BELA-BELA LOCAL MUNICIPALITY

OFFICE OF THE MUNICIPAL MANAGER

Information and Communication Technology

Helpdesk Support Procedure

TABLE OF CONTENTS

POLICY AUTHORITIES

Compiled by	D Nkuna
Designation	Divisional Manager IT
Signature	
Date	
Supported/Not Supported	
Designation	
Signature	
Date	
Approved/Not Approved	
Designation	
Signature	
Date	
Effective Date	From date of approval

1. MANDATE OF THE ICT DIVISION

1.1 The Information and Communications Technology (ICT) Division has the mandate to deliver services, support and maintain ICT infrastructure, for the Municipality to realise its mandate.

2. OBJECTIVE OF THE DOCUMENT

2.1 This procedure establishes a governance structure which applies to all ICT systems and infrastructure support activities together with the acquisition of any IT hardware, software or externally sourced ICT Services.

3. APPLICABILITY OF THE DOCUMENT

3.1 This document applies to officials from the Division: Information and Communication Technology (ICT)

4. TERMS AND DEFINITIONS

Term	Definition
Information systems	Information systems means an interconnected set of information resources under the same management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications and people.
Electronic media	Electronic media means electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk or digital memory card; or transmission media internet, extranet (includes using internet technology to link a business with information accessible only to collaborating parties), private networks, etc.
Backup	Backup means creating a retrievable, exact copy of data.
Restoration	Restoration means the retrieval of files previously backed up and returning them to the condition they were at the time of backup.

5.   REFERENCES

5.1 International Guidelines

   a.   Control Objectives for Information Technology (COBIT)

5.2 International Standards

   b.   Information Technology Infrastructure Library (ITIL)

   c.   ISO/IEC 17799: Edition 1, 2000 – Information Technology – Code of practice for Information Security Management

5.3 National Policy

   a.   Constitution of the Republic of South Africa, Act 108 of 1996

   b.   The Electronic Communications and Transactions (ECT) Act 25 of 2002

   c.   National Strategic Intelligence Act 2 of 2000 applicable for South Africa

   d.   Regulation of Interception of Communications Act 70 or 2002

   e.   State Information Technology Act 88 of 1998

6.   ROLES AND RESPONSIBILITIES

6.1   The ICT Division shall ensure that the user of ICT services have access to the appropriate services to support the business functions.

6.2   The ICT Divison shall ensure that the procedure is followed as agreed.

6.3   ICT Division shall ensure that the necessary controls are in place to implement this procedure.

6.4   ICT Division aims to resolve all request for assistance on supported applications within the agreed SLA.

7.   SERVICE SUPPORT PROCESS

7.1 **Request Capture**: All requests from officials will be captured and verified in the helpdesk system

7.2 **Request Ticket**: A request ticket will be opened in tracks with the customer name,phone number and incident description

7.3 **Problem Resolution**: IT Technicians will attempt to resolve all problems and requests for supported systems and applications.If the problem remains unresolved it will be escalated to the next level of support

7.4 **Incidents Closure**: All incidents will be closed when resolution has been offered

7.5 **Customer Satisfaction** : Surveys will be established to ensure customer satisfation

7.6 Helpdesk Contact details

Contact Details	
Hours of Operation	07h30 – 16h00 Monday to Friday
Contact Number	
Email Address	helpdesk@belabela.gov.za
Incident Escalation 1	Dineo Motlhaka
Incident Escalation 2	Daniel Nkuna

8.   Helpdesk Requests

8.1   Incidents

    i.   Create, update and delete users in the business application systems

    ii.   Create, update and delete users in the domain

    iii.   Create, update and delete user folder shares

    iv.   Create, update and delete users in the Telephone Management System

v. Configure and install telephone handsets

vi. Addition and removal of machines from the domain

vii. Install, configure and update recommended or approved software

viii. Install and setup computer equipment and peripheral items

ix. Application software maintenance and support all requests for change

8.2 Service desk Support Services

Service Desk Services	
Operating Systems	Windows 7
Office Productivity	Microsoft Office 2010
Web Browser	Microsoft Internet Explorer
Antivirus Software	Symantec Antivirus
File Distribution Format	Adobe Reader
Application Systems	All business application software
Others	Any other applications that might be in line with business operations of the municipality

8.3 General Support

a. ICT support shall be available to all staff on the following:

i. General computing advice

ii. Network support services

iii. File backup and restore services

8.4 Levels of Support

a. ITIL uses three metrics for determining the order in which incidents are processed.

