MOPANI DISTRICT MUNICIPALITY

UNITY IN DIVERSITY

INFORMATION TECHNOLOGY

Incident Management Policy

TABLE OF CONTENTS

I. Acronyms and Abbreviations

MDM	Mopani District Municipality
MM	Municipal Manager
SMT	Senior Management Team
ICT	Information and Communication Technology
IT	Information Technology
IMT	Incident Management Team
ITO	Information Technology Office, manned by IT or ICT officer(s)

II. Clarification of Terms

Availability

Being accessible and useable upon demand by an authorized entity or user(s).

Confidentiality

The principle that information is not made available or disclosed to unauthorized individuals, entities or processes.

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 unauthorized manner.

Non-repudiation

The assurance that someone cannot deny something.

Service-desk

Central point of contact for handling IT user queries and other related issues.

1. PREAMBLE

In the course of **MDM** IT unit providing service, incidents may occur, some of which may have serious consequences for **MDM**, its service users, staff, and the public. The number of computer incidents and the resulting cost of business disruption and service restoration continue to escalate. Implementing IT policies, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of incidents are some the actions that can be taken to reduce the risk and drive down the cost of incidents.

An incident is defined as any unauthorized action taken on municipality information systems that reduces, compromises, or threatens the confidentiality, integrity, availability, or non-repudiation of the data or systems themselves. It is any event which is not part of the standard operation of a services which causes, or may cause an interruption to, or reduction in the quality of that service. This includes, but is not limited to, the following;

1.1 Removing or bypassing existing protection and control mechanisms:

1.2 Using or misusing control mechanisms to gain or grant unauthorized access or system privileges; or to escalate current privileges:

1.3 Reading, copying, modifying, or deleting data by an individual or program not authorized for such action

1.4 Abusing privileged access in order to monitor or impersonate another user, or reading that individual's private data without authorization;

1.5 Accidental or deliberate unauthorized change of data;

1.6 Attempting to explore or test for security vulnerabilities in information assets when not authorized to do so.

2. PURPOSE AND OBJECTIVES

2.1 The purpose of this policy is to ensure that unexpected disruptive events are managed and responded to with the objective of controlling the impact to **MDM** business within acceptable levels.

2.2 The aim of this policy is therefore not to allocate individual blame but to ensure that there is organizational learning from incidents to reduce future risk and to provide support for any service users and staff involved.

3. SCOPE OF APPLICATION

This policy, except otherwise indicated, is applicable to all **MDM** employees and contracted IT service providers when dealing with IT incidents in **MDM**.

4. LEGAL FRAMEWORK

The following publications govern the execution of the Incident Management Policy and were taken into consideration during the drafting of the Internet Acceptable Use Policy;

4.1 The Promotion of Access to Information Act, 2000 (Act no. 2 of 2000)

4.2 The Protection of Information Act, 1982 (Act no. 84 of 1982)

4.3 The State Information Technology Act, 1998 (Act no. 88 of 1998)

4.4 SABS/ISO 17799

4.5 Minimum Information Security Standards (MISS)

4.6 Guidelines for the Handling of Classified Information (SP/2/8/1)

4.7 Electronic Communications and Transaction Act, 2002 (Act no. 25 of 2002)

4.8 ITIL Information Technology Infrastructure Library

5. ADMINISTRATION OF THE POLICY

ITO is responsible for enforcing this policy and continuously ensuring monitoring and compliance.

6. POLICY ROLES AND RESPONSIBILITIES

To conduct operations as effectively and efficiently as possible, **MDM** IT seeks to improve its service at all levels and understands that valuable lessons can be learnt from incidents.

6.1 MM

6.1.1. MM has delegated the responsibility for the management of this policy to Senior Manager for Corporate Services or as he/she deems appropriate.

6.1.2. MM shall officially appoint members of the Incident Management Team

6.2 **MDM** Senior Management Team

6.2.1. SMT shall ensure that **MDM** staff is made aware of this policy and its requirements and that suitable and sufficient training is provided to ensure its implementation.

6.3 Incident Management Team

The IMT shall:

6.3.1. Ensure that all incidents are properly logged, analyzed and mitigated;

6.3.2. Ensure that appropriate reporting is in place to enable the effective management and control of incidents, and to identify potential problems at an early stage.

6.4 Service Desk

6.4-1, The Service Desk is responsible for maintaining an incident register which will include details such as logging date, review, escalation etc. where all incidents are recorded;

6.4.2. Ensure incidents a properly tacked, monitored and escalated as per agreed timelines;

6.4.3. Is responsible for the monitoring of the resolution process of all registered Incidents;

6.4.4. The Service Desk is the owner of all Incidents.

6.5 All Employees, Contractors and Visitors

6.5.1. It is the responsibility of all employees of the municipality (whether full time, agency, or as contractor) and anyone attending, working on or visiting any **MDM** premises, to abide by this policy and to report any incidents or near misses in which they were either directly involved or have witnessed.

