Republic of Namibia

OFFICE OF THE PRIME MINISTER
DEPARTMENT PUBLIC SERVICE I.T. MANAGEMENT

REVISED IT POLICY FOR THE PUBLIC SERVICE

2017

ACKNOWLEDGEMENT

The Office of the Prime Minister (OPM) through the Department Public Service Information Technology Management (DPSITM) would like to thank all Offices, Ministries and Agencies (O/M/As) and individuals who have contributed to this Revised IT Policy for the Public Service 2017. Your contribution is most valued.

OPM would also like express gratitude to the Permanent Secretaries Forum and the Cabinet Committee on Public Service for the guidance during the review process of the IT Policy for the Public Service Volume III.

OPM looks forward to co-operation from all O/M/As during the implementation phase of this Revised IT Policy for the Public Service 2017.

Table of Contents

FOREWORD 5

ACRONYMS AND ABBREVIATIONS 6

GLOSSARY OF CONCEPTS, TERMS AND JARGONS 7

EXECUTIVE SUMMARY 8

1. INTRODUCTION 10

2. BACKGROUND 10

3. RATIONALE 11

4. ALIGNMENT 11

5. GUIDING PRINCIPLES 11

5.1. MODULE I - INSTITUTIONAL ARRANGEMENT 11

5.1.1. Introduction 11

5.1.2. Objectives 12

5.1.3. Strategies 12

5.2. MODULE II – IT GOVERNANCE AND IT SERVICE MANAGEMENT 15

5.2.1. IT GOVERNANCE 15

5.2.1.1. **Introduction** 15

5.2.1.2. **Objectives** 15

5.2.1.3. **Strategies** 16

5.2.2. IT SERVICE MANAGEMENT (ITSM) 16

5.2.2.1. **Introduction** 16

5.2.2.2. **Objectives** 16

5.2.2.3. **Strategies** 16

5.3. MODULE III – OPEN, CO-OPERATIVE INFORMATION SYSTEMS AND DEVELOPMENT OF IT INFRASTRUCTURE 17

5.3.1. Introduction 17

5.3.2. Objectives 17

5.3.3. Strategies 18

5.4. MODULE IV - IT HUMAN RESOURCE MANAGEMENT AND DEVELOPMENT 18

5.4.1. Introduction 18

5.4.2. Objectives 19

5.4.3. Strategies 19

5.5. MODULE V - INFORMATION SECURITY MANAGEMENT 19
5.5.1. Introduction 19
5.5.2. Objectives 20
5.5.3. Strategies 20
5.6. MODULE VI - ACQUISITION OF IT GOODS AND SERVICES 20
5.6.1. Introduction 20
5.6.2. Objectives 20
5.6.3. Strategies 21
5.7. MODULE VII - IT ASSET MANAGEMENT 21
5.7.1. Introduction 21
5.7.2. Objectives 21
5.7.3. Strategies 21
6. IMPLEMENTATION ARRANGEMENTS /FRAMEWORKS 22
6.1. Institutional Arrangements 22
6.2. Legal and Regulatory Arrangements 22
6.3. Resource Mobilisation 22
7. MONITORING AND EVALUATION FRAMEWORK AND REPORTING: 23
8. ADVOCACY AND DISSEMINATION (COMMUNICATION STRATEGY): 23
9. IMPLEMENTATION ACTION PLAN: 23
10. POLICY REVIEW 24
11. CONCLUSION 24

FOREWORD

Information Technology (IT) has profoundly changed almost all aspects of society. It is now central to how people communicate, interact, make decisions and do business. This includes the way government operate and deliver services to citizens and businesses. There is also a concerted effort to deliver Online Services to citizens and businesses through the implementation of e-governance and this requires new approaches to the use and management of Information Technologies in the Public Service.

Government is further faced with emerging challenges and risks pertaining to information security management and cyber security. This has necessitated a review of the current IT Policy for the Public Service Volume III, which has been in use since 2003.

Building on the successes that have been achieved with the IT Policy for the Public Service Volume III, the Revised IT Policy for Public Service 2017 sets out how government can operate in a more effective, shared and integrated manner while delivering new and innovative online services to citizens and businesses. The revised policy is built on a vision of standardisation, consolidation, reduction in duplication of systems and infrastructure, shared services such as email and IT infrastructure, secure and authorised access to data, skilled IT personnel, better protection of citizens' private information and GRN data, and reduction of costs for provision of IT Services. The revised policy also places a greater emphasis on Information Security Management to minimize the risk of un-authorised access to government and citizen's data and to ensure minimal disruption to government operations.

Moving to a more integrated and shared infrastructure model will deliver efficiencies across the Public Service as it will allow O/M/As to collaborate and share information and facilitate easier data exchange and integration of systems in order to provide effective online services to citizens and businesses. Hence the need to adopt international best practice with regard to Governance and Management of IT Services, as well as Information Security Management in the Public Service. This revised policy is benchmarked on international best practice and its implementation is expected to yield significant benefits to the government.

The potential for improvement through the innovative use of technology is significant. Implementation will require a transformational programme of change, not just technological but administrative and cultural. When implemented, the revised policy will deliver an enhanced quality of service.

This Revised IT Policy for the Public Service 2017 was prepared by the Department Public Service IT Management within the Office of the Prime Minister in consultation with the Ministry of Information and Communications Technology (MICT) and the Public Service Committee on IT (PSCOIT) and I wish to express my appreciation for their efforts and I look forward to seeing the positive outcomes as the revised policy is implemented.

