



## ICT INCIDENT AND PROBLEM MANAGEMENT POLICY

|   |               |
|---|---------------|
| <b>REFERENCE NUMBER</b>                     | 6/1/2/7/P/018 |
| <b>DIVISION RESPONSIBLE FOR FORMULATION</b> | IT Section    |
| <b>EFFECTIVE DATE</b>                       | 01 July 2024  |
| <b>POLICY PUBLISHED DATE</b>                | 01 July 2024  |
| <b>DATE OF NEXT REVIEW</b>                  | June 2025     |

**Approval**

|                             |   |  |                        |
|-----------------------------|---|--|------------------------|
| <b>DOCUMENT:</b>            | <b>Incident and Problem Management Policy</b> |  |                        |
| <b>Copy Number:</b>         | <b>Original Copy</b>                          |  |                        |
| <b>Compiled by:</b>         | Lamla Luke                                    | <b>Reviewed by:</b>                      | Management and Council |
| <b>Compilation Date:</b>    | April 2021                                    | <b>Review Date:</b><br><b>Management</b> |                        |
| <b>Version:</b>             | V 1.0   | <b>Review date:</b><br><b>Council</b>    |                        |
| <b>Distribution:</b>        | All   | <b>Classification:</b>                   | <b>Policy</b>          |
| <b>Document Release</b>     |   | <b>Document Approval</b>                 |                        |
| <b>Releasing Authority:</b> | Director: Corporate Services                  | <b>Approval Authority:</b>               | CHDM Council           |
| <b>Date Released:</b>       |   | <b>Date Approved:</b>                    | <b>24 May 2024</b>     |

## Contents

|  |           |
|--|-----------|
| Definitions .....                                      | 4         |
| 1. Problem Statement .....                             | 5         |
| 2. Purpose.....  | 5         |
| 3. Legislative Framework.....                          | 6         |
| 4. Scope .....   | 6         |
| 5. Policy .....  | 6         |
| 6. Incident Management Procedure .....                 | 7         |
| <b>Audience and Applicability .....</b>                | <b>9</b>  |
| <b>Responsibilities of the Municipal Manager .....</b> | <b>10</b> |
| <b>Responsibilities of the IT Manager .....</b>        | <b>10</b> |
| <b>Escalation Procedure .....</b>                      | <b>10</b> |
| <b>Policy Compliance .....</b>                         | <b>11</b> |
| Compliance Measurement .....                           | 11        |
| Exceptions .....                                       | 11        |
| Enforcement .....                                      | 11        |
| <b>Reporting &amp; Disclosure Requirements .....</b>   | <b>11</b> |
| 7. INCIDENT MANAGEMENT PROCESS CHARTS .....            | 11        |
| <b>Approval.....</b>                                   | <b>13</b> |

## Definitions

|                     |  |
|---------------------|--|
| <b>Incident</b>     | An 'Incident' is any event which is not part of the standard operation of the service and which causes, or may cause, an interruption or a reduction of the quality of an IT service.  |
| <b>ITIL</b>         | <p><b>ITIL</b>, formerly known as the <b>Information Technology Infrastructure Library</b>, is a set of practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business.</p> <p>ITIL describes processes, procedures, tasks, and checklists which are not organisation-specific but can be applied by an organization for establishing integration with the organization's strategy, delivering value, and maintaining a minimum level of competency. It allows the organization to establish a baseline from which it can plan, implement, and measure. It is used to demonstrate compliance and to measure improvement.</p> |
| <b>Helpdesk</b>     | A help desk is a resource intended to provide the customer or end user with information and support related to an institution's products and services. The purpose of a help desk is usually to troubleshoot problems or provide guidance about products such as computers, electronic equipment or software.  |
| <b>Service Desk</b> | A Service Desk is a primary IT service within the discipline of IT service management (ITSM) as defined by the Information Technology Infrastructure Library (ITIL). It is intended to provide a Single Point of Contact ("SPOC") to meet the communication needs of Users and IT employees.   |

## 1. Problem Statement

This policy describes the procedure to control the ICT process of managing calls and incidents logged with the ICT and Systems units. The process covers incident identification, analysis, resolution and review as conducted by the Helpdesk Operator. This document refers to other connecting processes and documents rather than the information being repeated and duplicated.

## 2. Purpose

The purpose of this policy is to establish a uniform process for incident management and define the steps involved in responding to employee IT-related incidents at Chris Hani District Municipality. The objective of incident management is to restore normal service operations as quickly as possible. To do so ensures minimal adverse impacts on CHDM operations. It also ensures that the best possible levels of service quality and availability are maintained. Incident management is planned and performed following established policies, procedures, and standards.

