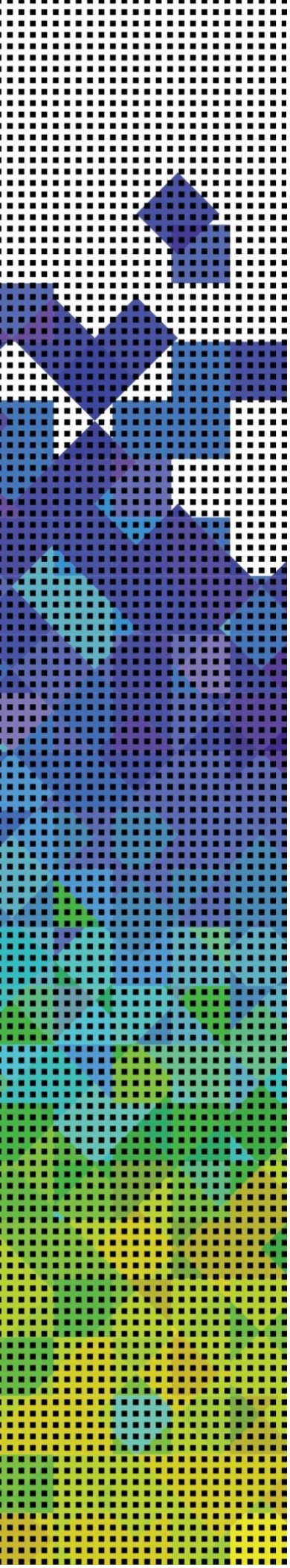

عمان الرقمية
e.oman

سلطنة عُمان
وزارة التقنية والاتصالات
Sultanate of Oman
Ministry of Technology and Communications

ICT Services Continuity Policy

April 2020

Contents

1. Purpose

The purpose of this policy is to define the overall governance for the ICT services continuity within the government administrative units to ensure the continuity of the services during disruptive events.

2. Scope

This policy applies to all ICT services that support critical business functions of government administrative units.

3. Definitions

- **MTC:** Ministry of Technology and Communications.
- **ICT:** Information and Communications Technology
- **ICT Services**: All systems supporting interactions, information provision, information storage, or communications provision and the ICT Facilities to communicate both internally and externally.
- **ICT Continuity:** Capability of the government administrative units to plan for and respond to disruptive event to continue ICT services at an acceptable predefined level.
- **ICT Service Continuity Plan (ICTSCP)**: a framework outlines how an organisation, applications, services, or technical components can be managed and recovered from disruptive event.

- **Disruptive event:** An event that threatens to disrupt critical business functions.

4. Policy Statements

The following statements apply:

1. Government administrative units are required to develop and implement, in consultation with MTC, appropriate ICT Service Continuity Plan (ICTSCP).
2. ICTSCP shall be developed and reviewed based on business impact analysis and risk assessment of government administrative units.
3. ICTSCP shall comply with official policies, frameworks, mandates and standards issued and circulated by MTC.
4. The ICT departments/divisions of government administrative units shall be prepared for and responsible for the management and recovery of ICT services in case of a disruptive event.
5. Government administrative units shall define the recovery resources that are required to support ICT service continuity in case of a disruptive event.
6. ICTSCP roles, responsibilities, competencies and authorities are required to be defined and documented.
7. ICTSCP are required to be reviewed regularly with the business function at planned periods and when significant changes occur.
8. ICT divisions/departments of government administrative units shall manage and oversee the implementation of this policy.

5. Ownership & Review

- This policy is issued by Ministry of Technology and Communications (MTC).
- Ownership of this Policy is vested with MTC and it will be reviewed annually or when required.

6. Policy Compliance

- MTC conducts policy compliance audits and report findings to the Cabinet.
- Any exception to this policy shall be approved by MTC

7. Related Guidance

- Royal Decree 118/2011 'Data Classification Law
    - 42/2015- Data Classification Law amendment
    - 26/2019- Data Classification Law amendment
- "IT Governance Policy" by Information Technology Authority (ITA)[1]
- "IT Governance Charter" by Information Technology Authority (ITA)
- "Information Security Management Framework" by ITA.
- "IT Service Continuity Framework" by ITA.
- "IT Risk management framework" by ITA.
- "Data and Information Systems Security Classification Mapping" by ITA.
- ITA circular number: 3-2015 "General Information Security Policy".

[1] ITA (Information Technology Authority): Currently MTC (Ministry of Technology and Communications)

- ITA circular number: 1-2017 “Security assessment of application & e-Services”.
- Oman e-Governance & Architectural Framework (OeGAF), ITA