ACRONYMS AND ABBREVIATIONS

ACRONYM	DESCRIPTION
CCPS	Cabinet Committee on Public Service
DPSITM	Department of Public Service Information Technology Management
GRN	Government of the Republic of Namibia
HRD	Human Resource Development
IT	Information Technology
ISM	Information Security Management
ISO	International Standards Organisation
ITG	Information Technology Governance
ITIL	Information Technology Infrastructure Library
ITSM	Information Technology Service Management
MICT	Ministry of Information and Communications Technology
OMAs	Offices, Ministries, Agencies
OPM	Office of the Prime Minister
PSCOIT	Public Service Committee on IT
RCs	Regional Councils
SLA	Service Level Agreement
SMART	Specific, Measurable, Achievable, Relevant and Time-bound
UCS	Unified Communication System

GLOSSARY OF CONCEPTS, TERMS AND JARGONS

CONCEPT	DESCRIPTION
Cloud Computing	Cloud computing is a general term for the delivery of hosted services over the internet.
Cyber Security	Cybersecurity is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.
Information Security Management	Information Security Management (ISM) refers to the identification of security risks, and the implementation of a set of policies and procedures for systematically managing an organization's sensitive data. The goal of ISM is to minimize risk and to ensure business continuity by pro-actively limiting the impact of security breaches.
Information Technology Service Asset Management	An Information Technology Service Asset is classified as any GRN-owned or licensed software, information system, business application, network or hardware that is used in the delivery and support of business activities. The Information Technology Service Asset Management process typically involves gathering, documenting and recording of a detailed inventory of an organization's hardware and software and then using that information to make informed decisions about IT-related consolidation, procurement, redistribution and support.
Information Technology Governance	Information Technology Governance (ITG) is defined as the processes that ensures the effective and efficient use of IT in enabling an organization to achieve its goals. IT Governance ensures that IT projects are aligned, directed and monitored to support the specific goals and objectives of the O/M/As at a whole- of- government level.
Information Technology Service Management	Information Technology Service Management (ITSM) refers to a strategic approach for designing, delivering, managing, supporting and improving the way information technology (IT) is used within an organization. The goal of ITSM is to ensure that the correct mix of processes, people and technology are established to ensure that organizations can meet their business objectives.
Information Technology Steering Committee	An Information Technology Steering Committee is an administrative body that reviews, monitors and prioritizes major IT projects within an organization from a cross-functional perspective.
Interoperability Framework	Interoperability is the ability of disparate and diverse organisations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between the organisations, through the business processes they support, by means of the exchange of data between their respective Information Technology (IT) systems.
Open Standards	Open Standards are standards made available to the general public and are developed (or approved) and maintained via a collaborative and consensus driven process. Open Standards facilitate interoperability and data exchange among different products or services and are intended for widespread adoption.
Unified Communication System	Unified Communications System (UCS) refers to the integration of communication tools such as email and instant messaging to help people exchange ideas and do their work more effectively.

EXECUTIVE SUMMARY

The IT Policy for the Public Service was adopted in 1993 (Cabinet Decision Number 41st/7.12.93/009) and was revised and adopted in 2003 (Cabinet Decision Number 26th/23.09.03/001) as the IT Policy for the Public Service Volume III. The IT Policy for the Public Service Volume III comprised of seven modules addressing various aspects of IT Service Management within the Public Service.

The IT Policy for the Public Service Volume III has been implemented over the past fourteen years and some of the significant achievements are as follows:

- The Public Service Committee on IT (PSCOIT) comprising of Heads of IT from all Offices/Ministries and Agencies (O/M/As) was successfully constituted. PSCOIT in collaboration with the Department of Public Service IT Management (DPSITM) has since served as the consultative body for the formulation of specifications for computer equipment, policies, standards, guidelines and operational procedures for the Public Service.
- Ministerial Information Technology Units (MITU) have also been established in all O/M/As. The Ministerial Information Technology Units provide IT support within their respective O/M/As.
- Most O/M/As have deployed back-office administrative Information Management Systems that complies to open standards to enable exchange of data with other systems.
- Information Technology Infrastructure has successfully been deployed in O/M/As and Regional Councils (RCs) to enable provision of essential services such as Internet and Email.
- A shared Unified Communication System (UCS) has been setup at the Office of the Prime Minister, Department Public Service IT Management to host and provide email service to all Civil Servants.

Despite these major achievements over the years, new challenges have since emerged, particularly with regard to Information Security Management, Cyber Security, Sharing of Data and IT Service Management to mention but a few. These challenges coupled with major technological advancements such as Cloud Computing have necessitated a review of the IT Policy for the Public Service Volume III to address the gaps and to align to best practice. The Revised IT Policy for the Public Service 2017 aims to build on the successes of the IT Policy for the Public Service Volume III and sets the direction for the management of IT Services in the Public Service into the future based on international best practice.

The Revised IT Policy for the Public Service 2017 comprises of the following seven modules:

Module I – Institutional Arrangement: This module sets the direction with regard to the establishment of organizational structures and various committees, as well as their roles and responsibilities to ensure effective management of IT Services within the Public Service.

Module II – IT Governance and IT Service Management: This module provides directives with regards to the Governance and Management of IT Services within the Public Service with the core objectives being; Benefits Realisation, Risk Optimisation and Resource Optimisation.

Module III – Open, Co-operative Information Systems Architecture and Development of IT Infrastructure: This module provides directives on the establishment of IT infrastructure within O/M/As and RCs as well as the development and implementation of information management systems based on open standards.

Module IV - Human Resources Development and IT Personnel Administration: This module provides guidance on the management and skills development of IT personnel in the Public Service to ensure that GRN has the prerequisite skills in managing and supporting IT Service Management.

Module V – Information Security Management: This module aligned to international standards such as ISO 27001 and 27002 provides guidance on how to protect GRN's data from unauthorised access. The goal of Information Security Management is to minimize risk and ensure business continuity by pro-actively limiting the impact of a security breach.

Module VI – Acquisition of IT Goods and Services: This module provides directives on the acquisition of IT Goods and Services in the Public Service. The goal is to effectively manage the procurement of IT Goods and Services to avoid waste of state funds through unnecessary expenditure and to ensure compliance to the Public Procurement Act.

Module VII - IT Asset Management: This module provides guidance on the record keeping and disposal of all IT Assets in the Public Service. The goal is to ensure an accurate record of all information technology assets, their relationships and lifecycle costs to enable GRN to make informed decisions about IT-related consolidation, procurement, redistribution and support.

The Revised IT Policy for the Public Service 2017 will be implemented across O/M/As and RCs in phases and its implementation will be monitored and reviewed on a quarterly basis.

1. INTRODUCTION

Information Technology has undergone major innovation and development over the past decade, and this has presented new opportunities for innovative use of technology to deliver better services to citizens and businesses. These major developments have however also presented major challenges such as information security management and cyber security threats which require new approaches to the management of IT Services in the Public Service.

