

تعميم رقم (٥ / ٢٠٢٠)
حول سياسة استمرارية خدمات التقنية والاتصالات
وسياسة التواصل عن بعد لموارد وبيئة التقنية والاتصالات

من خلال سعي وزارة التقنية والاتصالات لتنفيذ استراتيجية عمان الرقمية، ودعمًا لوحدات الجهاز الإداري للدولة في التعامل مع الحالات غير الاعتيادية والأحداث الطارئة، فقد أعدت الوزارة سياستي استمرارية خدمات التقنية والاتصالات، والتواصل عن بعد لموارد وبيئة التقنية والاتصالات وذلك للعمل والتقيّد بهما ضمن إجراءات وخطط العمل الحكومية.

ومرفق طي هذا التعميم السياستين باللغة العربية والإنجليزية. راجين من جميع وحدات الجهاز الإدارية للدولة التقيّد بكافة البنود الواردة في السياستين.

ولمزيد من المعلومات يرجى التواصل مع المختصين في هذه الوزارة من خلال البريد الإلكتروني standard@mtc.gov.om أو على الهواتف (٢٤٦٦٦٦١٣ - ٢٤٦٦٦٤٣٢ - ٢٤٦٦٦٦٢١).

وتفضلوا بقبول فائق الاحترام،،

المهندسة/ عزة بنت سليمان الإسماعيلية
وزيرة التقنية والاتصالات

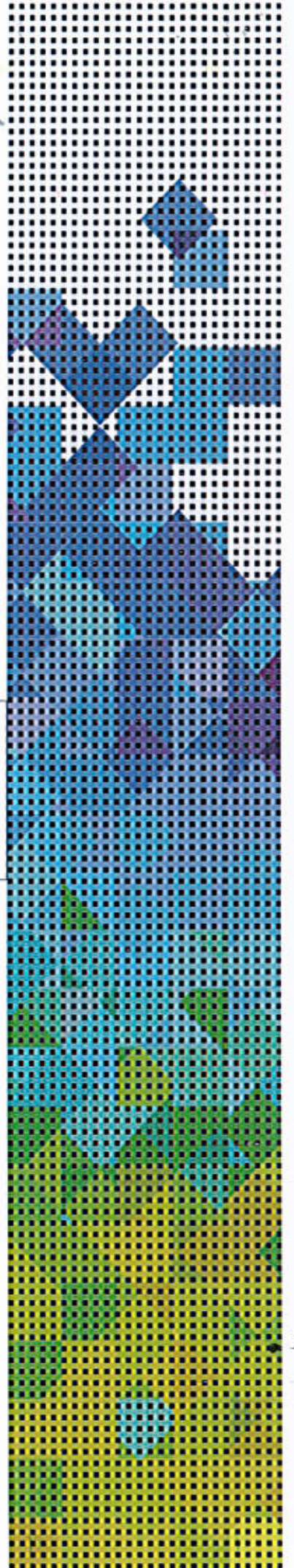


صدر في: ٦ رمضان ١٤٤١ هـ
الموافق: ٣٠ أبريل ٢٠٢٠ م



سياسة الوصول عن بعد لموارد بيئة التقنية والاتصالات

أبريل ٢٠٢٠م





المحتويات

١	الهدف	٣
٢	نطاق التطبيق	٣
٣	التعاريف والمصطلحات	٣
٤	بنود السياسة	٤
٥	الملكية والمراجعة	٥
٦	الالتزام بالسياسة	٥
٧	إصدارات ذات صلة	٥

سياسة الاتصال عن بعد لموارد وبينة تقنية المعلومات والاتصالات	النسخة الأولى	ابريل ٢٠٢٠	رقم الصفحة 2
---	---------------	------------	-----------------

١ الهدف

الهدف من هذه السياسة هو تنظيم الحوكمة العامة لإعداد واستخدام خاصية الوصول عن بعد لاداء مهام العمل عبر موارد وبيئة التقنية والاتصالات في وحدات الجهاز الإداري بالدولة.