7. POLICY CONTENTS

7.1 Reporting Events and Weaknesses

7.1.1 **MDM** seeks to encourage service users and other stakeholders to report incidents, to enable MDM to obtain a more complete picture of the risks that face the municipality and to improve services.

7.1.2 All incidents, security related environmental changes or software malfunctions with the potential to disrupt network traffic or operational systems, or threaten confidentiality, integrity or availability of any component of a **MDM** information system shall be reported to the line manager and/or the IT Office who should escalate all high impact incidents to the Incident Management Team and ITO as soon as possible so that prompt remedial action can be taken.

7.1.3 All **MDM** employees, IT staff, external parties, contractors and temporary staff shall be made aware of the incident reporting procedure and that they are required to report any incidents and malfunctions as soon as possible.

7.1.4 Users are not under any circumstances permitted to attempt to prove a suspected weakness since this may be interpreted as a potential misuse of the system.

7.1.5 Any party found guilty of violating this policy, and all other IT policies, will be subjected to a disciplinary process in line with the applicable human resources policies and/or code of conduct.

7.1.6 All system owners must report all significant environmental changes to the

ITO promptly. Such changes include changes of physical access means, changes of security responsibilities and changes of established security measures.

7.2 Management of Incidents And Improvement

7.2.1 The first priority in responding to any incident in **MDM** is to stop the incident itself and prevent its recurrence. Where the severity of the incident and its likelihood of recurrence justify it, management can and must take any steps necessary on a temporary basis, such as removing systems from operation, revoking system accesses or removing involved personnel from municipality facilities.

7.2.2 To address incidents, a formal incident response procedure shall be established setting out the action to be taken in the event on an incident. The procedures must consider:

7.2.2.1. The evaluation of reported incidents and weaknesses;

7.2.2.2. Collection and preservation of evidence related to the incident;

7.2.2.3. Determining actions to address the incidents and weaknesses; and

7.2.2.4. Monitoring progress on the actions.

7.2.3 Response procedures to address incidents must be documented indicating what actions and escalation needs to be taken in the event of incidents within categories such as:

7.2.3.1. Access control;

7.2.3.2. Network Security:

7.2.3.3. Critical IT Asset Rooms;

7.2.3.4. Equipment Security;

7.2.3.5. Communications Security:

7.2.3.6. Computer Virus;

7.2.3.7. Systems availability; and

7.2.3.8. Software Security.

7.2.4 The ITO must ensure that all open incidents and actions against open incidents and weaknesses are reviewed and monitored weekly.

7.2.5 Incidents and malfunctions shall be resolved and closed by IT staff and/or management in a timely manner consistent with documented response procedures.

7.2.6 IT HelpDesk shall provide feedback to individuals who reported the incident and notify them of results.

7.2.7 Mechanisms enabling types, volumes and costs of incidents to be quantified and monitored shall be in place to assist in identifying recurring or high impact incidents or malfunctions, as well as mitigating actions to prevent the recurrence or future impact of similar incidents.

7.2.8 It is the MM's responsibility to decide whether or not to inform law enforcement in the event of an incident where any breach of statute may have occurred.

7.2.9 Where a follow-up action against a person or organization after an incident involves legal action (either civil or criminal), evidence should be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

7.2.10 *For paper documents:* The original document should be kept securely with a record of the individual who found the document, where the document was found, when the document was found and who witnessed the discovery: any investigation should ensure that originals are not tampered with;

7.2.11 For information on computer media: Mirror images or copies (depending on applicable requirements) of any removable media, information on hard disks or in memory should be taken to ensure availability; the log of all actions during the copying process should be kept and the process should be witnessed: the original media and the log (if this is not possible, at least one mirror image or copy) should be kept securely and untouched.

8. VIOLATIONS

Non-compliance of this policy shall constitute violation of the policy and shall be treated in terms of the Municipality Disciplinary Code and Procedure Policy.

9. ADOPTION OF THE POLICY

This policy shall be considered by the relevant structures of the municipality and shall be adopted by Council.

10. Inception Date

This policy comes into effect from the date of adoption by Council of MDM or a date to be determined by the duly authorized and/or or authorized authority.

11. Policy Review

This policy shall be reviewed annually, or as and when a need arised, and changes will become effective upon adoption by Council.

12. Enquiries

Enquiries about the policy should be directed to the IT Office.