



Cloud First Policy

2026



Issuance and Distribution

Issuing Authority:

General Directorate of Policies and Governance
Ministry of Transport, Communications and
Information Technology



Governance@mtcit.gov.om

Issue Date **2026**

Document Control

Version	0.3
Date	2026
Issuing Authority	Ministry of Transport, Communications and Information Technology

Version	0.4
Date	2026
Issuing Authority	Ministry of Transport, Communications and Information Technology

Distribution List All State Administrative Apparatus
units and the Private Sector

Contents

Definitions and Terminology	3
Introduction	5
Objectives	6
Scope of implementation	6
Policy Provisions	7
Administrative and Contractual Requirements	8
Processing and Hosting Data Outside the Sultanate of Oman	11
Policy Management	12
Policy Compliance	12
Relevant publications	13



Definitions and Terminology

Beneficiary Unit:

State Administrative Units or institutions that own classified or sensitive data and information.

Service Provider:

Any unit that provides cloud computing services or data center services, including both licensed and authorized providers of public telecommunications services.

Cloud Computing:

A set of letters, numbers, symbols, or images used in the analysis and development of AI systems to provide solutions and predictions related to economic, social, or technical aspects.

An on-demand computing model that provides a shared pool of configurable computing resources and electronic systems which can be rapidly provisioned and managed with minimal effort. These resources include, but are not limited to:

- Servers
- Operating Systems
- Networks
- Software
- Applications
- Storage Resources

The model enables self-service provisioning, scalability, flexibility, and efficient resource management.

Ministry:

Ministry of Transport, Communications and Information Technology (MTCIT).

Center:

Cyber Defense Center (CDC).

Authority:

Telecommunications Regulatory Authority (TRA).

Hybrid Cloud:

A cloud computing model that combines two or more computing environments such as a private cloud, public cloud, and on-premises data centers allowing them to operate together through seamless integration and secure connectivity mechanisms.

Software as a Service (SaaS):

A cloud service model in which ready-to-use software applications are delivered to consumers over a cloud infrastructure that is owned and managed by the service provider.

Platform as a Service (PaaS):

A cloud service model that provides consumers with a ready-to-use platform for developing, testing, deploying, and managing applications on a cloud infrastructure operated by the service provider.

Infrastructure as a Service (IaaS):

A cloud service model that provides consumers with processing power, storage, networking, and other fundamental computing resources, enabling them to deploy and operate operating systems, applications, and other software.

PCI DSS Standard:

The Payment Card Industry Data Security Standard (PCI DSS) is an internationally recognized framework of security controls and administrative procedures designed to protect payment card data during processing, transmission, storage, purchasing, collection, and payment transactions.

Introduction

The Government of the Sultanate of Oman adopts a Cloud First approach due to its positive economic impact on fostering the digital economy, improving the efficiency of technology resource management, promoting innovation, developing national capabilities, and creating an enabling environment for the growth of the local digital market.

In alignment with Oman Vision 2040 and its digital transformation objectives, cloud computing serves as a fundamental platform for enabling emerging digital technologies such as Artificial Intelligence (AI) and the Internet of Things (IoT). It also supports the development of smart services, efficient data analytics, and evidence-based strategic decision-making while providing scalable, flexible, and resilient technology infrastructure and platforms.



Objectives

This policy aims to achieve the following objectives:

- 2.1 Adopt cloud computing as the primary hosting option for government information technology projects.
- 2.2 Improve operational efficiency and optimize government expenditure through flexible and centralized technology infrastructure.
- 2.3 Strengthen national digital sovereignty and ensure the protection of government data in accordance with applicable Omani laws and regulations.
- 2.4 Promote the adoption of cloud computing services in line with the latest technological developments to support digital transformation initiatives and ensure the availability of the necessary technological capabilities.

Scope of implementation

This Policy apply to all administrative Government Units from the issuance date, and exception is made to the security and military .units in the Sultanate

Policy Provisions

State Administrative Units shall adopt cloud computing as the preferred strategic and technical option when developing, upgrading, or procuring government information systems, applications, and digital services.

Government Units shall contract only with Cloud Computing Service Providers holding a valid authorization issued by the Telecommunications Regulatory Authority (TRA) in accordance with the Cloud Computing Services and Data Centers Regulation.

Furthermore, government units shall coordinate with the Ministry of Transport, Communications and Information Technology (MTCIT) before establishing new government data centers or expanding existing ones to ensure alignment with:

- National Digital Transformation priorities.
- The objectives of the National Program for Digital Economy and
- Government technology infrastructure strategies.

4.1 Administrative and Contractual Requirements

These controls are intended to regulate the administrative and contractual aspects associated with the use of cloud computing services by State Administrative Units, ensuring effective governance, safeguarding government interests, and enhancing the efficient management of resources.

Government units shall comply with the following requirements:

4.1.1 Data Classification

Government data shall be classified before being hosted on cloud computing services in accordance with the Data Classification Policy issued under the National Data Governance and Management Framework.