There is also a demand from citizens and businesses for secure online services and this requires effective support teams to ensure that the online services are up and running at all times. This will also require secure and effective means of sharing data and information across the Public Service and hence appropriate measures need to be put in place to safe guard citizen and GRN data from un authorised access and protect GRN systems from Cyber Attacks.

The delivery of IT services will need to be responsive and effective in the face of these challenges and within the financial constraints. GRN will therefore adopt the concept of technology 'as a service' underpinned by a strong service culture from a professional IT workforce to enable GRN to deliver effective services to citizens and business and to support internal operations.

This Revised IT Policy for the Public Service 2017 comprising of seven (7) modules addresses various aspect of IT Service Management and IT Governance and has been aligned to international best practice taking into consideration the unique needs of GRN aimed at addressing the current challenges and to create a new platform for innovative use of technology such as cloud computing, shared services, and technology as a service in the Public Service.

Guidelines and Standard Operating Procedures will further be developed in support of this policy making it easier for O/M/As and RCs to implement.

2. BACKGROUND

The IT Policy for the Public Service Volume III was adopted in 2003 (Cabinet Decision Number 26TH/23.09.03/:001).The policy comprised of seven (7) modules addressing various aspects of IT within the Public Service, namely:

- **Institutional Arrangements** which dealt with the organizational structures and various committees which had to be established. Most of the organizational structures and committees have been established as directed by the policy with the exception of the Cabinet Committee on IT that was never constituted.
- **Open, Co-operative Information Systems Architecture:** Most O/M/As have deployed back-office administration systems, however a challenge exists to make some of the systems inter-operable. There is now a need for systems to be able to exchange data particularly with the demand for on-line services by citizens and businesses.
- **Human Resources Development:** Most O/M/As and RCs have dedicated training budgets. The skills and training needs are identified as per the Performance Management Policy. IT personnel have undergone various specialized training over the years, however the government has faced a challenge of retaining the trained and highly skilled personnel in specialized areas as they have often ventured off to the private sector that offers higher remuneration packages compared to government, a situation which has left government to rely heavily on Service Providers. There is a need to consolidate and share specialized skills across the Public Service, particularly in the area of IT Service Management, which includes critical processes such as Information Security Management (ISM).
- **Computer Security:** Security measures such as access control to server rooms, installation of anti-viruses software on Personal Computers, Laptops and Servers have been implemented, however these measures are no longer adequate considering the sophisticated techniques and approaches being employed by Cyber Criminals, hence a need to align to international best practice on Cyber Security and Information Security Management to safeguard against unauthorized access of GRN data and to minimize the impact of security breaches on GRN operations.
- **Development of Information Technology Infrastructure:** Most O/M/As and RCs have developed IT infrastructure which enable provision of crucial services such as internet and email. OPM-DPSITM in

conjunction with Telecom Namibia has also developed a multiprotocol label switching (MPLS) network aimed at providing connectivity to GRN offices in the regions. Furthermore, OPM - DPSITM has also developed IT infrastructure at all the Regional Councils, referred to as points of presence (POPs) aimed at connecting all Regional Councils to the GRN Data Center in Windhoek to enable staff members to access services such as internet, email and applications such as the Integrated Financial Management System(IFMS) and Payroll.

- **Acquisition of Hardware, Software and Services:** Standard Specifications have been formulated over the years that have been used by O/M/As to procure IT Goods and Services as per the Tender Board Act. There is a need to align the procurement of IT Goods and Services to the new Public Procurement Act.
- **Information Technology Personnel Administration:** Information Technology Personnel are administered and managed as per the GRN HR Polices, Staff Rules, Labor Act and the Public Service Act.

The IT Policy for the Public Service Volume III has been in effect since 2003, and despite the significant achievements over the years, the policy has since not been revised and new challenges pertaining to management of IT Services such Information Security Management, Sharing of Data, etc., have emerged that necessitated the review of the current policy.

3. RATIONALE

Government has increasingly become reliant on Information Technology to render services to citizens and businesses and to support internal operations. The IT Policy for the Public Service Volume III has been revised to address the new challenges pertaining to the management of IT Services in government which must be addressed if more customer-focused and effective public services are to be delivered.

4. ALIGNMENT

The Revised IT Policy for the Public Service 2017 is aligned to the following national policies, international standards and frameworks:

- Overarching Information Communications Technology (ICT) Policy for the Republic of Namibia 2009
- ISO 27001 and 27002 on Information Security Management
- ISO 20000, the standard upon which IT Service Management (ITSM) is defined
- ISO 31000 for Risk Management
- ISO 15504 Information Technology Process Assessment
- Information Technology Infrastructure Library (ITIL) which is a globally recognized set of best practices and standards that support IT Service Management (ITSM)
- Control Objectives for Information and Related Technologies (COBIT) which ensures compliance of Governance Principles
- The NamCode – The corporate governance code for Namibia

5. GUIDING PRINCIPLES

The guiding principle is to ensure that there is effective governance and management of IT Services in the Public Service underpinned by standardised Policies, Procedures and Processes aligned to "Best Practice" to improve GRN internal operations and to support the delivery of effective services to citizens and business.

5.1. MODULE I - INSTITUTIONAL ARRANGEMENT

5.1.1. Introduction

Cabinet, through Decision No. 41st/7.12.93/009 had approved the IT Policy for the Public Service Volume III to enable O/M/As to plan and implement their computerisation activities, and where the Department of Public Service Information Technology Management (DPSITM) serves as a central agent to monitor, control and co-ordinate all computer activities within the public service.

Central technical support, management of government information systems, hardware, software and services procurement, maintenance and consultancy contract agreements, training and re-training of IT personnel, all need to be coordinated.

This module is, therefore, intended to clearly delineate the roles and responsibilities of the various institutions involved in public service information technology activities.

The module outlines the following:

- Duties and responsibilities of the Cabinet Committee on Public Service (CCPS);
- Duties and responsibilities of the Permanent Secretaries Forum;
- Roles and responsibilities of the Department of Public Service Information Technology Management (DPSITM);
- Duties and Responsibilities of the Public Service Committee on IT (PSCOIT);
- Roles and responsibilities of Ministerial IT Steering Committees (MITSC);
- Roles and responsibilities of Ministerial IT Units (MITU).

