ELIAS MOTSOALEDI
LOCAL MUNICIPALITY

ICT CYBER SECURITY POLICY AND PROCEDURE

MUNICIPAL COUNCIL RESOLUTION NUMBER

M25/26-51

APROVED AT THE COUNCIL MEETING OF 28 MAY 2026
EFFECTIVE DATE 01/07/2026

MR

Table of Contents

I. Definitions

Accountability: ensuring that the actions of an entity/individual may be traced uniquely to that entity/individual, who may then be held responsible for that action.

Authentication: establishing the validity of a claimed entity/verification of the identity of an individual or application.

Availability: being accessible and usable upon demand by an authorised entity.

Confidentiality: the principle that information is not made available or disclosed to unauthorised individuals, entities or processes.

Identification and authentication: functions to establish and verify the validity of the claimed identity of a user.

Information and communication systems: applications and systems to support the business, utilising information technology as an enabler or tool.

Information technology: any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of vocal, pictorial, textual and numerical data or information.

Integrity: the inherent quality of protection that maintains the accuracy of entities of an information and communication system and ensures that the entities are not altered or destroyed in an unauthorised manner.

Monitoring: performance measurement to ensure the confidentiality, availability and integrity of operational systems and information.

Password: confidential authentication information composed of a string of characters.

Sensitive information: Information in this category may not be distributed without consideration of its sensitive nature.

Private information: is personal information, including personal intellectual property, which is accessible only by its owner and those to whom the owner directly entrusts it, except under exceptional circumstances. Examples: Intellectual property, email.

Confidential information: is the Municipality's information normally handled in the same manner as private information but may be accessed by other authorised employees under limited additional circumstances. Examples: ID number, date of birth, medical records, education record, and financial record.

Internal information: is Municipality information that is intended for distribution within the Municipality.

Public Information: Information in this category is distributed without restriction. Examples: Marketing materials, Municipality website

Top Secret: shall be applied to information, the unauthorised disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security. Example: Compromise of complex cryptologic and communications intelligence systems.

Secret: shall be applied to information, the unauthorised disclosure of which reasonably could be expected to cause serious damage to the national security. Example: Revelation of significant intelligence operations.

1. Purpose and objectives

The purpose of this procedure is to create a secure, reliable, and trustworthy cybersecurity environment that protects critical information and infrastructure whilst strengthening human values and awareness of cybersecurity, in support of the Elias Motsoaledi Local Municipality Strategic Plan.

Cyber threats are viewed as similar to natural disasters or other catastrophic events, where the duration and severity of the event could have a subsequent impact on the municipality's services.

This document must be read in conjunction with the ICT Disaster Recovery Plan, the ICT Security Control Policy and Cybersecurity Incident Response Plan (CIRP) as part of business continuity, focusing on mitigating the impact of forecasted disasters on specific targeted systems and processes. For this document, the recovery of ICT system operations is the primary focus.

The objectives of this plan are to:

1.1 Apply cost-effective protection to security classified and unclassified information which is processed by Elias Motsoaledi Local Municipality information and communication systems.
1.2 Promote awareness and culture of Cybersecurity.
1.3 Promote compliance with appropriate technical and operational cybersecurity standards and best practices.

2. Scope of Application

The focus of the Cyber Security Procedure is the recovery and business continuity from a serious disruption in activities due to the unavailability of Elias Motsoaledi Local Municipality's facilities because of cyber-attacks and related events.

This procedure is applicable to everyone who makes use of the Elias Motsoaledi Local Municipality ICT network.

3. Administration of the procedure

The ICT Manager is responsible for enforcing this procedure, providing guidance and managing cybersecurity within the Municipality.

4. Information System Security

4.1 Cyber Security Assessment

Numerous cyber threats pose risks to Elias Motsoaledi Local Municipality, which may adversely affect service delivery. The Municipality must establish and maintain a structured process to identify, assess, and manage cybersecurity vulnerabilities and potential threats.

a) Asset Management
The Municipality shall:

- Maintain a comprehensive and continuously updated ICT Asset Register covering all hardware, software, data, and information systems.
- Classify information assets based on sensitivity and criticality (e.g., confidential, restricted, public).
- Assign ownership and accountability for all ICT assets.
- Ensure that all assets containing personal information are protected in line with POPIA requirements.
- Implement controls to safeguard assets throughout their lifecycle (acquisition, use, storage, and disposal).

(Refer to ICT Asset Register)

b) Types of Threats
The Municipality shall recognise and manage cybersecurity threats, including, but not limited to:

- Data loss, destruction, or corruption
- Ransomware, malware, phishing, and social engineering attacks
- Unauthorised access, hacking, and system compromise
- Insider threats (negligent or malicious)
- Leakage of confidential or personal information (POPIA breach)
- Integrity risks leading to unreliable or manipulated data.
- Man-in-the-Middle (MITM) attacks.
- SQL injection and application-layer vulnerabilities

Furthermore, the Municipality shall continuously conduct vulnerability assessments and security scans of its network to proactively identify emerging threats. This process must be read in conjunction with the ICT Operational Risk Register.

