وزارة النقل والاتصالات
وتقنية المعلومات

IT Risk Management Policy

February 2026

ص.ب: ٣٣٨ روي/ الرمز البريدي: ١١٢ الهاتف:٢٤٦٨٥٥٥٧/٢٤٦٨٥٥٥٢ فاكس: ٢٤٦٨٥٠٥٠ البريد الالكتروني: mtcit_d@mtcit.gov.om

Issuance and Distribution:

Issuing Authority	E-mail	Issue Date
General Directorate of Policies and Governance Ministry of Transport, Communications and Information Technology	Governance@mtcit.gov.om	٢٠٢٦

Document Control:

Version	Date	Issuing Authority	Comments
0.1	٢٠٢٦	Ministry of Transport, Communications and Information Technology	

Distribution List	
١	All State Administrative Apparatus units

ص.ب: ٣٣٨ روي/ الرمز البريدي: ١١٢ الهاتف:٢٤٦٨٥٥٥٧/٢٤٦٨٥٥٥٣ فاكس: ٢٤٦٨٥٠٥٠ البريد الالكتروني: mtcit_d@mtcit.gov.om

Contents:

ص.ب: ٣٣٨ روي/ الرمز البريدي: ١١٢ الهاتف:٢٤٦٨٥٥٥٧/٢٤٦٨٥٥٥٢ فاكس: ٢٤٦٨٥٠٥٠ البريد الالكتروني: mtcit_d@mtcit.gov.om

Introduction:

In alignment with the directions of the Ministry of Transport, Communications, and Information Technology to strengthen digital assets and enhance the efficiency of digital services, and considering the increasing reliance on information technology across the units of the State's administrative apparatus, the need has arisen to establish a policy governing the management of information technology risks.

This policy aims to provide a unified approach to risk management and to clearly define roles and responsibilities, ensuring the preparedness of government units and their contractors to manage potential technological risks. The policy also supports the enhancement of digital security and contributes to the effective and reliable advancement of digital transformation initiatives.

Objectives:

- To protect government digital assets from current and emerging technological threats.
- To assess and manage information technology risks effectively, ensuring business continuity and the stable delivery of digital services at the highest levels of security.
- To enhance the ability of government units to make strategic decisions based on risk assessment and analysis.
- To ensure alignment with the national emergency management framework in the Sultanate, as well as with relevant policies, regulations, and legislation.

ص.ب: ٣٣٨ روي/ الرمز البريدي: ١١٣ الهاتف:٢٤٦٨٥٥٥٧/٢٤٦٨٥٥٥٢ فاكس: ٢٤٦٨٥٠٥٠ البريد الالكتروني: mtcit_d@mtcit.gov.om

Purpose:

To define the core responsibilities of government units and their contractors in managing information technology risks, including the identification, assessment, treatment, and monitoring of risks in a systematic manner, in order to ensure effective risk management, protect digital assets, and maintain continuity of services.

Scope of Implementation

1. **State Administrative Units:** All units within the State's administrative apparatus.
2. **Third Parties:** External information technology service providers and contractors engaged by government units.

Policy Statements

1. General Statements

Government administrative units must:

1. Integrate risk management as an integral part of the unit's information technology strategy.
2. Develop and approve a comprehensive internal policy for managing the risks of IT systems and projects, in compliance with national laws and regulations, including the Personal Data Protection Law and other relevant cybersecurity legislation.
3. Designate a team responsible for managing information technology risks within the unit's organizational structure.
4. Identify and classify IT assets according to their sensitivity and importance, to ensure their protection and effective management.
5. Conduct periodic assessments of information technology risks and maintain a documented register including their sources, impacts, and mitigation measures.
6. Develop and implement risk treatment plans, including incident response plans and business continuity plans, in accordance with the approved risk priorities.

ص.ب: ٣٣٨ روي/ الرمز البريدي: ١١٢ الهاتف:٢٤٦٨٥٥٥٧/٢٤٦٨٥٥٥٢ فاكس: ٢٤٦٨٥٠٥٠ البريد الالكتروني: mtcit_d@mtcit.gov.om

7. Establish and implement specific procedures to manage risks associated with critical and sensitive systems, enhancing protection and minimizing the likelihood of disruption to vital services.
8. Periodically monitor the effectiveness of the risk management policy and improve it based on assessment results, incidents, and technological or organizational changes.
9. Establish a clear mechanism for escalating high-priority risks to senior management or relevant authorities, ensuring timely decisions based on an accurate assessment of potential impact.

2.Controls for External IT Service Providers and Contractors:

Government units are committed to incorporating information technology risk management controls into contracts and agreements with external IT service providers and contractors throughout the project lifecycle from engagement to delivery or service termination according to the following:

1. Fully comply with all relevant national laws, including the Personal Data Protection Law issued under Royal Decree No. (6/2022), and all legislation governing the information technology and cybersecurity sector.
2. Adhere to the information technology risk management policy approved by the unit when signing contracts.
3. Conduct a comprehensive risk assessment for any system or service to be provided before implementation, including critical and sensitive systems within the unit.
4. share the results of risk assessments with the unit and obtain approval before actual operation of the service or system.
5. Apply appropriate technical controls to address identified risks, such as encryption, access control, backup, and network segregation, and update these controls based on risk assessment results or unit requirements.
6. Provide the unit with periodic reports including the overall security status, any detected technical or security incidents, and any cases of non-compliance with the policy or contractual terms, if applicable.

ص.ب: ٣٣٨ روي/ الرمز البريدي: ١١٢ الهاتف:٢٤٦٨٥٥٥٧/٢٤٦٨٥٥٥٢ فاكس: ٢٤٦٨٥٠٥٠ البريد الالكتروني: mtcit_d@mtcit.gov.om

7. Immediately and formally notify the unit of any security or technical incident that could impact government systems or data.
8. Fully cooperate with the government unit in any audit related to information technology risk management, including granting unit representatives' access to relevant documents, records, and technical systems upon request for verification or assessment purposes.

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

1. 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

- ISO/IEC 27001:2022
- ISO/IEC 27005:2018
- ISO 22301:2019
- ISO 31000:2018
- NIST SP 800-30 Rev.1 (2012)
- NIST SP 800-37 Rev.2 (2018)
- COBIT 2019 Framework

ص.ب: ٣٣٨ روي/ الرمز البريدي: ١١٢ الهاتف:٢٤٦٨٥٥٥٧/٢٤٦٨٥٥٥٢ فاكس: ٢٤٦٨٥٠٥٠ البريد الالكتروني: mtcit_d@mtcit.gov.om