٢ نطاق التطبيق

تنطبق هذه السياسة على جميع وحدات الجهاز الإداري بالدولة التي توفر خاصية الوصول عن بُعد لموارد وبيئة التقنية والاتصالات لاداء مهام العمل .

٣ التعاريف والمصطلحات

الوصول عن بعد لموارد وبيئة التقنية والاتصالات: أي شكل من أشكال الاتصال بأنظمة وشبكات العمل التقنية ومواردها من خارج بيئة العمل الاعتيادية.

بيئة التقنية والاتصالات: مجموعة الانظمة والحلول التقنية المستخدمة لإدارة أعمال وحدات الجهاز الاداري بالدولة. ويمكن تصنيف بيئة التقنية والاتصالات على أنها نطاقات عمليات أو إنتاج أو اختبارات.

موارد التقنية والاتصالات: تشمل الأجهزة (أجهزة الشبكة، أجهزة الحماية والخوادم) والبرمجيات (الأنظمة والتطبيقات) المستخدمة من قبل وحدات الجهاز الاداري بالدولة.

أدوات التقنية والاتصالات: الأجهزة أو المعدات (سواء المملوكة للوحدة الحكومية أو الشخصية) المستخدمة للوصول عن بعد وتتضمن أجهزة الحوسبة المكتبية (أجهزة سطح المكتب) والحوسبة المحمولة (أجهزة الحاسوب المحمولة، الهواتف المحمولة والاجهزة اللوحية).

المستخدمين : موظفي وحدات الجهاز الاداري بالدولة والأطراف ذات العلاقة من مقاولين وموردين متعاقد معهم وغيرهم من المخول لهم باستخدام خاصية الوصول عن بعد.

سياسة الاتصال عن بعد لموارد وبيئة تقنية المعلومات والاتصالات	النسخة الأولى	ابريل ٢٠٢٠	رقم الصفحة 3
--	---------------	------------	-----------------

٤ بنود السياسة

لتنظيم خاصية الوصول عن بعد لموارد وبيئة التقنية والاتصالات في وحدات الجهاز الإداري بالدولة، تطبق البنود التالية:

١. تطبيق الحلول التقنية المناسبة لتفعيل خاصية الوصول عن بعد لموارد وبيئة التقنية والاتصالات، بالتشاور مع وزارة التقنية والاتصالات.
٢. الالتزام بإعداد إجراءات وإرشادات طلب الوصول عن بعد لموارد وبيئة التقنية والاتصالات واستخدامها، بالتشاور مع وزارة التقنية والاتصالات.
٣. الالتزام بتحديد المستخدمين المخول لهم باستخدام خاصية الوصول عن بعد مع بيان أدوارهم ومسؤولياتهم وتحديد بيئة وموارد التقنية والاتصالات التي تنطبق عليها هذه الخاصية.
٤. الالتزام بتوفير الحد الأدنى من متطلبات الوصول عن بعد من موارد وأدوات التقنية والاتصالات بما في ذلك الاتصال بشبكة المعلومات العالمية للمستخدمين بعد أن تخضع لتقييم أمني.
٥. التأكد أن أدوات التقنية والاتصالات المستخدمة في الإتصال عن بعد تدعم أجهزة الحوسبة المكتبية والمحمولة ويجب أن تخضع للمعايير الأمنية الصادرة من وزارة التقنية والاتصالات.
٦. الالتزام بأمن المعلومات وسرية وخصوصية البيانات عند تفعيل خاصية الوصول عن بعد بما يتوافق مع السياسات والمعايير والإرشادات الصادرة عن وزارة التقنية والاتصالات والوحدات الحكومية ذات العلاقة الأخرى.
٧. الالتزام بجاهزية وإعداد أقسام/ دوائر/ قطاعات التقنية والاتصالات لتكون مسؤولة بشكل مركزي عن إدارة ودعم خاصية الوصول عن بعد.
٨. الالتزام برصد وتسجيل جميع أنشطة الوصول عن بعد إلى موارد التقنية والاتصالات وبيئاتها.
٩. يتولى قسم / دائرة أمن المعلومات الإشراف على تنفيذ هذه السياسة.