Roles and responsibilities for managing the incident management process and procedures are defined, assigned, and communicated. Incident management relies on the effective and efficient operations of other processes. There is a close interface between incident management, problem management and change management processes, as well as the function of the Help Desk or Service Desk.

This incident management policy and procedure is aligned with the principles of ITIL incident management. Therefore, the CHDM council adopts ITIL as an approved IT service management framework. In ITIL activities of the incident management process are:

Incident detection and recording

Classification and initial support

Investigation and diagnosis

Resolution and recovery

Incident closure

Incident ownership, monitoring, tracking and communication

### **3. Legislative Framework**

- ISO 20000 - IT Service Management standard
- ITIL Framework
- CHDM ICT Governance Framework
- Batho Pele Principles

### **4. Scope**

This policy applies to all employees and councillors of CHDM. The policy defines call logging procedures for all ICT-related incidents including ICT Infrastructure and Application Systems.

### **5. Policy**

1. One incident management process will be utilized throughout the organization.
2. The incident management process owner is accountable for the entire incident management process and has the authority to develop policies and procedures for the process.
3. Incident management will provide a single definition of an incident that will be common and utilised throughout IT and other processes.
4. Incident management has the responsibility for supporting only the software and hardware that have been deemed required and approved by both IT and the organisation through Service Level Management.
5. All incidents, regardless of where they are detected, will be logged and updated in a single incident management tool.
6. The Service Desk will be the first point of contact for users.
7. All incidents will be prioritized based on impact and urgency defined in the priority model that has been created for incident and change management.

8. In the event the Service Desk or any other support level exceeds its ability to resolve a particular Incident, the incident will be escalated to the appropriate individual/group.
9. All work and progress toward incident resolution, regardless of the support level or staff member, will be documented in the incident tracking tool on the helpdesk system on an ongoing and timely basis.
10. The status of incidents will be provided or made available to customers throughout the lifecycle of the incident through resolution and recovery.
11. The Service Desk will own the lifecycle of all incidents. All activities associated with the incident are the responsibility of the individuals and groups involved in resolving the incident.
12. Communication will be provided to departments concerning any known or expected degradation of service and impact on service delivery.
13. Incident closure is the result of the user validating that the resolution to the incident has been met and the service has been restored to the user's satisfaction.
14. Incident management metrics and management reports will be provided to management and the ICT Steering Committee.
15. Reviews are conducted by the ICT Manager and Systems Manager monthly.

## **6. Incident Management Procedure**

### **6.1. Logging of the Calls**

- 6.1.1. Calls must be logged by the user via email to [helpdesk@chrishanidm.gov.za](mailto:helpdesk@chrishanidm.gov.za) or with the Helpdesk Operator via email to [tmfakadolo@chrishanidm.gov.za](mailto:tmfakadolo@chrishanidm.gov.za) or telephonically by calling 0458084737. Calls are only logged to the Helpdesk Operator email.
- 6.1.2. All calls to the Helpdesk Operator must be recorded on the call logging Sheet, Appendix A, which will be maintained by the Helpdesk Operator and must be entered into the Helpdesk system/Spreadsheet when it is available.

6.1.3. Details such as Call Reference Number, User's Name, date and time logged, nature of issue and priority status must be recorded by the Helpdesk Operator on the call logging sheet.

6.1.4. The user must be issued with a reference number.

6.1.5. Calls must be classified on the system or call logging sheet as per the categories below:

6.1.5.1. Network;

6.1.5.2. Software;

6.1.5.3. Email;

6.1.5.4. Hardware;

6.1.5.5. User account;

6.1.5.6. Other.

## **6.2. Priority of Calls**

6.2.1. Calls logged/ incidents are classed as High, Medium and Low based on the nature of the call logged.

6.2.2. Calls logged/ incidents will be resolved according to the timeframes below:

| <b>Criticality of Calls logged/ Incidents</b> | <b>Timeframe of Resolution</b> |
|---|--------------------------------|
| High  | Within 1 hour                  |
| Medium  | Within 8 hours                 |
| Low   | Within 24 hours                |

6.2.3. All calls with a high risk must be classified as high and must be attended to as such.

6.2.4. Calls logged must be attended to and resolved timeously.

## **6.3. The person assigned to an incident**



- 6.3.1. All calls will be assigned to the relevant IT staff according to classification by the Helpdesk Operator at his discretion depending on the nature and level of the call. The following are guidelines for assigning calls.
- 6.3.1.1. Network-related incidents/calls – network administrator
  - 6.3.1.2. Software
    - 6.3.1.2.1. Financial Systems – Systems Administrator
    - 6.3.1.2.2. Microsoft – Network Administrator or PC Support Technician
  - 6.3.1.3. Email – Network Administrator or PC Support Technician
  - 6.3.1.4. Hardware – PC Support Technician
  - 6.3.1.5. User account – Network Administrator or Systems Administrator
- 6.3.2. Calls may be escalated to a higher level or delegated to a lower level.
- 6.3.3. Calls that may not be resolved internally will be escalated to second-line support following the relevant Service Level Agreements.
- 6.3.4. Upon resolution of the call, the Helpdesk Operator must update the system or complete the call logging sheet recording the date and time-resolved and must record the resolution of the incident for future reference.
- 6.3.5. The Helpdesk Operator and users must also sign the form as an acknowledgement that the call has been resolved.