5.1.2. Objectives

5.1.2.1. To ensure that there is a clear delineation of roles and responsibilities between the various institutions involved in the management of IT Services in the public service;

5.1.2.2. To promote collaboration between all key stakeholders in the Public Service, and to ensure that value will be created through effective management of IT resources;

5.1.2.3. To ensure that Governance and Management of IT Services addresses and caters for the evolving needs of government.

5.1.3. Strategies

The main strategy is to clearly delineate the roles and responsibilities of the various institutions involved in public service information technology governance and management activities as follows:

5.1.3.1. **Cabinet Committee on Public Service (CCPS)**

This section describes the roles and responsibilities of the Cabinet Committee on Public Service (CCPS).

Terms of Reference

- To set the overall objectives and goals of IT Service Management as a discipline in government that is aligned to strategic plans and objectives of government;
- To promote the standardization of IT Service Management in government, and adoption and implementation of best practices with regards to Information Security, Governance and Management of IT Services;
- To promote sharing of IT infrastructure, resources, data and services amongst O/M/As and RCs, to eliminate costly duplications and inefficiencies; and
- Monitor the implementation of policy, review and amend the IT policy when required.

5.1.3.2. **Permanent Secretaries Forum (PSF)**

This section describes the roles and responsibilities of the Permanent Secretaries Forum (PSF).

Introduction

The Permanent Secretaries in their capacity as Accounting Officers for the O/M/As will play a vital role in the implementation and oversight of this Revised IT Policy for the Public Service 2017. Hence, there is a need for the Permanent Secretaries Forum to provide the necessary support and guidance with the implementation of this policy.

Terms of Reference

5.1.3.2.1. To be responsible for the implementation of the Revised IT Policy for the Public Service 2017 within their respective O/M/As;

5.1.3.2.2. To provide feedback on the progress with the implementation of the Revised IT Policy for the Public Service 2017 to Cabinet Committee on Public Service;

5.1.3.2.3. To review and provide guidance on new IT Policy initiatives;

5.1.3.3. **Department Public Service Information Technology Management (DPSITM)**

This section describes the roles and responsibilities of the Department of Public Service Information Technology Management (DPSITM).

Introduction

Cabinet, through Decision No. 41st/7.12.93/009, has approved the establishment of IT Division/Units in O/M/As. It has also approved the retention of the Department of Public Service Information Technology Management (DPSITM) in the Office of the Prime Minister to function as a central agent for governance, co-ordination, monitoring, and controlling government information technology activities. As a central agent, DPSITM should thus act as an information technology policy initiator, policy executive body, information management authority as well as a technical and functional support center.

DPSITM should thus play a leading role in the computerisation of the Namibian Public Service. It should therefore, be equipped with advanced information technology facilities and an up-to-date information technology library, and staffed with well-educated, highly-trained, experienced professionals and dedicated personnel.

Terms of Reference

5.1.3.3.1. To develop and co-ordinate the implementation of IT Governance and IT Service Management Frameworks in the Public Service based on international best practice;

5.1.3.3.2. To develop and co-ordinate the implementation of professional standards and technical support programmes;

5.1.3.3.3. To periodically conduct government IT needs analyses;

5.1.3.3.4. To review, monitor and co-ordinate the implementation of integrated strategic plans for the development of inter-ministerial management information systems;

5.1.3.3.5. To conduct internal audit and compliance assessments of IT Policies;

5.1.3.3.6. To setup, maintain and operate a common shared government Data Centre and Disaster Recovery Site;

5.1.3.3.7. To setup and maintain a government-wide Unified Communication System (email, etc.);

5.1.3.3.8. To initiate IT Policy proposals and present them to the Permanent Secretaries Forum;

5.1.3.3.9. To co-ordinate and maintain an up to date register of systems and applications within government;

5.1.3.3.10. To co-ordinate and maintain an up to date register of government IT Assets;

5.1.3.3.11. To promote and co-ordinate the development of sectoral information systems;

5.1.3.3.12. To be responsible for data and information resources management within the government; including computer, data and information security;

5.1.3.3.13. To monitor the acquisition of hardware and software, and entry into service level agreements and contracts in collaboration with the Office of the Attorney General;

5.1.3.3.14. To be responsible for the development of management information systems and website for the Office of the Prime Minister and extension of this service to other O/M/As and RCs when requested;

5.1.3.3.15. To develop, manage, operate and maintain an integrated government-wide management information systems which is to be located at DPSITM;

5.1.3.3.16. To develop, manage, operate and maintain an e-Government and Interoperability platform for on-line services and data exchange;

5.1.3.3.17. To provide technical assistance and support to O/M/As and RCs in the development, implementation, operation and maintenance of their management information systems;

5.1.3.3.18. To organize and conduct research and training programmes to develop the skillsets of IT personnel within the Public Service; and

5.1.3.3.19. To undertake any IT-related assignment which the Office of the Prime Minister or Cabinet may deem fit.

5.1.3.4. Public Service Committee on IT (PSCOIT)

This section describes the duties, responsibilities and constitution of the Public Service Committee on IT (PSCOIT).

Introduction
For the effective coordination of government information system planning, development and implementation, there is a need to have a body on which each O/M/As is represented. This committee shall be a policy- proposal advisory and consultative body, which provides policy inputs, reviews and amendments on such IT policies for consideration by DPSITM.

Terms of Reference

5.1.3.4.1. To serve as a forum for discussing IT policies related matters and dissemination of information that cut across O/M/As;
5.1.3.4.2. To co-ordinate the implementation of policies and professional standards in the government;
5.1.3.4.3. To review IT policies and provide amendment proposals for consideration by the DPSITM; and
5.1.3.4.4. To undertake any tasks as requested by Cabinet.

Constitution
PSCOIT shall comprise of heads of IT that have been designated by the respective Permanent Secretaries from O/M/As.

5.1.3.5. Ministerial Information Technology Units (MITU)

This section describes the roles and responsibilities of the Information Technology Units in O/M/As.