4.2 Cybersecurity Protection

The Municipality shall implement appropriate technical and organisational measures to prevent, detect, respond to, and recover from cybersecurity incidents

a) Identity Management and Access Control

- Information users will be given the minimum level of access to systems and information that their duties require.
- Human Resources Management and/or respective Strategic Business Unit Managers must report a change of an employee status or role to ICT.
- Remote access to the network or systems will be strictly granted through completion and approval of access request forms and monitored as per the ICT User Account Management Policy. This applies to Municipal employees and Consultants.
- Implement strong authentication mechanisms (e.g., multi-factor authentication where applicable).
- Monitor and log all access to critical systems for audit and accountability purposes.
- Passwords and private keys (physical or digital) must be protected and may not be shared.

b) Awareness and Training

Security education, training, and awareness programmes will be conducted to ensure that employees understand security threats and concerns and are consistently equipped to apply security principles. The training and awareness sessions will be held regularly.

The Municipality shall:

- Implement mandatory cybersecurity awareness programmes for all employees, councillors, and relevant stakeholders
- Provide continuous training on:
    - Phishing and social engineering risks
    - Password and authentication security
    - Data protection and POPIA compliance
    - Safe use of ICT systems and internet resources
- Conduct periodic simulated phishing exercises and awareness campaigns
- Ensure all employees formally acknowledge ICT security policies

c) Information Protection Processes

- Backups will be performed daily and tested as per the Disaster Recovery Plan.
- All computers and servers accessing the Municipal network shall be installed with the Municipal-approved Anti-Virus software.
- In an event where a computer is suspected to be infected with malware, an incident management process will be invoked and perform the following steps to resolve the issue:

Step 1: Disconnect the computer from the network and reset user account passwords
Step 2: Backup critical files, excluding program files
Step 3: Patch both the Anti-Virus and the Operating Systems
Step 4: Run a full scan
Step 5: Restart and reset the password
Step 6: Perform the necessary tests and connect it to the production network

The Municipality shall:

- Establish and maintain a formal Cybersecurity Incident Response Plan
- Ensure all cybersecurity incidents are:
  - Reported immediately
  - Logged and classified
  - Investigated and resolved
- Assign roles and responsibilities for incident response
- Perform post-incident reviews and implement corrective actions

4.3 Threats Detection

The municipality has implemented tools to manage and monitor network security threats, ensuring proactive responses and quick action in the event of unforeseen cybersecurity incidents.

a) Network Security Scanning Tool

- Network security scanning will be conducted monthly
- Auto-generated report with identified threats will be reviewed, and recommendations will be implemented
- Steering meetings will be held to discuss the content of the report and the resolutions thereof

b) Firewall

The Municipality has Firewalls in place with built-in intrusion detection software that controls and restricts both network connectivity and Internet services

c) Anti-Virus Software

The Municipality has Anti-Virus in place to detect, quarantine and/or delete malicious code, to prevent malware from destroying the network

d) Email Scanning Tool

The Municipality has the Email Scanning tool in place that scans both the incoming and outgoing emails for threat identification

4.4 Cyber Security Incidents Response and Recovery

The Municipality has implemented the Disaster Recovery plan and Disaster Recovery Site to ensure the restoration of critical computer systems and networks as quickly as possible in the event of a cyber-attack.

In the event of a cyber-attack, the following processes will unfold:

- The ICT team will communicate the attack to the Communication Unit to inform relevant stakeholders of the attack.
- The ICT Response Team, together with relevant service providers, will investigate what has transpired.
- Depending on the nature of the attack, the teams will resolve the issue or escalate to the Senior Manager Corporate Services for further investigations.
- If the result of the investigation shows that it's a cybercrime, then a criminal case will be registered with the relevant authorities.
- Disaster Recovery Plan will then be invoked for the recovery process.

- Based on the investigation's reports, the ICT team will implement security measures and controls to harden security and ensure there is continuous improvement.

5. Roles and Responsibilities

The Risk Committee shall:

- Ensure that the necessary information security controls are implemented and complied with as per this procedure.

The ICT Division shall:

- Approve and authorise information security procedures
- Ensure that all users are aware of the applicable policies, standards, procedures and guidelines for information security
- Ensure that policy, standards and procedural changes are communicated to applicable users and management
- Evaluate information security potential risks and introduce countermeasures to address these risks
- Revise the information security policy and standards for effective information security practices
- Facilitate and coordinate the necessary information security procedures within the Municipality
- Report and evaluate changes to information security policies and standards
- Coordinate the implementation of new or additional information security controls
- Review the effectiveness of information security measures and implement remedial controls where deficits are identified
- Coordinate awareness strategies and rollouts to communicate information security mitigation solutions effectively
- Coordinate awareness strategies and rollouts to communicate information security mitigation solutions effectively

6. Review period

The procedure shall be reviewed as needed.

