الوثيقة الاستشارية

هذا المستند هو مسودة معدة لأغراض التشاور فقط. هذه ليست النسخة النهائية وهي قابلة للتغيير بناءً على الملاحظات الواردة خلال فترة التشاور.

سياسة الحد الأدنى المطلوب من سياسات تكنولوجيا المعلومات الداخلية للجهات الحكومية

التاريخ: مارس 2025 | النسخة: 1.0.0 | المرجع: P007

إخلاء المسؤولية / الحقوق القانونية

قامت وزارة الاتصالات وتكنولوجيا المعلومات بتصميم وإعداد هذا الإصدار بعنوان "سياسة الحد الأدنى المطلوب من سياسات تكنولوجيا المعلومات الداخلية للجهات الحكومية" وذلك وفق المرجع رقم P007 (المُشار إليه فيما يلي باسم "الوثيقة")، والذي يُعَدُّ في المقام الأول مرجعاً استرشادياً للجهات الحكومية، وكبار المسؤولين، والمعنيين بإدارة تكنولوجيا المعلومات، وإدارة المخاطر والمتخصصين في مجال أمن المعلومات في دولة قطر.

تم إعداد "الوثيقة" وفقاً لقوانين دولة قطر، ولا يجوز استخدامها لدعم أي حق نيابة عن أي شخص أو كيان ضد دولة قطر أو هيئاتها أو مسؤوليها. وإذا نشأ تعارض بين هذه الوثيقة وقوانين دولة قطر، تكون الأولوية لقوانين دولة قطر. تم بذل كافة الجهود الممكنة لإعداد هذه "الوثيقة" بشكل دقيق، إلا أنه لا يمكن تقديم أية ضمانات أو تعهد بشأن دقة "الوثيقة" أو اكتمالها أو حداثتها. وتمت إضافة روابط المواقع الإلكترونية الأخرى للاسترشاد فقط ولا تشكل ضماناً أو تعهداً بأن هذه المواقع لا تزال نشطة ومحدّثة، ولا يعتبر ذلك اعتمادًا للمواد التي تتضمنها هذه المواقع أو أية جهة أو منتج أو خدمة مرتبطة بها.

إن أيّة عملية نسخ لهذه "الوثيقة" سواء كان ذلك بشكل جزئي أو كلي، بغض النظر عن الأدوات التي تم استخدامها لذلك، تستوجب الإشارة إلى أنَّ وزارة الاتصالات وتكنولوجيا المعلومات هي مصدر ومالك محتوى "الوثيقة". ويجب الحصول على إذن كتابي مُسبق من وزارة الاتصالات وتكنولوجيا المعلومات في حال نسخ واستخدام محتوى الوثيقة بهدف التسويق التجاري. وتحتفظ الوزارة بالحق في تقييم وظائف وقابلية التطبيق لجميع النسخ المُعدة للأغراض التجارية. ولا يجوز تفسير الإذن الكتابي لوزارة الاتصالات وتكنولوجيا المعلومات على أنَّه مصادقة من قبلها للنسخ التي تم تطويرها ولا يجوز لمستخدم المحتوى إساءة تفسير ذلك أو نشره في أية وسيلة من وسائل الإعلام أو في النقاشات الشخصية / الاجتماعية.

دولة قطر

وزارة الاتصالات وتكنولوجيا المعلومات - قطاع شؤون الحكومة الرقمية

إدارة سياسات ومعايير الحكومة الرقمية

الموقع الإلكتروني: http://www.mcit.gov.qa

البريد الإلكتروني: policy@mcit.gov.qa

الاختصاص القانوني

تحدِّد المادةُ رقم 17[1] من القرار الأميري رقم 57 لسنة 2021 الاختصاص القانوني لوزارة الاتصالات وتكنولوجيا المعلومات (المُشار إليها فيما يلي باسم "الوزارة")، وتنصُّ على أن وزارةَ الاتصالات وتكنولوجيا المعلومات لديها صلاحية الإشراف على قطاع الاتصالات وتكنولوجيا المعلومات وتطويره في دولة قطر على نحوٍ يتسِّقُ ويتماشى مع الصلاحيات التالية، وهي ليست على سبيل الحصر:

- الإشراف على قطاع الاتصالات وتكنولوجيا المعلومات وتطويره تماشيًا مع متطلبات التنمية الوطنية.
- الإشراف على تأسيس بيئة تنظيمية مُناسبة لتحقيق المُنافسة العادلة.
- دعم قطاع الاتصالات وتكنولوجيا المعلومات، وتطويره، وتحفيزه، وتشجيع الاستثمار.
- تأمين وتطوير ورفع كفاءة البنية التحتية المعلوماتية والتكنولوجية.
- رفع مستوى الوعي حول أهمية الاتصالات وتكنولوجيا المعلومات لتحقيق التقدُّم للمجتمع، وبناء اقتصاد رقمي قائم على المعرفة، وتحسين حياة الفرد.
- تنفيذ برامج الحكومة[2] الإلكترونية والمجتمع الذكي والإشراف عليها
- تقوية البنية التحتية والقدرات الحكومية في مجال الاتصالات وتكنولوجيا المعلومات.