Introduction
Cabinet has approved the establishment of Ministerial IT Units through Decision No. 41st/7.12.93/009 to develop, implement, and maintain information technology services for the establishment. Most O/M/As have established Information Technology Units. Based on the size of the O/M/As, amount and complexity of information systems developed or to be developed within that establishment, a structure may be adopted to cater for the following functions:

- **IT Operations and Technical Management** to be responsible for the day-to-day maintenance and management of the IT infrastructure. Tasks include backup and restore, maintenance and support activities, monitoring, managing and supporting the IT infrastructure.
- **Information Security Management** to protect information and information infrastructure assets against the risks of loss, misuse, unauthorised access, disclosure or damage, and to ensure business continuity by pro-actively limiting the impact of security breaches.
- **Applications Management** to be responsible for managing applications throughout their lifecycle, including designing, testing, operating, supporting and improving IT services, as well developing the skills required to manage the applications.
- **Facilities Management** to be responsible for the management of the physical environment where the IT infrastructure is located. Tasks includes all aspects of managing the physical environment, for example power and cooling, building access management, and environmental monitoring.
- **Service Desk** to be the single point of contact between users and IT Service Management. Tasks include user support, managing incidents and requests.

The number of IT personnel required can be increased if the needs are justified. This shall be motivated by the O/M/As and shall be endorsed by DPSITM before the Public Service Commission can approve the creation of additional posts.

5.1.3.6. Ministerial Information Technology Steering Committee (MITSC)

Each O/M/A which intends to embark on a computerization initiative shall be required to set up a Ministerial Information Technology Steering Committee (MITSC).

The MITSC shall provide overall leadership and direction to the implementation of IT projects, as defined by the policy directives and guidelines from DPSITM. It shall serve as the administrative body that reviews, monitors and prioritizes major IT projects within the O/M/A.

Constitution of the Ministerial Information Technology Steering Committee (MITSC)

The Chairperson of the MITSC shall be the Permanent Secretary of the O/M/A.

In his/her absence, the chairperson shall be the Deputy Permanent Secretary, his/her delegate or the person who represents the O/M/A on the Public Service Committee on IT.

Members of the MITSC shall be appointed by the Permanent Secretary and shall constitute of the heads of the different IT Functions, the person who represents the O/M/A on the Public Service Committee on IT as well as the heads of the different business units of the O/M/A.

Terms of Reference for the MITSC

The Ministerial Information Technology Steering Committee shall:

5.1.3.6.1. Develop IT strategies and plans (both short, medium and long-term) aligned to the O/M/As strategic business objectives and goals;
5.1.3.6.2. Provide overall direction and leadership for the implementation of IT Projects within the O/M/As;
5.1.3.6.3. Prioritize IT initiatives and projects in line with the O/M/As business strategy and priorities;
5.1.3.6.4. Monitor and review IT initiatives and projects on a regular basis;
5.1.3.6.5. Monitor and review contracts and service level agreements with suppliers;
5.1.3.6.6. Provide oversight with the implementation of IT Policies within the O/M/As; and
5.1.3.6.7. Endorse the acquisition of hardware, software and other services and submit all proposals, master plans, and other computerization plans to DPSITM for approval. The DPSITM will not process any IT request without the written consent of the Permanent Secretary of the line O/M/A.

5.2. MODULE II – IT GOVERNANCE AND IT SERVICE MANAGEMENT

5.2.1. IT GOVERNANCE

5.2.1.1. Introduction

At its most fundamental level, IT governance defines who makes decisions and how those decisions are made. IT governance is the process by which institutions align IT actions with their goals and objectives. This involves establishing decision rights (who decides what) and an accountability framework (who is responsible for what) for encouraging desirable behaviours and actions in the deployment and use of IT.

5.2.1.2. Objectives

5.2.1.2.1. To enable the strategic and tactical alignment of IT with GRN objectives, priorities and goals;
5.2.1.2.2. To understand the value and impact of IT investments (financial and human resources);
5.2.1.2.3. To identify opportunities for improved IT utilization;
5.2.1.2.4. To support visible and transparent decision making;
5.2.1.2.5. To establish and sustain effective IT policies;
5.2.1.2.6. To establish performance measurements;
5.2.1.2.7. To identify and mitigate risks; and
5.2.1.2.8. To satisfy regulatory and formal compliance requirements.

5.2.1.3. Strategies

DPSITM established through Cabinet Decision No. 41st/7.12.93/009 as a central agent to monitor, control and co-ordinate all IT activities within the public service shall:

5.2.1.3.1. Develop and adopt an IT Governance Framework for the Public Service aligned to GRN's strategic objectives and goals;

5.2.1.3.2. Coordinate and provide oversight for the implementation of IT Governance in the Public Service;

5.2.1.3.3. Report identified IT related risks and their implications to the Permanent Secretaries' Forum and the Cabinet Committee on Public Service;

5.2.1.3.4. Monitor the implementation of IT policies and report the progress to the Permanent Secretaries' Forum and the Cabinet Committee on Public Service; and

5.2.1.3.5. Submit proposals for improvements to IT policies and IT Governance to the Permanent Secretaries' Forum and the Cabinet Committee on Public Service for review, evaluation and approval.

5.2.2. IT SERVICE MANAGEMENT (ITSM)

5.2.2.1. Introduction

IT Service Management (ITSM) is a process-based practice intended to align the delivery of IT services with the needs of an institution leading to effective service delivery. An ITSM framework based on best practice shall be adopted for the Public Service.

5.2.2.2. Objectives

5.2.2.2.1. To ensure that the correct mix of processes, people and technology are established so that organizations can meet their business objectives; and

5.2.2.2.2. To effectively manage all IT services and underlying technology components and support resources.

5.2.2.3. Strategies

DPSITM established through Cabinet Decision No. 41st/7.12.93/009 as a central agent to monitor, control and co-ordinate all IT activities within the Public Service shall:

5.2.2.3.1. Develop and adopt an IT Service Management Framework for the Public Service aligned to GRN's requirements;

5.2.2.3.2. Coordinate and oversee the implementation of IT Service Management in the Public Service;

5.2.2.3.3. Develop operational guidelines and procedures to be adopted by O/M/As and RCs when implementing IT Service Management;

5.2.2.3.4. Develop skills and capacity of IT personnel in the Public Service in the discipline of IT Service Management and adopted frameworks, through internationally accredited trainings, and knowledge and skills transfer;

5.2.2.3.5. Carryout audit and compliance assessments to ensure that IT Service Management aligned to IT Governance is implemented in the Public Service;

5.2.2.3.6. Report on the progress of the implementation of IT Service Management to the Permanent Secretaries' Forum and the Cabinet Committee on Public Service; and

5.2.2.3.7. Submit proposals for improvements to IT Service Management to the Permanent Secretaries' Forum and the Cabinet Committee on Public Service for review, evaluation and approval.