i. Impact - The effect on business that an incident has

ii. Urgency - The extent to which the incident's resolution can bear delay

iii. Priority - How quickly the service desk should address the incident

b. Priority values are defines as follows:

     i.   Priority 1 = low = 16hrs
    ii.   Priority 2 = normal = 8hrs
   iii.   Priority 3 = medium = 4hrs
   iv.   Priority 4 = high = 2hrs

c. ITIL suggests that priority be made dependent on Impact and Urgency. Out-of-box, this is true on incident forms. Priority is generated from Urgency and Impact according to the following table:

	URGENCY 1	URGENCY 2
IMPACT 1	PRIORITY 1	PRIORITY 2
IMPACT 2	PRIORITY 2	PRIORITY 3
IMPACT 3	PRIORITY 3	PRIORITY 4

d. It should be noted that the Expected Resolution Time is merely an estimate, since resolution of the incident may require involvement of external parties who are not bound by time estimates indicated in the table.

8.5 Methods of Communication

a. An incident may be reported to ICT through the following means of communication:

     i.   Telephone
    ii.   Email
   iii.   Cell phone
   iv.   Walk in

b. The originator will report an incident to Helpdesk. If the nature of the incident is such that the incident can be resolved immediately, such as password reset, for instance, then the Help desk agent will attend to the incident immediately, and update the call logging system accordingly.

c. For second line support calls, Helpdesk will log the incident on the call logging system, prioritize and assign incident to an available resource to resolve the call.

d. Once the call has been logged, the originator will be issued with a call reference number used to follow up on progress and resolution of incident. The call will remain open on the system until the incident has been resolved.If the resolution of an incident may require involvement of external suppliers or service providers (third line of support). In that case, the originator will be informed of such arrangement and possible delays in the resolution of the incident.

f. In the event that the incident is complicated and cannot be resolved within reasonable time periods, or that the resolution of the incident may be prohibitively costly, then the originator will be advised on available options.

g. Before closing any call, the Helpdesk agent must confirm with the originator whether the call has been resolved satisfactorily. Once the incident has been resolved, the call logging system will be updated and the call closed.

9.   CHECKLIST INCIDENT PRIORITY

10.1   The priority of an Incident is a function of the following components:

a.   Urgency (available time until the resolution of the Incident), i.e.
   i.   1: to 0.5 hrs.
   ii.   2: to 2.0 hrs.
   iii.   3: to 6.0 hrs.

b.   Degree of severity (damage caused to the business), i.e.
   i.   1: "High" (interruption to critical business processes)
   ii.   2: "Normal" (interruption to the work of individual employees)
   iii.   3: "Low" (hindrance to the work of individual employees, continuation of work possible by means of a circumventive solution)

10.2   Priority (for example in stages 1, 2 and 3): The result from the combination of urgency and the degree of severity

10.   CHECKLIST INCIDENT ESCALATION

11.1 The Escalation of Incidents follows pre-defined rules:

    a. Defined triggers for Escalations, i.e. combinations of

        i. Degree of severity of an Incident (severe Incidents are, for example, immediately escalated)

        ii. Duration (an Escalation occurs, if the Incident was not resolved within a pre-determined period, as for example the maximum resolution times agreed within the SLAs)

        iii. In an ideal case this would be system-controlled triggered by customisable Escalation rules

11.2 Defined Escalation levels in the form of an Escalation Hierarchy:

        i. 1st Level Support

        ii. 2nd Level Support

        iii. 3rd Level Support

        iv. ICT: Manager

11.3 Assigned triggers to the Escalation Hierarchy (conditions/rules, which lead to the Escalation to a particular level within the Escalation Hierarchy)

11. CHECKLIST CLOSURE OF AN INCIDENT

12.1 The following entries of an Incident Record are investigated for their integrity and completeness during the closure of an Incident:

    a. Protocol of actions

        i. Person in charge

        ii. Support Group

        iii. Time and Date

        iv. Description of the activity

    b. Documentation of applied workarounds

    c. Documentation of the root cause of the Service interruption

    d. Date of the Incident resolution

    e. Date of the Incident closure

12. PROCEDURE REVIEW

This document must be reviewed annually or if necessary to determine if it complies with the current security regulations. In the event that significant related regulatory changes occur, the procedures will be reviewed and updated as needed.