelligence and Monitoring

The municipality will:

- Leverage external threat intelligence sources to monitor emerging risks.
- Implement a Security Information and Event Management (SIEM) system for real-time threat detection.
- Establish an early-warning system to mitigate potential cyber threats.

4.3 Data Classification and Protection

Municipal data will be classified into:

- **Public Data:** Openly accessible and non-sensitive.
- **Internal Data:** Used within municipal operations but not publicly disclosed.
- **Confidential Data:** Sensitive information requiring strict access control.
- **Restricted Data:** Highly sensitive data with the highest security controls.

Data encryption, access controls, and secure storage mechanisms will be applied accordingly.

5. Cybersecurity Controls and Measures

5.1 Network and Endpoint Security

The municipality will implement:

- Firewalls, Intrusion Detection/Prevention Systems (IDS/IPS), and VPNs for secure communication.
- Endpoint protection software on all municipal devices.
- Regular network vulnerability assessments.

5.2 Identity and Access Management (IAM)

- Enforce multi-factor authentication (MFA) for all critical systems.
- Implement role-based access controls (RBAC) to restrict unnecessary access.
- Periodically review and revoke inactive user accounts.

5.3 Secure Software Development and Patch Management

- Adopt secure coding practices for internally developed applications.
- Regularly update software and apply security patches to mitigate vulnerabilities.

5.4 Cloud Security and Data Backup

- Implement security controls for cloud-based services.
- Conduct regular cloud security assessments.
- Maintain offsite data backups for disaster recovery.

6. Compliance and Regulatory Adherence

The municipality will ensure compliance with:

- **COBIT 5 DSS06.06** for data security and classification.
- **Protection of Personal Information Act (POPIA)** for data privacy.
- **ISO 27001** information security management guidelines.
- **NIST Cybersecurity Framework** for comprehensive security management.

Regular audits and assessments will be conducted to maintain compliance.

7. Cybersecurity Awareness and Training

7.1 Employee Awareness Programs

- Conduct mandatory cybersecurity training sessions.
- Implement phishing awareness campaigns.
- Provide role-based cybersecurity training for key personnel.

7.2 Public Awareness Initiatives

- Engage citizens in cybersecurity awareness efforts.
- Promote safe digital practices through municipal communications.

8. Incident Response and Business Continuity

8.1 Incident Response Framework

- **Identification:** Detect and assess cyber incidents.
- **Containment:** Implement measures to limit damage.
- **Eradication:** Remove the threat and affected systems.
- **Recovery:** Restore operations and data integrity.
- **Lessons Learned:** Conduct post-incident reviews to prevent recurrence.

8.2 Business Continuity and Disaster Recovery (BCDR)

- Establish redundancy for critical municipal services.
- Perform periodic disaster recovery testing.
- Maintain an alternative data center for emergency operations.

9. Continuous Monitoring and Improvement

9.1 Cybersecurity Metrics and Reporting

- Track key performance indicators (KPIs) such as incident response time and security compliance.
- Maintain a cybersecurity dashboard for executive oversight.

9.2 Threat Hunting and Penetration Testing

- Conduct regular penetration testing.
- Deploy honeypots to detect potential attacks.

9.3 Strategy Review and Updates

- Annually review and refine the cybersecurity strategy.
- Adapt to emerging threats and technological advancements.

10. Conclusion

The successful execution of this cybersecurity strategy requires strong leadership, continuous investment, and a commitment to best practices. By proactively addressing cybersecurity risks and fostering a security-conscious culture, the Umzimvubu Local Municipality can safeguard its digital assets and ensure the resilience of its operations against evolving cyber threats.

11. POLICY REVIEW AND APPROVAL

- This policy will be reviewed **annually** or whenever significant changes occur in the network infrastructure.
- The ICT Manager is responsible for ensuring compliance and implementation of this policy.

12. DOCUMENT OWNER AND APPROVAL

The Municipality is the owner of this document. The Executive Management of the Municipality is responsible for ensuring that this policy document is reviewed regularly to ensure that it remains relevant to the organisation. This document was approved by the Executive Management and is issued on a version controlled basis under the signature of the ICT Governance Champion. Every page of this document must also be initialled by the Governance Champion.

APPROVAL OF THE POLICY

The Municipality Council has improved this policy and amendments thereof.

AUTHENTICATION

The amendment of this policy was approved by the municipal council on the 29/04/2025

As per council resolution number ULMC 073

Signed off

MR. GPT NOTA

MUNICIPAL MANAGER

CLLR. NG MDZINWA

SPEAKER OF THE COUNCIL