رقم الصفحة	٢٠٢٠ ابريل	النسخة الأولى	سياسة الاتصال عن بعد لموارد وبيئة تقنية المعلومات والاتصالات
4			

٥ الملكية والمراجعة

- هذه السياسة صادرة عن وزارة التقنية والاتصالات.
- تعود ملكية هذه السياسة إلى وزارة التقنية والاتصالات وستُراجع سنوياً أو عندما تقتضي الحاجة.

٦ الالتزام بالسياسة

- تتولى وزارة التقنية والاتصالات مراقبة الالتزام بالسياسة وعرض نتائج التقيد والالتزام لمجلس الوزراء.
- يتعين موافقة وزارة التقنية والاتصالات عند أي استثناء لهذه السياسة.

٧ إصدارات ذات صلة

- المرسوم السلطاني رقم ٢٠١١/١١٨ "قانون تصنيف البيانات"
- ٢٠١٥/٤٢ تعديل قانون تصنيف البيانات
- ٢٠١٩/٢٦ تعديل قانون تصنيف البيانات
- سياسة حوكمة تقنية المعلومات الصادرة عن هيئة تقنية المعلومات (سابقاً).
- إطار عمل حوكمة تقنية المعلومات الصادر عن هيئة تقنية المعلومات (سابقاً).
- إطار عمل إدارة أمن المعلومات الصادر عن هيئة تقنية المعلومات (سابقاً).
- إطار عمل استمرارية خدمات تقنية المعلومات الصادر عن هيئة تقنية المعلومات (سابقاً).
- إطار عمل إدارة مخاطر تقنية المعلومات الصادر عن هيئة تقنية المعلومات (سابقاً).
- دليل إرشادات تصنيف البيانات ونظم أمن المعلومات الصادر عن هيئة تقنية المعلومات (سابقاً).
- تعميم رقم ٢٠١٥/٣ السياسة العامة لأمن المعلومات
- تعميم رقم ٢٠١٧/١ التقييم الأمني للتطبيقات والخدمات الإلكترونية.

رقم الصفحة	٢٠٢٠ ابريل	النسخة الأولى	سياسة الاتصال عن بعد لموارد وبينة تقنية المعلومات والاتصالات
5			



سياسة استمرارية خدمات التقنية والاتصالات

أبريل ٢٠٢٠ م



جدول المحتويات

١	الهدف	٣
٢	نطاق التطبيق	٣
٣	التعاريف والمصطلحات	٣
٤	بنود السياسة	٤
٥	الملكية والمراجعة	٤
٦	الالتزام بالسياسة	٥
٧	إصدارات ذات صلة	٥

سياسة استمرارية خدمات تقنية المعلومات والاتصالات	النسخة الأولى	ابريل ٢٠٢٠	رقم الصفحة 2
---	---------------	------------	-----------------

١ الهدف

الهدف من هذه السياسة هو تنظيم الحوكمة العامة لاستمرارية خدمات التقنية والاتصالات في وحدات الجهاز الإداري بالدولة لضمان استمرارية الخدمات خلال الحالات غير الاعتيادية والاحداث الطارئة.

٢ نطاق التطبيق

تنطبق هذه السياسة على جميع خدمات التقنية والاتصالات المشغلة والداعمة للخدمات الأساسية في وحدات الجهاز الإداري بالدولة.

٣ التعاريف والمصطلحات

خدمات التقنية والاتصالات: جميع الأنظمة التي تشغل وتدعم معالجة وتدفق وتوفير المعلومات أو تخزينها أو توفير الاتصال وتسهيلات التقنية والاتصالات للتواصل داخليًا وخارجيًا.

