Oshana Regional Council

ICT PLAN
2024

"Pioneering Connectivity
and Innovation"

HIGH LEVEL STATEMENTS

The Oshana Regional Council was established with effect from 31 August 1992 under Section 2 (1) of the Regional Councils Act, 1992 (Act 22 of 1992).

Mission

Oshana Regional Council is committed to govern, plan, and coordinate the implementation of social economic development programmes for sustainable development and improvement of the living standards of the inhabitants.

Vision

Our vision is to be a leading region in the provision of socio-economic development and improved quality of life for inhabitants.

CORE VALUES

Integrity
The quality of being honest and having strong moral principles. We will operate under the auspice of integrity, behaves ethically and do the right thing, even behind closed doors.

Transparency
We will be open to public scrutiny in all our actions taken

Inclusiveness
We ensure that our actions include all groups of people and treat them fairly and equally

Accountability
Being answerable to the people we serve

Innovative
To come up with new ideas, methods and techniques for serving our clients

Responsiveness
To act promptly and effectively to community needs. An institution that responds to its clients and stakeholders within a reasonable time frame

Preface:

In an era defined by the remarkable growth of information and communication technologies, The Council recognizes the pivotal role that Information and Communication Technology (ICT) plays in our mission to serve and empower our community. The Council envisions using ICT as a driving tool behind efficiency, accessibility, and progress of service delivery to its inhabitants. This ICT Plan encapsulates our dedication to fostering an environment where technology is a powerful enabler of our core values. The foundational principle of this plan is pioneering connectivity and innovation – connecting our users to the ICT services they require through new processes and moving away from existing traditional methods. Our ICT Plan places the spotlight on inclusivity, recognizing that ICT services should be accessible to all. We understand that a digital divide can hinder progress, and this plan seeks to bridge that gap, ensuring that all users can benefit from our digital initiatives. We acknowledge that our ICT Plan is not a static document, it is a commitment to pioneering innovation, fostering connectivity, and ensuring that Oshana Regional Council remains at the forefront in this digitalization era. We pledge to stay at the forefront of ICT, embracing new tools, processes, and best practices to elevate our Council.

SINCERELY,

HON. ANDREAS UUTONI
CHAIRPERSON
OSHANA REGIONAL COUNCIL

Acknowledgement

We wish to express our sincere acknowledgment and gratitude to the following:

1. Dedicated Team: We commend the tireless efforts and expertise of our IT section and The Deputy Director of Administration, whose commitment to this plan has been instrumental in its development.

2. Political Office Bearers: We acknowledge the support and inputs provided by our regional leadership, who recognize the importance of technology use for the betterment of our region.

3. Council Staff: We are deeply grateful for the feedback, and active involvement of our officials who have contributed to the development of this plan.

4. Stakeholders: We extend our thanks to our stakeholders who provided their valuable knowledge and best practices in shaping this plan.

Your contributions have been indispensable in shaping this plan, and we look forward to your continued support and collaboration in its implementation.

Sincerely,

TEOPOLINA HAMUTUMUA
CHIEF REGIONAL OFFICER
OSHANA REGIONAL COUNCIL

Table of Contents

ABBREVIATIONS AND DEFINITIONS

Abbreviation	Term
GRN	Government of the Republic of Namibia
ICT	Information and Communications Technology
IT	Information Technology
ITSC	Information Technology Steering Committee
OMAs/RCs	Offices/ Ministries /Agencies /Regional Councils
IoT	Internet of Things
ITIL	Information Technology Infrastructure Library
OPM	Office of The Prime Minister
MURD	Ministry of Urban and Rural Development
ONARC	Oshana Regional Council

EXECUTIVE
SUMMARY

Oshana Regional Council (ONARC) recognizes the vital role that Information and Communication Technology (ICT) plays in delivering effective and efficient public service.

This ICT Plan is a strategic blueprint that underscores our commitment to the use of technology for the benefit of our inhabitants. Our ICT Plan is born from a steadfast commitment to promoting innovation, and digital transformation. It serves as a roadmap to guide The Council's operation in embracing technology responsibly and ethically. The plan defines the appropriate and inappropriate use of the Council's IT resources, information security management, provision and management of ICT devices, password management, service desk requests, and escalation modes.

