DCSR POLICY: IT SERVICE MANAGEMENT POLICY

DOCUMENT INFORMATION AND LOG

Document name	**IT Service Management Policy**
Version	**1.0**
Approval Date	**March 2025**
Review date	**2027/2028**

INFORMATION TECHNOLOGY SERVICE MANAGEMENT POLICY

RELATED DOCUMENTS

Determination and Directive on the Implementation of the Public Service Corporate Governance of Information and Communication Technology Policy Framework version 2

DCSR Internet Policy;

DCSR Email Policy;

DCSR Acceptable Computer Use Policy;

DCSR User-Id and Password Policy;

Circular: Internet and Electronic Mail Abuse in Government;

SSA's Minimum Information Security Standards (MISS);

Web Content Filtering Procedure; and

MPG Email Standards.

CONTENTS

1. Policy Purpose 4
2. Information Technology Service Management Description 4
3. Scope 4
4. Definitions 4
5. Acronyms 5
6. Risks 5
7. Responsibility 5
8. Inputs and Outputs Policy Amendments 6
9. Publishing the User-ID and Password Policy 6
11. Policy Violations 6
12. ITSM Policy Statements 6
13. Enforcement 7
14. Review of the Policy 8
15. Policy Approved 8

1. Policy Purpose

The purpose of the ICT Service Management Policy is to set out the implementation and management of quality ICT services that meet the needs of the DCSR. This policy will serve as the functional commitment of ICT to the business of the DCSR.

2. Information Technology Service Management Description

IT Service Management (ITSM) can be described as how IT teams manage the end-to-end delivery of IT services to end users. This includes all the processes and activities to design, create, deliver, and support IT services.

3. Scope

The ITSM Policy will apply to all users of services, systems and applications provided by the DCSR.

4. Definitions

Hackers: Persons or entities that perform malicious activity using Information Technology systems. The hacker refers to an individual who gains unauthorised access to computer systems for the purpose of stealing and corrupting data.

ITSM: Information Technology Service Management represents the activities that are performed by an organisation to design, build, deliver, operate and control information technology (IT) services offered to end users.

IT Security: Refers to techniques for ensuring that data stored on a workstation or server cannot be read or compromised. Most security measures involve data encryption and passwords.

Password: A secret series of characters that enables a user to access a file, computer, or program. Each workstation user must enter his or her password before the computer will respond to commands. The password helps to ensure that unauthorized users do not access the computer. In addition, data files and programs may require a password.

Transversal System: PERSAL, BAS or LOGIS
User-ID: A User-ID is a unique identification of workstation users. The User-ID is used to gain access to Information Technology services, systems and applications. User-IDs are also used to audit workstation user's activities.

5. Acronyms

MPG:	Mpumalanga Provincial Government;
HOD:	Head of Department;
ICT:	Information Communication Technology;
IT:	Information Technology;
OGITO:	Office of the Government IT Officer;
GITO	Government Information Technology Officer; and
ITSM:	Information Technology Service Management

6. Risks

The risks attached to the DCSR ITSM include the following:

- Implementation

  There are some risks associated with IT service management. One of the biggest risks is that it can be difficult to implement and manage. Additionally, if not properly implemented, IT service management can lead to increased costs and decreased employee productivity.

- End User satisfaction

  Another risk is that IT support staff may not have the necessary skills to properly manage the services being delivered. This can result in poor service quality and customer satisfaction.

- Expensive

  ITSM can also be expensive, which can impact an organization's bottom line. As a result, it is important to carefully consider the risks associated with ITSM before implementing it.

- Complex and time-consuming,

  ITSM can be complex and time consuming and lead to higher expectations than can be delivered by the IT unit which can lead to delays in service delivery.

7. Responsibility

The Director-General as Accounting Officer for the DCSR: Mpumalanga will be responsible for the Department's overall ITSM Policy. OGITO will assist sections to make all users aware of this policy. The DCSR Information Technology's infrastructure and policies will be jointly managed and controlled by the DCSR and the Mpumalanga Department of Finance Information Technology Bureau.

8. Inputs and Outputs Policy Amendments

Any ITSM policy changes will be discussed between the DCSR and the Mpumalanga Department of Finance IT Bureau. The policy outputs and changes will be added to the policy document for review. The ITSM policy outputs will be consulted upon and agreed to between the DCSR and the Mpumalanga Department of Finance Information Technology Bureau.

All IT Policies must be submitted to the ICT Steering Committee for consideration and recommendation before being submitted for approval to the Director-General.

9. Publishing the User-ID and Password Policy

The User ID and Password Policy shall be made available and accessible to all employees through awareness sessions, websites and hard copy manuals.

10. Monitoring and Evaluation

It is important that the policy is monitored so as to prevent the unlawful use and access to the DCSR Information Technology infrastructure and systems.

11. Policy Violations

Violations of policies governing the use of the DCSR ITSM Policy may result in restriction of access to information technology resources. In addition, disciplinary action, up to and including dismissal, may be applicable under other policies, guidelines, implementing procedures, or collective bargaining agreements.

12. ITSM Policy Statements

Implementation

- The DCSR will ensure that business required systems are designed around the principles of confidentiality, integrity and availability of information.
- The DCSR will co-ordinate all IT activities in full transparency with other parties involved during the planning, design, transition, delivery and improvement of services.

Management

- The DCSR: Mpumalanga will establish, implement, maintain and continually improve Information Technology Management Systems.

- The DCSR will provide the human, technical, information and financial resources necessary to implement and operate the ITSM.

- The DCSR will implement and maintain appropriate systems and procedures to prevent activities or actions that pose a threat to the security of information and data, including information held and managed on behalf of and/or by staff, contractors and suppliers.

- The DCSR will ensure that information systems are monitored and managed to ensure the safety of information and data.

Meeting the Business Needs

- All IT Decision-making shall take into consideration the risks, requests from line units, benefits, feasibility and financial impact.

- The DCSR will ensure risks are identified and evaluated, eliminated or controlled.

- The DCSR will ensure that a detailed business case is drawn up for every IT project and system, required by units.

Functional Commitment

- The DCSR will provide the human, technical, information and financial resources necessary to implement and operate the ITSM.

- The DCSR shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the ITSM and operation of services.

- The DCSR will co-ordinate all IT activities in full transparency with other parties involved during the planning, design, transition, delivery and improvement of services.

13. Enforcement

Any transgression of this policy shall be handled in accordance with Human Resource Disciplinary Procedures.

14. Review of the Policy

This Policy shall be reviewed every three (3) years as a minimum or whenever the need for a policy review arises.

15. Policy Approved

MR EM MAHLANGU
(A) HEAD: CULTURE, SPORT AND RECREATION
DATE 07/11/2025