#### **6.4. Monthly review**

A monthly review of calls and incidents logged must be performed by the ICT Manager and Systems Manager, indicating compliance, long outstanding calls and trends.

#### **Audience and Applicability**

The Incident Management Policy applies to everyone in the Municipality who has access to the ICT services and network infrastructure of the Municipality.

## **Responsibilities of the Municipal Manager**

The Municipal Manager at the advice of the IT Manager can decide on the following:

1. Review of the incident management policy,
2. Change the incident management policy if it is not compliant with information security legislation,
3. Propose amendments and /or deletions on the policy.

## **Responsibilities of the IT Manager**

1. The IT Manager is responsible for assessing and evaluating the risk of the accessing of the abuse or misuse of computer systems.
2. Appropriate rights or revocation thereof of those rights to the Municipal employees violating the incident management policy,
3. Ensure that the incident management policy is effective and user-friendly.

## **Escalation Procedure**

1. CHDM employees shall escalate any deviations or violations of the incident management policy to the Help Desk operator.
2. The Help Desk Operator after evaluating the merits of the violation and the extent of the violation shall report the violation or breach to the ICT Manager.
3. The ICT Manager shall immediately issue a directive to the Help Desk Operator to suspend the use of certain devices to institute a formal and proper investigation.
4. On the outcome of the investigation, the IT Manager shall inform the Municipal Manager of such for a ruling or further investigation upon which a decision shall be taken on the necessary course of action.
5. The IT Manager may allow deviation only based on an operation that requires such an intervention.
6. The Municipal Manager may approve or decline such request for a deviation.

## Policy Compliance

### Compliance Measurement

The IT Section team will verify compliance with this policy through various methods, including but not limited to, periodic walk-throughs, remote desktop tools, business tool reports, internal and external audits, and feedback to the policy owner.

### Exceptions

Any exceptions to this policy must be approved in writing by the Municipal Manager.

### Enforcement

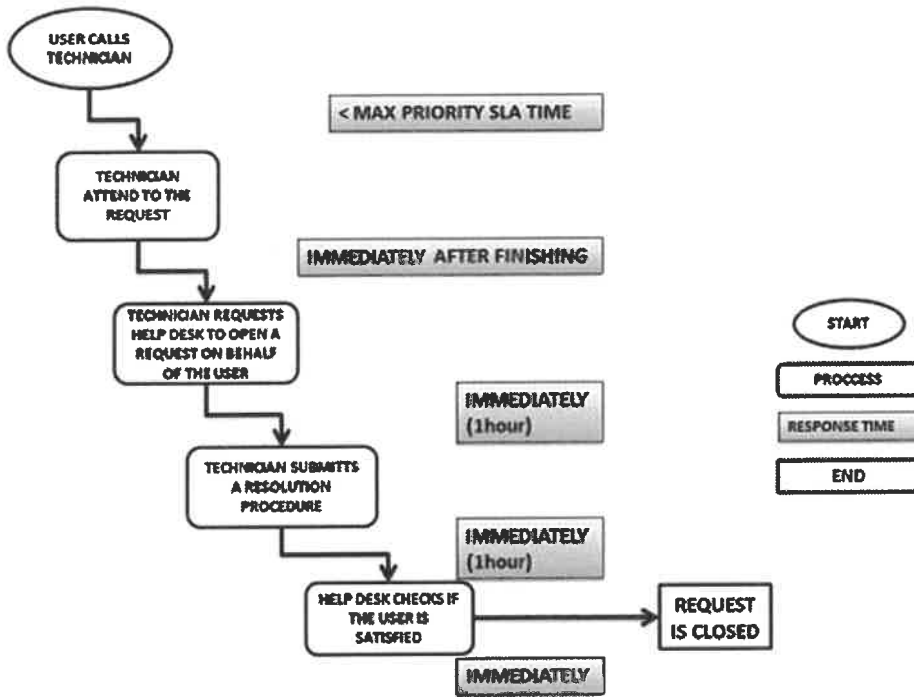
An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. IT Section reserves the right to restrict any device or connection that does not comply with this policy.