INTRODUCTION

The ICT Plan aims to streamline administrative processes, improve communication channels, and foster collaboration among different departments in the Council. Embracing modern IT solutions and practices leads to increased efficiency and productivity, ultimately resulting in better service delivery to citizens and businesses. The plan encourages the exploration of emerging technologies like Artificial Intelligence, and Internet of Things (IoT) to create new and efficient solutions to public challenges. A technology-driven public servant can offer more accessible services to citizens. From online portals for information dissemination to digital service platforms, the ICT Plan can facilitate easy access to government services, thereby improving the overall citizen experience.

1. NEED ASSESSMENT

An in-depth assessment of the Council's current ICT infrastructure, systems, and processes reveals opportunities for improvement, particularly in areas such as digital accessibility, data management, accountability and responsibility for ICT equipment, incident reporting, acquisition of IT equipment and IT asset management.

1.1 METHODOLOGY

- ICT survey
- Stakeholder consultation

2. OBJECTIVES

The objectives of this Plan are to:

2.1 Improve Operational Efficiency: Streamline internal processes through automation and digitalization, reducing paperwork and manual interventions.

2.2 Outlines the Acceptable Use of ICT equipment within the Council.

2.3 Strengthen Data Security: Build awareness of cybersecurity to protect and safeguard institution data from unauthorized users.

2.4 Ensure Policy Compliance: Align the ICT plan with the National ICT policy.

3. STRATEGIES AND INITIATIVES

3.1 IT Steering Committee (ITSC): Establish an administrative body that reviews, monitors, and prioritizes major IT projects from a cross-functional perspective.

ITIL Framework: Best practice for IT Service Management; aligns IT services with business needs.

4. DIGITAL INCLUSIVITY

Recognizing the importance of digital equity, we outline our commitment to bridging the digital divide, ensuring that ICT services are accessible to all internal stakeholders. The Council will ensure digital transformation through the implementation of e-Government initiatives, mobile apps, and virtual technology platforms that make it easier for users to interact with each other.

5. CYBERSECURITY

In an era of evolving threats, we prioritize cybersecurity, implementing security measures to protect data from unauthorized access, use, disclosure, disruption, modification, or destruction. In this regard, the IT section will share information related to cyber-attacks and security among Council Staff regularly.

5.1 Capacity Building Enhancement:
- Identify ICT skill gaps for learning development needs.

6. ICT INFRASTRUCTURE

The Council is committed to maintaining its ICT infrastructure to ensure that it remains resilient, scalable, and capable of supporting our growing digital needs.

7. ACQUISITION OF ICT EQUIPMENT

This module provides directives on the acquisition of IT Goods and Services in the Council. The goal is to effectively manage the procurement of IT goods and services to avoid waste of state funds and resources through unnecessary expenditure and to ensure compliance with the Public Procurement Act.
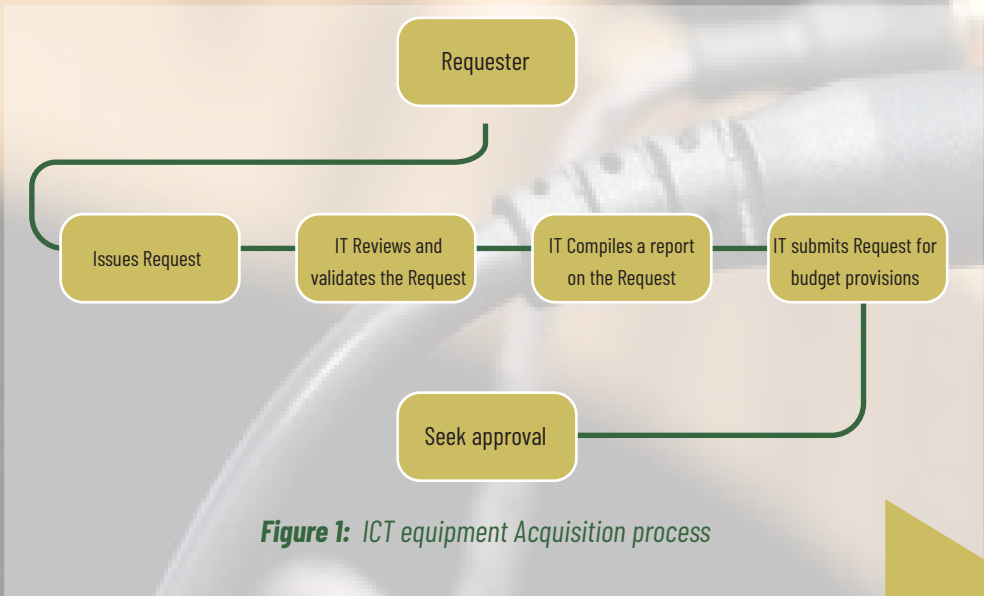
This involves the acquisition of the following:

- Hardware: complete systems and peripherals.
- Software: System applications and Software applications.
- Services: desktop support and maintenance, software support, consultancy services, and other support services.

7.1 ESTABLISHED STRUCTURE

- The requestor (Council Staff) identifies a need (hardware, software, system, service, gadget, etc), a request is submitted to the IT section, an IT specialist performs analysis and assessment on the matter, and a report on the identified need is compiled which is presented and submitted during budgetary meetings to seek for approval.

```
                    ┌──────────────┐
                    │  Requester   │
                    └──────────────┘
┌──────────────┐ ┌──────────────────┐ ┌──────────────────┐ ┌──────────────────┐
│Issues Request│ │  IT Reviews and  │ │IT Compiles a report│ │IT submits Request for│
│              │ │validates the Request│ │  on the Request  │ │ budget provisions │
└──────────────┘ └──────────────────┘ └──────────────────┘ └──────────────────┘
                    ┌──────────────┐
                    │ Seek approval│
                    └──────────────┘
```

Figure 1: *ICT equipment Acquisition process*

8. MANAGEMENT OF COUNCIL ICT RESOURCES

8.1 Acceptable Use of ICT Resources

- The Council ICT Resources e.g. (computers, printers, systems, hardware, internet) are provided to the users to carry out tasks related to their assigned duties and assist in the efficient and effective day-to-day operations of the Council, including but not limited to collaboration and exchange of information within and between OMAs/RCs, other branches of government and private sector.

8.2 General Use Principles

- Users shall avoid improper use of Council ICT resources at all times.
- Using Council ICT resources for unlawful and inappropriate activities shall lead to disciplinary action being taken against such users.

To help improve the effectiveness of the use of these resources, incidental and occasional personal use shall be on condition that such use does not:

- Violate laws of the Republic of Namibia or international laws
- Violate existing policies of higher Offices/Ministries (OPM and MURD).
- Disrupt or distract the conduct of public service business
- Involve personal business activity
- Disclose the Council data to any entity not authorized to receive such information
- Involve illegal activities with intentions to harm the Council and its staff.

9. PROVISION OF COUNCIL ICT RESOURCES

The council provides ICT resources to its users to execute Council-related work.

- Upon issue of the ICT equipment, the IT Official should ensure correct details are captured (Serial number, make, assignee) and recorded in the IT asset register.
- Users shall return all Council ICT devices in working condition such as desktop computers, laptops, speakers, 4G devices, tablets/iPads, and external hard drives to Procurement (Stock Control Unit) when they leave the Council.

- Council ICT equipment, unless intended to be portable, shall not be altered, relocated, or removed from their designated stations without consent from the IT Section.
- The user shall report all lost or stolen equipment to the relevant authority within two working days and provide a police declaration with the case number to the Procurement Administration division.
- Replacement of any ICT equipment due to losses, theft, or damage shall be done as per the recommendation by the IT Section.