O/M/As and RCs shall:

5.2.2.3.8. Implement relevant IT Service Management Processes aligned to the needs of the O/M/As and RCs;

5.2.2.3.9. Ensure that the IT structure has clearly defined roles and responsibilities for managing IT services in relation to defined IT Service Management Processes;

5.2.2.3.10. Ensure that performance of IT services is measured and reported to management;

5.2.2.3.11. Ensure that feedback from business stakeholders, IT support and management is used to continually improve IT services;

5.2.2.3.12. Through the IT Steering Committees, ensure that IT initiatives and investments are aligned to the mission and strategic objectives of the O/M/As and RCs;
5.2.2.3.13. Ensure that IT related risks and impact on businesses are identified and managed;
5.2.2.3.14. Ensure that all IT plans and projects are regularly monitored, reviewed and discussed at management level; and
5.2.2.3.15. Ensure that regular IT Steering Committee meetings are conducted to ensure that objectives are being addressed and achieved.

5.3. MODULE III – OPEN, CO-OPERATIVE INFORMATION SYSTEMS AND DEVELOPMENT OF IT INFRASTRUCTURE

5.3.1. Introduction

Information Technology has traditionally been delivered on a standalone basis with limited sharing of infrastructure and services between various government entities. Some O/M/As and RCs have acquired expensive, heterogeneous computer equipment from multiple vendors that, in some cases, are incompatible with each other. This has created silos resulting in little or no sharing of information between systems. Since information cannot easily be shared between such computing systems, duplication of resources is inevitable.

GRN requires applications software and business applications to carryout administrative processes and deliver services to citizens and businesses. The objective of this module is to define the conditions for the acquisition, development, implementation and maintenance of business Applications by the GRN. Business applications store and process a significant amount of the GRN's critical and confidential information. It is imperative that business applications are appropriately acquired or developed to ensure the minimum security requirements and procurement processes are followed to prevent duplication of purchasing and ensure supportability.

A challenge also exists to create a model where services can be delivered on a shared basis within the existing developed structures while meeting the needs of different O/M/As and RCs. Significant scope exists to expand existing IT shared services initiatives and create new opportunities for the elimination of duplication and to create greater efficiencies across the Public Service. The provision of a more integrated infrastructure and common systems will make it easier for O/M/As and RCs to collaborate and share data and information.

There is now a worldwide trend to move information systems from vendor locked-in proprietary environments and mainframes to open systems. Open systems are defined as information systems in which the components and protocols conform to standards independent of a particular vendor.

Open systems will help O/M/As and RCs move their information systems from vendor–locked in architectures to other architectures based on open standards when needed. This will enable the sharing of resources through networked systems, and will help to ensure interoperability and compatibility between computer systems.

5.3.2. Objectives

The objectives are:

5.3.2.1. To enable an open, multi-vendor environment that will allow for interoperability and compatibility between different technologies and applications;
5.3.2.2. To create shared IT services to support integration across the wider Public Service to drive efficiency, standardisation, consolidation, reduction in duplication and thus to minimise additional capital expenditure;
5.3.2.3. To eliminate duplication of business applications and Systems in the Public Service;
5.3.2.4. To establish a GRN -wide Enterprise Architecture based on best practice;
5.3.2.5. To facilitate increased data sharing across the Public Service in line with legal and statutory obligations to enable the delivery of integrated services and improve the decision making processes;
5.3.2.6. To establish a secure GRN Private Cloud; and

5.3.2.7. To consult with Telecom Namibia and ensure that;

i. Existing infrastructures are used at mutually agreed upon cost;
ii. Data and information transfer is secure; and
iii. Networks are based on accepted international standards and practices.

5.3.3. Strategies

OPM – DPSITM shall:

5.3.3.1. Adopt an Interoperability Framework for the Public Service that addresses the information, business process and technical dimensions of interoperability;
5.3.3.2. Set standards specifications for networks, hardware, business applications and software platforms based on open standards;
5.3.3.3. Research and review new technological advances and recommend technologies to be used in the Public Service;
5.3.3.4. Establish and host a GRN Private Cloud;
5.3.3.5. Develop and adopt an Enterprise Architecture together with operational procedures and guidelines for the Public Service;
5.3.3.6. Develop guidelines and operational procedures to be adopted by O/M/As and RCs for development of IT infrastructures and deployment of enterprise resource planning systems;
5.3.3.7. Conduct audit and compliance assessments to verify conformance of business applications and information systems in O/M/As and RCs to open standards; and
5.3.3.8. Establish a GRN Wide Area Network in partnership with Telecom Namibia to connect all O/M/As and RCs to ensure secure access to GRN services.

O/M/As and RCs:

5.3.3.9. Deploy and support hardware, business applications and software platforms based on standard specifications developed for the Public Service;
5.3.3.10. Ensure that the acquisition or development of business applications is based on a formal business case approved by the Permanent Secretary of the line O/M/A and DPSITM. Business requirements must be defined and documented prior to the acquisition or development of any business application;
5.3.3.11. Make use of existing business applications and systems where possible;
5.3.3.12. Ensure that internal and outsourced software development complies with all relevant information security management and software development policies, procedures and standards;
5.3.3.13. Engage Telecom Namibia for the development and establishment of IT networks; and
5.3.3.14. Exchange data through the Governmental Interoperability Framework when possible.

5.4. MODULE IV - IT HUMAN RESOURCE MANAGEMENT AND DEVELOPMENT

5.4.1. Introduction

IT enabled services can only be effectively delivered if the IT personnel responsible for managing and supporting such IT Services are equipped with the prerequisite skills and competencies to effectively manage and support IT Services. Delivery of IT-enabled services requires a wide range of skills from support services and infrastructure management, project management, information security management, systems architecture and software development.

It is thus imperative that IT personnel in the Public Service are assessed in collaboration with Human Resources Development (HRD) to identify skills gaps and the relevant trainings and certifications to address the skills gaps.

Thus a collaborative framework for on-going capacity and skills development of IT Human Resources in O/M/As and RCs need to be developed.