استمرارية خدمات التقنية والاتصالات: قدرة وحدات الجهاز الإداري بالدولة على التخطيط والاستجابة للحالات غير الاعتيادية والاحداث الطارئة لاستمرار خدمات التقنية والاتصالات عند مستوى مقبول محدد مسبقًا.

خطة استمرارية خدمات التقنية والاتصالات: إطار تنظيمي يحدد كيف يمكن إدارة واستعادة الوحدات الحكومية للتطبيقات أو الخدمات أو المكونات التقنية عند الحالات غير الاعتيادية والاحداث الطارئة.

الاحداث الطارئة: حدث متوقع / غير متوقع يهدد بتعطيل خدمات التقنية والاتصالات بوحدات الجهاز الاداري للدولة .

سياسة استمرارية خدمات تقنية المعلومات والاتصالات	النسخة الأولى	ابريل ٢٠٢٠	رقم الصفحة 3
--	---------------	------------	-----------------



٤ بنود السياسة

لتنظيم إستمرارية خدمات التقنية والاتصالات في وحدات الجهاز الإداري بالدولة ، تطبق البنود التالية :

١. إعداد وتنفيذ خطة لاستمرارية خدمات التقنية والاتصالات بما يتوافق مع هذه السياسة وبالتشاور مع وزارة التقنية والاتصالات .
٢. يراعى عند اعداد ومراجعة الخطة إجراء تحليل تأثر الأعمال وتقييم المخاطر .
٣. الالتزام عند اعداد خطة استمرارية خدمات التقنية والاتصالات بالسياسات والمعايير والأطر التي تصدرها وزارة التقنية والاتصالات.
٤. الالتزام بجاهزية وإعداد اقسام/ دوائر/ قطاعات التقنية والاتصالات لإدارة واستعادة خدمات التقنية والاتصالات في الحالات غير الاعتيادية والاحداث الطارئة.
٥. الالتزام بتحديد وتوفير موارد الاسترداد المطلوبة لدعم واستعادة استمرارية خدمات التقنية والاتصالات أثناء الحالات غير الاعتيادية والاحداث الطارئة.
٦. الالتزام بتحديد وتوثيق الأدوار والمسؤوليات والاختصاصات ومستوى السلطة الادارية وإتخاذ القرارات ذات الصلة ضمن خطة استمرارية خدمات التقنية والاتصالات.
٧. الالتزام بمراجعة خطة استمرارية خدمات التقنية والاتصالات بصفة دورية في الفترات المخطط لها وعندما تقتضي الحاجة.
٨. تتولى اقسام/ دوائر/ قطاعات التقنية والاتصالات إدارة ومتابعة تنفيذ هذه السياسة.

٥ الملكية والمراجعة

- هذه السياسة صادرة من وزارة التقنية والاتصالات
- تعود ملكية هذه السياسة إلى وزارة التقنية والاتصالات وستُراجع سنويًا أو عندما تقتضي الحاجة.

رقم الصفحة	ابريل ٢٠٢٠	النسخة الأولى	سياسة استمرارية خدمات تقنية المعلومات والاتصالات
4			

٦ الالتزام بالسياسة

- تتولى وزارة التقنية والاتصالات مراقبة الالتزام بالسياسة وعرض نتائج التقيد والالتزام لمجلس الوزراء.
- يتعين موافقة وزارة التقنية والاتصالات عند أي استثناء لهذه السياسة.