9.1 Software Usage
- Users shall not download and install software products on the Council computers. The download/ use of any software system will only be made possible through a request to the IT section.
- Software purchased by the Council shall be used as per its software license agreements.

9.2 Bring Your Own Device
- Prior approval should be granted on the use of outside devices by the IT section.
- Users accessing the Council network through personally owned devices such as laptops shall ensure that such devices are protected with the latest version of anti-virus software.
- Users are solely liable for the security of their devices. The Council shall not be held liable for any losses of devices, or data stored on personal devices accessing the Council network.
- In the event of unforeseen circumstances, support services on outside devices will be provided by the IT section but with limitations on software and hardware.

9.3 Disposal of ICT Resources
A formal communique from the Human Resource Management Division should be sent to the IT Section on the terminations of service for any staff member.

The IT section will take the following action:
I. Dismissal – access rights will be disabled immediately
II. Suspension – access rights will be disabled immediately until reinstatement
III. Resignation – access rights will be disabled on the last day of work.

Furthermore, the IT Section will ensure that:
- Disabled accounts will be permanently deleted after three months.
- Unfit devices for work purposes shall be sent for auction through the right channel.

10. INFORMATION SECURITY MANAGEMENT

10.1 Data Protection

We emphasize the critical importance of data protection and privacy, detailing the measures and protocols in place to safeguard sensitive information.

The focus lies on the protection of the Council's ICT equipment and data against potential threats.

The following safeguard measures must be applied:

- Every user shall be assigned unique login credentials (username and password) to log into the Council's computer. Each user shall take full responsibility to protect their login credentials at all times.
- Users shall take full responsibility for actions undertaken on their user accounts.
- Users have a responsibility to promptly report suspected security breaches to their immediate supervisor or the IT section.
- Users should shut down their workstations when leaving their duty stations.
- Users should avoid sharing work-related correspondences through private email systems as this poses data security risks.
- Users shall maintain the locking of computer screens when not in use to avoid unauthorized access by others.
- The IT section shall ensure that all Council computers are installed with an updated anti-virus program.

11. PASSWORD MANAGEMENT

All passwords shall conform to the following minimum requirements:

a) At least eight (8) characters long.

b) Should not be anything someone can easily guess such as name, telephone number, date of birth, car name, etc.

c) Shall contain a combination of the following:

- Uppercase
- Lowercase
- Number
- Special Character (! @#$%^&?()*_+-={}[]<>., /)
- Passwords must be changed as per the IT set interval.
- Passwords shall never be stored in clear, readable format, as part of a login script, program, or automated process. The user will be held accountable should the password be compromised due to negligent actions.
- At least four (4) characters shall be changed when new passwords are created.
- To limit attempts at guessing passwords or compromising accounts, an account shall lockout after three (3) consecutive invalid password attempts, after which the user shall be required to consult the IT section to unlock and reset their password.

12. SUPPORT SERVICES

12.1 Service Desk Requests

An incident is an unplanned interruption to an Information Technology Service or reduction in the quality of an Information Technology Service.

IT section receives a wide variety of requests from users, including access to the internet, applications, system failure, computer upgrades, malfunctional telephone systems, etc.

12.2 Request fulfillment

Request Fulfillment is the practice tasked with overseeing the entire life cycle of service requests initiated by users, and the Service Desk supervises it. It involves managing various types of service requests, such as password resets, software installations/upgrades, and hardware defects. The approach to fulfilling a request may differ depending on the specific nature of the request. ONARC opts to handle service requests through the GRN Managed Engine Service Desk application in which an IT specialist logs a ticket on behalf of the user.

• Tier 1 Support:
Handled by lower-level technical personnel, this tier addresses basic issues like password resets and basic computer troubleshooting using predefined steps. Tier-one incidents are likely to become incident models due to their frequent recurrence, streamlining the resolution process.

• Tier 2 Support:
This support level consists of more experienced IT personnel, such as System Administrators. Tier 2 tackles more complex issues requiring specialized skills, training, or access to systems such as VIP, IFMS, and Pastel.

• Tier 3 Support:
This tier deals with issues that demand escalation to external IT specialists or third-party service providers for resolution.

