DCSR POLICY: CLOUD COMPUTING

DOCUMENT INFORMATION AND LOG

DOCUMENT NAME	CLOUD COMPUTING POLICY
VERSION	1.0
APPROVAL DATE	MARCH 2025
REVIEW DATE	2027/2028

RELATED DOCUMENTS

Determination and Directive on the Usage of Cloud Computing Services in the Public Service;
Memorandum of Understanding between the Culture, Sport and Recreation and the Provincial Treasury.
Electronic Communications and Transactions Act (ECT Act) 2002
The Financial Intelligence Centre Act (38 of 2001) (the FIC Act)
POPI Act no 4 of 2013
Culture, Sport and Recreation Internet Policy;
Culture, Sport and Recreation Email Policy;
Culture, Sport and Recreation Acceptable Computer Use Policy;
Culture, Sport and Recreation 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.

TABLE OF CONTENTS

Contents

1. Policy Purpose

The purpose of the Cloud Computing Policy is to give direction to the Culture, Sport and Recreation: Mpumalanga on considerations that must be made before procuring cloud services and to use the considerations outlined in this policy as guidance in considering existing cloud computing needs.

2. Cloud Computing Description

Cloud computing is the delivery of computing resources, such as IT infrastructure or data center over the internet. Cloud Computing allows institutions such as government departments to rent storage space or access software programs from a cloud service provider, instead of building and maintaining their own IT infrastructure or data center and 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 Cloud Computing Policy will apply to all users of services, systems and applications provided by the the Culture, Sport and Recreation.

This policy applies to the cloud-based variants of:

- Infrastructure as a Service (IaaS),
- Platform as a Service (PaaS), and
- Software as a Service (SaaS).

The policy applies to public cloud, private cloud, and community cloud implementations as well as any hybrid of cloud solutions or cloud and non-cloud hybrid solutions.

The policy promotes the use of cloud computing in government and fosters a structural approach to cloud adoption as required in the Directive on the usage of Cloud Computing Services in the Public Service.

4. Acronyms and Definitions

DPSA:	Department of Public Service and Administration
CSP:	Cloud Service Provider
GITOC:	Government Information Technology Officer Council
IaaS:	Infrastructure as a Service
ICT:	Information and Communications Technology

ISACA:	Information Systems Audit and Control Association
ISO:	International Standards Organisation
ISO17799:	Information security management Standard
NIST:	The National Institute of Standards and Technology
PaaS:	Platform as a Service
POPI:	Protection of Personal Information Act, 2013
PSA:	Public Service Act, 1994
SaaS:	Software as a Service
SITA:	State Information Technology Agency

5. Risks

A comprehensive risk assessment in relation to network access, storage and maintenance of public sector information and records must be conducted.

During the evaluation of ICT delivery options, risk profile assessments are required for each option. A full understanding of the risks and opportunities associated with cloud-based solutions is critical.

The evaluation of cloud options will address all identified risks and take account of:

- Ministerial Directive on Cloud Computing
- Minimum Information Security Standards (MISS)
- National Cyber Security Policy Framework (NCPF) 2015
- ISO 31000 Risk management – Principles and guidelines
- ISO/IEC 27000 series.

The mitigation of risks should include, but is not limited to:

- data location and retrieval,
- legal and regulatory risk,
- information governance and management,
- business continuity, security,
- privacy and licensing
- business continuity and disaster recovery plans.

Depending upon the service type, business need and delivery model adopted, an understanding and mitigation of risks will be required, including, but not limited to:

- **Security** - Cloud service providers must meet all applicable South African legislative requirements relating to the security of information.
- **Licensing** - Existing software licensing models to be re-evaluated and adapted accordingly.
- **Business continuity** - business continuity and disaster recovery plans in place.
- **Data location and retrieval** – Data must be stored on a SITA approved government Cloud.
- **Legal and regulatory** – Currently few legal precedents and many untested areas.
- **Information governance and management** – Service providers must comply with all applicable South Africa information management frameworks.
- **Privacy** – Cloud service providers must meet all applicable South African legislative requirements relating to the privacy of information. POPI Act.