5.4.2. Objectives

5.4.2.1. To ensure that GRN has qualified and competent IT Human Resources at all times;

5.4.2.2. To establish procedures for consolidation and sharing of IT Human Resources with specific attention to specialised skills and support for regional and remote offices to relieve the burden of additional budget allocations for creation of additional positions; and

5.4.2.3. To ensure that IT personnel have clearly defined roles and responsibilities aligned to international best practice on IT Service Management.

5.4.3. Strategies

OPM–DPSITM shall:

5.4.3.1. Collaborate with the Institutions of higher learning to develop IT degree and diploma courses relevant to the needs of the Public Service;

5.4.3.2. Establish a system of providing access to Internationally Accredited and recognised training courses that will enable IT professionals in the Public Service to improve and gradually attain various levels of competence in the work environment;

5.4.3.3. Develop guidelines and procedures to be adopted by O/M/As and RCs for the establishment and staffing of IT Units;

5.4.3.4. Conduct IT Skills Audit and establish IT Skills requirements for IT Personnel in the Public Service;

5.4.3.5. Facilitate trainings on specialised IT domains such as Information Security Management, Website and Application Development; and

5.4.3.6. Define strategies for collaboration of IT support resources, with specific attention to regional and remote offices to relieve the burden of additional budget allocations for creation of additional positions.

O/M/As and RCs shall:

5.4.3.7. Establish IT Units/Divisions based on adopted guidelines and procedures;

5.4.3.8. Create a dedicated budget vote for training and skills development of IT Personnel; and

5.4.3.9. Ensure that training and retention is carried out in line with the Human Resources Development Policy.

5.5. MODULE V - INFORMATION SECURITY MANAGEMENT

5.5.1. Introduction

Information Security Management (ISM) refers to the identification of security risks, and the implementation of a set of policies and procedures for systematically managing an organization's sensitive data. The goal of ISM is to minimize risk and ensure business continuity by pro-actively limiting the impact of a security breach.

ISM should be an integral part of IT Service Management within O/MA/s and RCs to ensure:

- **Confidentiality:** The propriety right that information is not made available or disclosed to unauthorized individuals, entities, or processes.
- **Integrity:** The propriety right of safeguarding the accuracy and completeness of information assets.
- **Availability:** The propriety right of information being accessible and usable upon demand by an authorized entity.

To effectively manage information security, a set of Policies shall be developed by the DPSITM in collaboration with Stakeholders, and shall be adopted with Procedures and Processes to be implemented across all O/M/As and RCs.

5.5.2. Objectives

5.5.2.1. To ensure compliance with all applicable statutory and regulatory requirements pertaining to confidentiality, integrity and availability of data and information; and

5.5.2.2. To ensure on-going inter-governmental collaboration, advisory and consultation on Cyber Security and mitigation strategies to stakeholders within GRN.

5.5.3. Strategies

OPM – DPSITM shall:

5.5.3.1. Develop a comprehensive Information Technology Security Policy and Acceptable Use of GRN IT Resources Policy for the Public Service based on international best practice to be implemented in support of this policy;

5.5.3.2. Develop skills and competencies in Information Security Management across all O/M/As and RCs; and

5.5.3.3. Establish an inter-governmental platform for collaboration and exchange of information on Information Security related matters.

O/M/As and RCs shall:

5.5.3.4. Implement the Information Technology Security Policy and the Acceptable Use Policy of GRN IT Resources Policy for the Public Service;

5.5.3.5. Ensure that employees, suppliers and contractors comply to Security Policies; and

5.5.3.6. Create awareness amongst staff members on Information Security with specific attention to Cyber Security.

5.6. MODULE VI - ACQUISITION OF IT GOODS AND SERVICES

5.6.1. Introduction

This section deals with the acquisition of computer hardware, software and services, including contract services (consultancies), by the different O/M/As and RCs. It includes, among others, the three different types of acquisitions that O/M/As and RCs can make.

- Hardware: complete systems and peripherals.
- Software: application packages, systems utilities, software and applications development.
- Services: hardware support and maintenance, desktop support and maintenance, software support and maintenance, facility management, data capturing services, consultancy services and other support services.

Acquisition is one of the financial risk factors in any organisation, if not effectively controlled. Thus, DPSITM is mandated with the effective control of IT expenditure within Public Service.

It is also in the interest of the government as a global organisation to prevent silos (own needs) and to rather focus on collaboration through sharing of information and infrastructure. This can only be achieved by ensuring that procurement processes are aligned to IT Policies.

To effectively manage procurement of IT Goods and Services, a process-based approach aligned to the Public Procurement Act shall be adopted.

5.6.2. Objectives

5.6.2.1. To ensure that all O/M/As and RCs strictly acquire hardware, software and services as set out in the IT Acquisition Instruction Manual;

5.6.2.2. To ensure that software and hardware acquired conforms to the policy of the government on open systems;

5.6.2.3. To ensure that hardware acquired conforms to international best practice on green technology;
5.6.2.4. To ensure that prices for IT goods and services are properly bench-marked to avoid GRN being over-priced; and
5.6.2.5. To ensure that all contract agreements for services are standardised and scrutinised by the Office of the Attorney General, and effectively managed.

5.6.3. Strategies

OPM –DPSITM shall:

5.6.3.1. Develop an IT Acquisition Instruction Manual aligned to the Public Procurement Act;
5.6.3.2. Develop standard specifications for acquisition of IT Goods and Services for the Public Service that conforms to international best practice on green technology and open standards;
5.6.3.3. Adopt standard Service Level Agreements and Contracts for IT Goods and Services for the Public Service in collaboration with the Office of the Attorney General; and
5.6.3.4. Conduct audit and compliance assessments to ensure that IT Goods and Services are procured in-line with the Public Procurement Act.

O/M/As and RCs shall:

5.6.3.5. Procure IT Goods and Services as per the IT Acquisition Instruction Manual;
5.6.3.6. Create a dedicated budget vote for the acquisition of IT Goods and Services; and
5.6.3.7. Ensure that Service Level Agreements and Contracts on IT Goods and Services are in place and effectively managed.

5.7. MODULE VII - IT ASSET MANAGEMENT

5.7.1. Introduction

An IT Service Asset is classified as any GRN-owned or licensed software, information system, business application, network or hardware that is used in the delivery and support of business activities. IT Service Asset and Configuration Management provides an accurate record of technology assets, their relationships and lifecycle costs.