12.3 THE INCIDENT MANAGEMENT PROCESS

Incidents go through a structured workflow that encourages efficiency and best results for both IT and users. The Incident Management Process typically follows these steps:

Figure 2: *ITIL Incident Management Process*

ITIL Incident Management process is a structured approach used to handle and resolve Information Technology service incidents efficiently and effectively. It aims to minimize ICT service disruption to users, restore services to normal operation, and prevent recurring incidents.

The key steps involved in the Information Technology Infrastructure Library Incident Management process are further explained below:

12.3.1 Incident Identification:
- The process begins with identifying and recording incidents reported by users or detected through monitoring systems. Incidents can be anything that causes an interruption or reduction in the quality of an Information Technology service.

12.3.2 Incident Logging:
- The identified incidents are logged onto the Managed Service Desk system. This includes recording essential information such as the incident description, the affected service, and the user's contact details.

12.3.3 Incident Categorization and Prioritization:
- Incidents are categorized based on their nature and impact. Prioritization is determined by considering factors like the business impact, urgency, and the number of affected users.

12.3.4 Initial Diagnosis and Investigation:

• The IT support team performs an initial diagnosis to determine the cause of the incident and if it can be resolved at the first level (Tier 1) of support. If not, the incident is escalated to higher support tiers (Tier 2 or Tier 3).

12.3.5 Incident Resolution and Recovery:

• The IT team works on resolving the incident and restoring the affected service to normal operation. Regular updates are provided to the user throughout the resolution process.

12.3.4 Incident Closure:

• Once the incident is resolved, it is marked as closed on the system. Closure includes obtaining user confirmation that the service is functioning correctly.

12.3.5 Incident Escalation:

• Incidents may be escalated to higher support levels if they cannot be resolved at the initial support level or if they have a significant impact on the business.

12.3.6 Incident Review and Analysis:

• After incident closure, a post-incident review is conducted to analyze the root cause, identify areas of improvement, and prevent similar incidents from occurring in the future.

12.3.7 Incident Communication:

• Throughout the incident management process, communication with users and stakeholders is crucial to manage expectations, provide updates, and inform them about the status of the incident.

13. IT ASSET REGISTER MANAGEMENT

This module involves gathering detailed hardware device information within the Council. IT inventory management helps the institution to manage its assets more effectively. The inventory information should be kept up-to-date, and stored in a custom-developed database. Redundant and non-functional IT Assets should be disposed of.

IT Section should:

• Ensure that all IT Assets in the Council are identified, controlled and properly cared for throughout their lifecycle.

14. REVIEW

This ICT Plan shall be reviewed after 3 years or when other circumstances arise such as:
Situations that comprise the council to carry its mandates. The review process shall be conducted in consultation with the internal and external stakeholders.

15. CONCLUSION

The ICT plan outlined a comprehensive and strategic roadmap that aims to transform our operations, enhance service delivery, and foster innovation in the digital age. By leveraging cutting-edge technologies and establishing a robust infrastructure, we are poised to address current challenges and capitalize on emerging opportunities.

The plan prioritizes key areas such as cybersecurity, data management, and digital literacy to ensure the integrity, confidentiality, and accessibility of our information. The commitment to ongoing training and professional development for our staff is crucial, as it ensures that they are equipped with the skills needed to navigate the ever-evolving ICT landscape. Collaboration with external stakeholders, including private sector partners and neighboring governments, will be fostered to create synergies and share best practices.

As we embark on the implementation phase, it is imperative that we remain agile and adaptive to changes in technology and the needs of our community. Regular assessments and updates to the plan will be conducted to ensure its relevance and effectiveness over time.

Ultimately, this ICT plan is not just a technological blueprint; it is a strategic investment in the future of the Council. Through its successful execution, we anticipate improved efficiency, transparency, and citizen engagement, reinforcing our commitment to providing high-quality services to the residents we serve. By embracing digital transformation, we position ourselves as leaders in the smart and connected government space, ready to meet the challenges of the 21st century.