4.1.2 Selection of Service Providers

Government units shall contract only with cloud computing service providers and data center providers holding a valid (Category Four) authorization issued by the Telecommunications Regulatory Authority (TRA) in accordance with the Cloud Computing Services and Data Centers Regulation.

Whereas, a government unit intends to host classified data under categories other than those permitted by the applicable regulation, prior approval shall be obtained from the Ministry of Transport, Communications and Information Technology (MTCIT).

4.1.3 Service Level Agreement (SLA)

All contractual requirements shall be documented in a comprehensive Service Level Agreement (SLA).

The SLA shall include, at a minimum, key operational requirements such as:

- Service Availability
- Reliability
- Scalability
- Business Continuity

This is to ensure the protection of the rights and interests of the government unit.

4.1.4 Cybersecurity Incident Management

The government unit and the cloud service provider shall clearly define their respective roles and responsibilities regarding the management and response to cybersecurity incidents within the contractual agreement and the Service Level Agreement (SLA), ensuring clear accountability and obligations for each party.

4.1.5 Capacity Building

Government units shall ensure that Information Technology personnel receive appropriate training in cloud computing technologies to enable them to efficiently manage, operate, and administer cloud-hosted services and applications.

4.2 Security Requirements

These controls are intended to establish information security requirements governing the use of cloud computing services by State Administrative Units, ensuring the protection of government data, strengthening cybersecurity, and reducing risks associated with cloud computing services.

Accordingly, government units shall comply with the following security controls when utilizing cloud computing services in accordance with the Cloud Computing Services and Data Centers Regulation.

4.2.1 Risk Management

Government units shall conduct periodic Cloud Computing Risk Assessments at intervals determined by the unit, with reference to the Cloud Computing Governance Framework issued by the Ministry of Transport, Communications and Information Technology.

4.2.2 Compliance with Laws and Regulations

Government units shall comply with all applicable legislation, laws, and regulations in the Sultanate of Oman, as well as all information security policies and standards issued by:

- Ministry of Transport, Communications and Information Technology (MTCIT)
- Cyber Defense Center (CDC)
- Telecommunications Regulatory Authority (TRA)

4.2.3 Data Encryption

Government data and information hosted, processed, transmitted, or exchanged through cloud computing environments shall be encrypted in accordance with approved security requirements.

4.2.4 Provider Security Compliance

Government units shall ensure that cloud service providers comply with all applicable information security requirements, cybersecurity incident management procedures, and security best practices as prescribed by the Cloud Computing Services and Data Centers Regulation issued by the Telecommunications Regulatory Authority.

4.2.5 Compliance with the PCI DSS Standard

Government units shall ensure compliance with the Payment Card Industry Data Security Standard (PCI DSS) for all systems that process, store, or transmit electronic payment card data.

4.2.6 Security Audit Reports and Incident Logs

Government units shall require cloud service providers, through contractual agreements, to provide access to:

- Information security audit reports;
- Cybersecurity assessment reports; and
- Security incident logs and related records,

to enable the government unit to verify compliance with applicable security requirements and contractual obligations.



5. Processing and Hosting Data Outside the Sultanate of Oman

Where a government unit intends to host, process, or operate government data or applications outside the Sultanate of Oman, it shall comply with the following requirements:

5.1 Software as a Service (SaaS)

The requested cloud service shall be provided under the Software as a Service (SaaS) model, whereby the entire platform is hosted within a trusted cloud environment.

5.2 Compliance with External Cloud Computing Policy

Government units shall comply with the Policy and Controls for the Use of External Cloud Computing Services issued by the Cyber Defense Center (CDC) under Circular No. 6/2025, ensuring full compliance with the approved security and regulatory requirements of the Sultanate of Oman.

5.3 Prior Approval

Prior approval shall be obtained from the Cyber Defense Center (CDC) before hosting or processing government data or applications outside the Sultanate of Oman.



6. Policy Management

1. This policy is owned by the Ministry of Transport, Communications and Information Technology and will be subject to revision whenever necessary.
2. This policy shall be implemented by the date of its approval and circulation by the Ministry of Transport Communications and Information Technology.

Policy Compliance

The Ministry of Transport, Communications and Information Technology shall monitor the compliance of the units and present the results of compliance to the Council of Ministers.

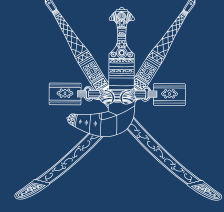


Related Documents

- ➡ Personal Data Protection Law (2022)
- ➡ Executive Regulation of the Personal Data Protection Law (2024)
- ➡ National Artificial Intelligence and Advanced Digital Technologies Program (2024)
- ➡ Personal Data Protection Policy for State Administrative Units (2024)
- ➡ Information Technology Risk Management Framework (2014)
- ➡ Cybercrime Law (2011)
- ➡ National Records Law (Royal Decree No. 52/2024)
- ➡ National Data Governance Framework (2025)

وزارة النقل والاتصالات وتقنية المعلومات

Ministry of Transport, Communications
and Information Technology



mtcit.gov.om