### Reporting & Disclosure Requirements

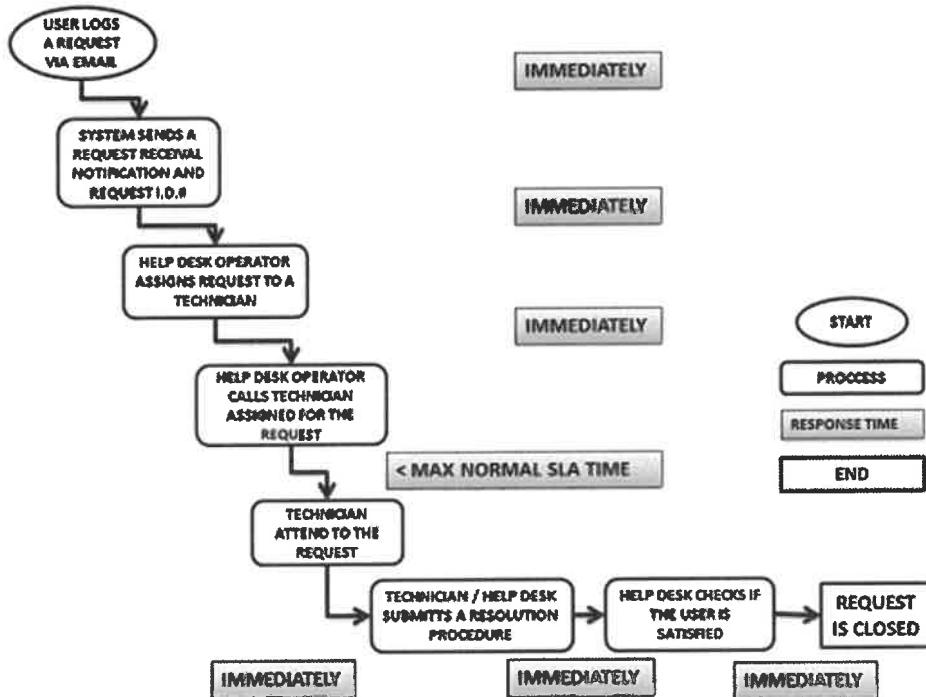
The IT Manager shall report from time to time the management, administration and operationalisation of the policy implementation to the Municipal Council.

## 7. INCIDENT MANAGEMENT PROCESS CHARTS

### HIGH PRIORITY



**NORMAL PRIORITY**



## Approval

### EFFECTIVE DATE

This Policy takes effect on the 01<sup>ST</sup> of July 2024

Policy Adopted at the Chris Hani District Municipality Council meeting, dated 24 May 2024.

**Council Resolution number: C143  
2023-2024**

Signed by Municipal Manager:

G. Mashig  
Initial & Surname

[Signature]  
Signature

\_\_\_\_\_  
Date

Signed by Speaker of Council:

J. CENGANI  
Initial & Surname

[Signature]  
Signature

\_\_\_\_\_  
Date

### Annexure A – Incident request form

| Customer Details       |           | Respondant Details |         |     |
|------------------------|-----------|--------------------|---------|-----|
| Date:                  | Call Ref: | Name:              |         |     |
| Site Name:             | Code :    | ARRIVAL DATE: / /  | TIME: H | MIN |
| CONTACT:               | TELL :    | COMPLETED : / /    | TIME: H | MIN |
| MACHINE<br>TYPE MODEL: | LOCATION: | Signature :        |         |     |

### ACTIVITY

*Adopted in an Ordinary Council meeting held on 24 May 2024*

|      |  |              |  |        |  |                 |  |        |  |
|------|--|--------------|--|--------|--|-----------------|--|--------|--|
| Call |  | Installation |  | Revamp |  | De-installation |  | Survey |  |
|------|--|--------------|--|--------|--|-----------------|--|--------|--|

**CALL DETAILS**

| SCOPE OF WORK FAULT | RESOLUTION(POINT FORMAT) |
|---------------------|--------------------------|
|                     |                          |
|                     |                          |
|                     |                          |
|                     |                          |
|                     |                          |
|                     |                          |
|                     |                          |
|                     |                          |

**CURRENT EQUIPMENT /REPLACED EQUIPMENT DETAILS/ PART USED**

| OLD PARTS | SERIEL NO |  | NEW PART | SERIEL NO |
|-----------|-----------|--|----------|-----------|
|           |           |  |          |           |
|           |           |  |          |           |
|           |           |  |          |           |
|           |           |  |          |           |
|           |           |  |          |           |
|           |           |  |          |           |
|           |           |  |          |           |
|           |           |  |          |           |

**Correspondent Authorization**

|                     |              |
|---------------------|--------------|
| NAME:               | DESIGNATION: |
| EMPLOYEE SIGNATURE: | DATE:        |
| <b>Comment:</b>     |              |
|                     |              |

|  |
|--|
|  |
|  |

Supervisor: Sign.....Date:.....