The IT Service Asset Management process typically involves gathering, documenting and recording of a detailed inventory of an organization's hardware and software and then using that information to make informed decisions about IT-related consolidation, procurement, redistribution and support.

To effectively manage all GRN IT Assets, a process-based approach to IT Service Asset Management through utilisation of tool sets shall be adopted.

5.7.2. Objectives

5.7.2.1. To provide an overall framework for the management of IT Assets in the Public Service from acquisition to disposal.

5.7.3. Strategies

OPM – DPSITM shall:

5.7.3.1. Develop and adopt a formal IT Service Asset Management Process with operational procedures and guidelines for the Public Service;
5.7.3.2. Develop procedures for safe disposal and replacement of IT equipment's for the Public Service based on national and international best practice policies;
5.7.3.3. Coordinate and oversee the implementation of IT Service Asset Management in the Public Service;

5.7.3.4. Deploy and maintain a central, shared IT Service Asset Management application/ information management system to be used by O/M/As and RCs to record and maintain their IT Assets; and

5.7.3.5. Conduct audit and compliance assessments to ensure that IT Service Asset Management is implemented in the Public Service.

O/M/As and RCs shall:

5.7.3.6. Implement a formal IT Service Asset Management process;

5.7.3.7. Implement a formal replacement cycle for computer hardware;

5.7.3.8. Ensure that the roles and responsibilities for IT Service Asset Management are assigned to appropriate staff;

5.7.3.9. Maintain an up to date IT Service Asset Register on the shared IT Service Asset Management application/ information management system; and

5.7.3.10. Dispose of redundant IT Service Assets in accordance with Treasury Instructions.

6. IMPLEMENTATION ARRANGEMENTS /FRAMEWORKS

This section outlines the different frameworks and arrangements for the implementation of this policy. This includes the administrative and institutional structures, legal and regulatory arrangements as well as Monitoring and Evaluation plan.

6.1. Institutional Arrangements

The Institutional Arrangement for the implementation of this Revised IT Policy for the Public Service 2017 is described in Module I (Institutional Arrangements) of this policy.

6.2. Legal and Regulatory Arrangements

This Revised IT Policy for the Public Service 2017 has been aligned to the following National Policies and International Standard Organisation' standards:

- Overarching Information Communications Technology (ICT) Policy for the Republic of Namibia 2009
- ISO 27001 and 27002 on Information Security Management
- ISO 20000, the standard upon which IT Service Management (ITSM) is defined
- ISO 31000 for Risk Management
- ISO 15504 Information Technology Process Assessment.

6.3. Resource Mobilisation

6.3.1. All O/M/As and RCs will be required to make annual budgetary provision for the implementation of this policy.

6.3.2. O/M/As will further have to ensure that all IT personnel involved in IT Service Management functions have acquired the necessary skills and competencies through training and capacity building, and skills transfer.

6.3.3. Where needed, specialist expertise will be sought and shared across all O/M/As.

7. MONITORING AND EVALUATION FRAMEWORK AND REPORTING:

The Monitoring and Evaluation, and Reporting will be achieved through the following:

i) Implementation of an IT Service Support Management Tool

The Office of the Prime Minister, through the Department Public Service IT Management has acquired and implemented an IT service support management tool to help O/M/As manage the consumption of IT services, the infrastructure that supports the IT services and the performance of the IT Support teams. The tool has already been setup in OPM and some O/M/As such as the Ministry of Finance, and will be rolled-out to the rest of the O/M/A/s. The tool makes provision for accurate recording/reporting based on the requirements of the O/M/As such as:

- Performance of IT Support Teams
- Audit and Compliance Requirements
- Customer or User Satisfaction Surveys

ii) Audit and Compliance Assessments

An Audit and Compliance Unit has been established within the Department Public Service IT Management in the Office of the Prime Minister. The Unit will regularly carryout audit and compliance assessments to the Revised IT Policy for the Public Service 2017 across all O/M/As and the findings will be reported to the Permanent Secretaries' Forum and Cabinet Committee on Public Service.

8. ADVOCACY AND DISSEMINATION (COMMUNICATION STRATEGY):

The policy will be discussed at the Public Service Committee on IT (PSCOIT) meetings and thereafter published on the e-Service website. Presentations will also be made to each O/M/A and RC so that all aspects are clearly explained.

In addition a secure repository will be created for access by those who are authorised to do so, that will contain all relevant procedural documentation pertaining this policy.

9. IMPLEMENTATION ACTION PLAN:

TASK	RESPONSIBLE ORGANIZATION	Y1 (April 2017-March 2018)	Y2 (April 2018-March 2019)	Y3 (April 2019-March 2020)	Y4 (April 2020-March 2021)	Y5 (April 2021-March 2022)
Develop Operational Procedures, Guidelines for the implementation of the Revised IT Policy for the Public Service 2017	OPM: DPSITM					
Train and Certify Internal IT Audit Team within DPSITM						
Create Awareness on the Revised IT Policy for the Public Service 2017 in O/M/As and RCs	OPM: DPSITM					
Review current IT Structures of O/M/As	OPM, O/M/As and RCs					

and RCs and align roles to IT Service Management Framework						
Train and certify IT Staff in O/M/As and RCs to the required levels of competency to perform IT Service Management roles	OPM, O/M/As and RCs					
Implement relevant IT Service Management Processes in O/M/As and RCs	OPM, O/M/As and RCs					
Carryout Audit and Compliance Assessments in O/M/As and RCs	OPM:DPSITM					

10. POLICY REVIEW

The policy will be reviewed every five (5) years.

11. CONCLUSION

Information Technology (IT) plays a critical role in delivering and transforming the operations of government and has also become fundamental to how the government operates. Shifts in technology together with shifts in people's expectations for online Government services require new approaches to Information Technology (IT) in the Public Service to operate in a more integrated and effective manner.

Building on the successful delivery of many existing services, the Revised IT Policy for the Public Service 2017 sets out how we can operate in a more efficient, shared and integrated manner across all of Government while delivering new and innovative online services to citizens and businesses.

The potential for improvements through the innovative use of technology is significant. Implementation will require a transformational programme of change, not just technological but administrative and cultural.

When implemented, this Revised IT Policy for the Public Service 2017 will create a new model for IT delivery across the Public Service; delivering more efficiency and effectiveness in service delivery through a more integrated and shared environment.