6. Responsibility

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

The Accounting Officer is responsible for ensuring that this policy and all Cloud Computing standards are satisfied before approving any required external Cloud Service.

It is also further required that compliance with the Cloud Computing Policy is regularly reviewed by the Culture, Sport and Recreation's Risk Committee.

7. Inputs and Outputs Policy Amendments

Any Cloud Computing Policy changes will be discussed between the Culture, Sport and Recreation and the Mpumalanga Department of Finance IT Bureau. The policy outputs and changes will be added to the policy document for review. The Cloud Computing Policy outputs will be consulted upon and agreed to between the Culture, Sport and Recreation 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.

8. Publishing of the Cloud Computing Policy

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

9. Monitoring and Evaluation

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

10. Policy Violations

Violations of policies governing the use of the Culture, Sport and Recreation Cloud Computing 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.

11. Cloud Computing Policy Statements

The goal of the Culture, Sport and Recreation is to reduce the cost of ICT by eliminating duplication and fragmentation and will lead by example in using cloud services to reduce costs, improve productivity and improve services that are suited to the user's requirements.
The Culture, Sport and Recreation is required to use cloud services for any new ICT services and when replacing any existing ICT services, whenever the cloud services:

- are fit for purpose;
- offer the best value for money; and
- provide sufficient risk management to information and ICT assets.

The decision on the appropriate ICT delivery model will be based on an assessment of the business case which must be completed BEFORE implementation. At a minimum the Business Case must include the following:

- Scope of the Cloud Services Required;
- The budget over the short, medium and Long term;

- A calculation of the Total Cost of Ownership over the medium and Long term;
- The Human resource skills required to support the cloud service;
- The infrastructure required to enable the proper operation of the cloud service (Broadband Connectivity);
- The intended Benefit for the Culture, Sport and Recreation;
- The detailed outcome of the Risk Assessment, a summary of the key risks and recommendations for mitigation;
- The Business Case must be approved by the Director-General before cloud services are consumed and must be regularly reviewed; and
- Value for money should and must be apparent.

The Culture, Sport and Recreation Cloud Computing Policy has as its aim:

- Reducing the Total Cost of Ownership in line with the SITA ICT House of Value by eliminating duplication of solutions and fragmentation and leveraging the efficiencies of on-demand ICT services;
- Increasing productivity and agility, and thus improving services;
- Promoting green ICT by reducing government data centres;
- Developing ICT skills sets required for the Fourth Industrial Revolution; and
- Agility in the deployment of solutions and services.

This Cloud Computing Policy is therefore based on the following principles:

- Cloud should be the first option before any on-premises investment is done. The option should be fit for the purpose.
- Total cost of ownership should be cost effective in the medium to long term.
- Consider software as a service (SaaS) as the first cloud-first strategic option.
- Utilise the Government Cloud developed and maintained by the State Information Technology Agency (SITA), and engage SITA on the process to accredit existing Cloud Service Providers (CSP).

- Plan for cloud computing as a strategic enabler, rather than as an outsourcing arrangement or technical platform.
- Evaluate the benefits of cloud by comparing the costs of cloud with the costs of other technology platform business solutions.
- An enterprise risk management perspective to manage the adoption and use of cloud must be used.
- Integrate the full extent of capabilities that cloud computing offers with internal resources to provide a comprehensive technical support and delivery solution.
- Manage accountabilities by defining internal and provider responsibilities.

COPIES OF BOTH THE APPROVED BUSINESS CASE AND THE RISK COMMITTEE DECISION ON THE RISK ASSESSMENT MUST BE SUBMITTED TO THE DPSA PRIOR TO THE ACQUISITION OF ANY CLOUD COMPUTING SOLUTION.

12. Review of the Policy

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

13. Policy Approved

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