7. Signatories

Ms. NR Mahlakwane Pr Tech Eng
Municipal Manager

19/06/2026
Date

The Mayor
Cllr. Tladi MD

19/06/2026
Date

Annexure 1

CYBERSECURITY INCIDENT RESPONSE PLAN

1. Purpose

This Cybersecurity Incident Response Plan (CIRP) establishes a formal framework for identifying, managing, and responding to cybersecurity incidents within the Elias Motsoaledi Local Municipality.
The plan ensures:

- Protection of government data and services
- Rapid detection and response to cyber threats

2. Scope

This policy applies to:

- All users within the EMLM domain
- On-premises servers and infrastructure
- Microsoft 365 cloud services
- End-user devices managed via Intune
- Backup systems managed through Veeam

3. Objectives

The objective of this Cybersecurity Incident Response Plan is to ensure a consistent and effective approach to managing cybersecurity incidents across the municipality. It seeks to minimise disruption to critical public services by enabling timely detection, containment, and recovery from security incidents. Furthermore, the plan aims to safeguard sensitive citizen and organisational data from unauthorised access, loss, or compromise. In doing so, it promotes accountability through clearly defined roles and responsibilities, while also ensuring that all incidents are properly documented and managed in a manner that supports audit readiness and compliance with applicable regulatory requirements.

4. Incident Classification

Severity	Description	Example
Low	Minimal impact	Spam email
Medium	Limited disruption	Malware detected.
High	Major system impact	Server compromise
Critical	Data breach/ransomware	Citizen data exposure

5. Incident Response Process

5.1 Preparation

The municipality has implemented essential systems and practices in place to prevent and respond to cyber incidents effectively. This includes using tools such as Microsoft Defender for protecting devices and emails, Microsoft Intune to manage and secure devices, Azure AD Conditional Access to control user access, and Veeam for reliable data backup and recovery. Key activities during this stage involve keeping an updated record of all ICT assets, educating employees through regular

MR

cybersecurity awareness training, clearly defining how incidents should be escalated, and ensuring that secure backups are stored offline and protected from tampering.

5.2 Identification
Potential cybersecurity incidents are detected through various sources such as Microsoft Defender alerts, firewall and intrusion detection system logs, and reports from users. The ICT team then verifies whether the alerts are genuine, analyses system logs to understand the issue, and classifies the severity of the incident to determine the appropriate response.

5.3 Containment
This may include isolating affected devices using Intune, disabling compromised user accounts in Azure Active Directory, and blocking any malicious IP addresses or domains. For example, in the event of a ransomware attack, the affected server must be disconnected from the network immediately to prevent further damage.

5.4 Purge
The process involves eliminating malware using Microsoft Defender, fixing system vulnerabilities through updates and patches, resetting user credentials and enforcing multi-factor authentication, and reviewing system logs to ensure that no hidden threats remain.

5.5 Recovery
Once the threat has been removed, the recovery phase focuses on restoring normal operations. Systems are recovered using Veeam backups, tested to ensure they are functioning correctly, and safely reconnected to the network. Continuous monitoring is then conducted to ensure that the incident does not recur. It is also essential that backups are tested at least quarterly to ensure reliability.

5.6 Lessons Learned
Within five working days of the incident, a review is conducted to analyse what happened and how it was handled. Based on this, policies and controls are updated, and a detailed report is submitted to the ICT steering committee to ensure accountability and strengthen future response efforts.

6. Communication and Escalation
All cybersecurity incidents must be reported promptly to the ICT Helpdesk to ensure they are logged and addressed without delay. For incidents classified as high or critical, escalation to the ICT Manager must occur within one hour to enable swift decision-making and response. Where necessary, external communication will be initiated, including notifying relevant regulatory bodies in the event of a data breach, informing affected stakeholders, and engaging law enforcement authorities if the incident involves criminal activity.

7. Incident Response Tools
The municipality utilises a range of integrated tools to support effective incident detection, response, and recovery. These include Microsoft Defender for Endpoint and Microsoft 365 Defender for threat detection and protection, Microsoft Intune for device management and security enforcement, Azure Active Directory (Entra ID) for

MR

identity and access management, and Veeam Backup and Replication for secure data backup and system recovery.

8. Documentation and Reporting

All cybersecurity incidents must be thoroughly documented to ensure accountability, traceability, and audit readiness. Each incident record should include a unique incident ID, the date and time the incident was detected, details of the systems affected, the identified root cause, actions taken to contain and resolve the incident, and the final resolution. This documentation supports compliance requirements and provides valuable insights for improving future responses.

10. Testing and Continuous Improvement

To ensure the effectiveness of the incident response capability, the municipality will implement ongoing testing and improvement measures. This includes conducting annual penetration testing to identify vulnerabilities, performing quarterly incident response simulations to assess readiness, and regularly reviewing the implementation of CIS Controls to ensure alignment with best practices and evolving cybersecurity threats.

Signatories

Ms. NR Mahlakwane Pr Tech Eng
Municipal Manager

19/06/2026
Date

The Mayor
Cllr. Tladi MD

19/06/2026
Date