٧ إصدارات ذات صلة

- المرسوم السلطاني رقم ٢٠١١/١١٨ قانون تصنيف البيانات
 - ٢٠١٥/٤٢ تعديل قانون تصنيف البيانات
 - ٢٠١٩/٢٦ تعديل قانون تصنيف البيانات
- سياسة حوكمة تقنية المعلومات الصادرة عن هيئة تقنية المعلومات
- قواعد حوكمة تقنية المعلومات الصادر عن هيئة تقنية المعلومات (سابقاً).
- إطار إدارة أمن المعلومات الصادر عن هيئة تقنية المعلومات (سابقاً).
- إطار عمل استمرارية خدمات تقنية المعلومات الصادر عن هيئة تقنية المعلومات (سابقاً).
- إطار إدارة مخاطر تقنية المعلومات الصادر عن هيئة تقنية المعلومات (سابقاً).
- دليل إرشادات تصنيف البيانات ونظم أمن المعلومات الصادر عن هيئة تقنية المعلومات (سابقاً).
- التعميم رقم ٢٠١٥/٣ السياسة العامة لأمن المعلومات
- التعميم رقم ٢٠١٧/١ الأمني للتطبيقات والخدمات الإلكترونية
- النموذج المرجعي لحوكمة تقنية المعلومات (OeGAF) الصادر من هيئة تقنية المعلومات (سابقاً).

رقم الصفحة	٢٠٢٠ إبريل	النسخة الأولى	سياسة استمرارية خدمات تقنية المعلومات والاتصالات
5			

ICT Remote Access Policy

April 2020



Contents

1. Purpose.....	3
2. Scope	3
3. Definitions.....	3
4. Policy statements.....	4
5. Ownership & Review.....	5
6. Policy Compliance	5
7. Related Guidance	5

1. Purpose

The purpose of this policy is to define the overall governance for the provision and use of remote access to ICT resources and ICT environment within government administrative units.

2. Scope

This policy applies to all government administrative units implementing remote access to ICT resources or ICT environment to perform work-related activities remotely.

3. Definitions

- **MTC:** Ministry of Technology and Communications.
- **ICT:** Information and Communications Technology
- **ICT Remote Access:** Any form of access to ICT environment and ICT resources from a remote distance.
- **ICT Environment:** The ICT technologies utilized to conduct government administrative units' business. ICT environment is categorized into testing, staging and production.
- **ICT Resources:** Include hardware (i.e. security appliance, network appliance, servers), Software (i.e. systems and application).
- **ICT Tools:** Desktop computing (desktop computer) and portable computing (i.e. laptops, mobile, tablets...etc.) devices which are unit owned or personally owned used for remote access.



- **Users:** All government units' employees, contractors and other affiliates (vendors, agents, etc.) who are eligible for remote access.

4. Policy statements

The following statements apply:

1. Government administrative units are required to implement, in consultation with MTC, appropriate ICT remote access technical solution.
2. Government administrative units are required to comply with MTC issued procedures and guidelines for requesting and using ICT remote access.
3. Government administrative units shall define users with their roles and responsibilities, ICT resources and ICT environment that are eligible for ICT remote access.
4. Government administrative units are required to provide the eligible users for remote access with the minimum required resources including ICT tools and internet connectivity.
5. All ICT tools used for remote access are required to support desktop and portable computing and must comply with MTC published security measures.
6. Government administrative units are required to ensure the protection of sensitive information, security and privacy in compliance with policies, standards and guidelines of MTC and other government units.



7. All ICT remote access shall be centrally managed and supported by ICT departments of government administrative units.
8. All ICT remote access shall comply with official policies, frameworks, mandates and standards issued and circulated by MTC.
9. All remote access activities to ICT resources and ICT environment shall be monitored and logged.
10. Information security division/department of government administrative units shall oversee the implementation of the 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 and 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”.
- ITA circular number: 1-2017 “Security assessment of application & e-Services”.
- ITA circular number: 6-2015 “Government Network Security Architecture Framework”.
- ITA circular number: 2-2016 “Government Application and E-Services Security Architecture Framework”.
- ITA circular number: 3-2017 “End Point and Smart Devices Security Architecture and Configuration Framework”.
- Oman e-Governance & Architectural Framework (OeGAF), ITA

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

ICT Services Continuity Policy

April 2020

Contents

1. Purpose.....	3
2. Scope	3
3. Definitions.....	3
4. Policy Statements	4
5. Ownership & Review.....	5
6. Policy Compliance	5
7. Related Guidance	5



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