بالإضافة إلى ما سبق، يستند محتوى هذه السياسة إلى النصوص التالية:

- القرار الأميري رقم 47 لسنة 2022 بإنشاء إدارة سياسات ومعايير الحكومة الرقمية ومسؤولياتها التي تشمل على سبيل المثال لا الحصر تطوير السياسات والمبادئ التوجيهية والأطر الفنية لشؤون الحكومة الرقمية؛ اقتراح مشاريع الأدوات التشريعية ذات الصلة؛ وضع المعايير والمواصفات الفنية المتعلقة بالحكومة الرقمية؛ قياس مدى التزام الجهات الحكومية بالسياسات والمبادئ التوجيهية والأطر الفنية المتعلقة بشؤون الحكومة الرقمية.

[1] يمكن الوصول إلى كافة المصادر الخارجية من خلال قسم التشريعات والوثائق ذات الصلة.

[2] يمكن الاطلاع على المصطلحات التقنية ومعانيها في قسم مسرد المصطلحات والتعريفات.

التوافق الاستراتيجي

رؤية قطر الوطنية 2030		التنمية الاقتصادية	إن**شاء** بنى تحتية عالمية المستوى تتمتع بآليات فعالة لتقديم الخدمات ودعم المؤسسات العامة.
استراتيجية التنمية الوطنية الثالثة لدولة قطر 2024-2030		مؤسسات حكومية متميزة	بناء حوكمة فعالة وكفؤة وشفافة.
الأجندة الرقمية 2030		تكنولوجيا رقمية ثريها المعرفة	تعزيز البنية التنظيمية لقطاع تكنولوجيا المعلومات والاتصالات.

ملخص الوثيقة

الاسم	سياسة الحد الأدنى المطلوب من سياسات تكنولوجيا المعلومات الداخلية للجهات الحكومية
النسخة	1.0.0
مرجع الوثيقة	P007
نوع الوثيقة	سياسة
ملخص	تبيِّن هذه السياسة الحد الأدنى من سياسات تكنولوجيا المعلومات الداخلية التي يجب على جميع الجهات الحكومية وضعها واعتمادها. وهي تهدف في نهاية المطاف إلى الوصول إلى مستوى متماثل من نضج سياسات تكنولوجيا المعلومات على مستوى الجهات كافة، لتوفير نهج ثابت لتعزيز الممارسات الجيدة والحوكمة. ويجب على الجهات، حسبما تقتضي الضرورة، تحديث و/أو وضع سياسات داخلية جديدة لتكنولوجيا المعلومات لتلبية الحد الأدنى من المعايير المحددة في أحكام هذه السياسة وملاحقها.
تاريخ النشر	مارس 2025
تنطبق على	كافة الجهات الحكومية في دولة قطر.
فترة التطبيق	24 شهرًا من تاريخ نشر هذه السياسة
المالك	وزارة الاتصالات وتكنولوجيا المعلومات (الوزارة)

** في حال وجود أي استفسارات أو ملاحظات، يُرجى التواصل عبر البريد الإلكتروني التالي: policy@mcit.gov.qa.*

جدول المحتويات

قائمة الأشكال

1 مقدمة

يُعد تطبيق سياسات مُحكمة لتكنولوجيا المعلومات ركيزة أساسية لتعزيز تهيئة بيئة عنوانها الفعالية والأمان لتكنولوجيا المعلومات تسهم في نجاح الجهات الحكومية ووصولها إلى مرحلة النضج التام، فسياسات تكنولوجيا المعلومات الداخلية توفر نهجًا موحدًا لتطبيق أفضل الممارسات، وتلبية المتطلبات التنظيمية، وتنفيذ عمليات تكنولوجيا المعلومات بفعالية في مجالات من بينها، على سبيل المثال لا الحصر، الاتصالات والموارد ومستويات الخدمة والأمن والامتثال والمخاطر والجودة. وعلاوةً على ذلك، قد يثمر وضوح سياسات تكنولوجيا المعلومات الداخلية في رفع إنتاجية الموظفين من خلال توفير إرشادات سمتها الشفافية بشأن استخدام التكنولوجيا المقبول والحيلولة دون استغلال موارد تكنولوجيا المعلومات أو إساءة استخدامها.

أما نضج بيئة سياسات تكنولوجيا المعلومات الداخلية عبر مختلف الجهات الحكومية فيتباين تباينًا كبيرًا، إذ في الوقت الذي يحرز بعض هذه الجهات تفوقًا في الوفاء بالمتطلبات الأساسية ذات الصلة، يظل البعض الآخر بعيدًا عن مجرد تحديد احتياجات سياسات تكنولوجيا المعلومات الخاصة بها. وعلى الرغم من أن السياق والخدمات والاحتياجات الخاصة بكل جهة حكومية قد يشوبها الاختلاف، فهناك مجالات مشتركة لسياسة تكنولوجيا المعلومات يمكن تحديدها واستخدامها كخط أساس ينبغي وجوده لدى جميع الجهات الحكومية.

وتهدف هذه السياسة إلى تحقيق مستوى من الاتساق بين الجهات الحكومية من خلال تحفيز إنشاء واعتماد الحد الأدنى من سياسات تكنولوجيا المعلومات الداخلية بما يتماشى مع الأحكام الواردة في هذه الوثيقة.

1.1 الحد الأدنى من سياسات تكنولوجيا المعلومات الداخلية

بعد مراجعة شاملة لأفضل الممارسات والدول الرائدة والدول المجاورة، فإن سياسات تكنولوجيا المعلومات الداخلية الاثنتا عشرة الموضحة في *الشكل رقم 1* تشكِّل جزءًا أساسيًا من إطار الاستخدام الفعال والآمن والمتوافق لموارد التكنولوجيا. فهي تساعد في حماية الجهة وموظفيها والجهات المعنية لديها مع إنمائها، كما ترسي في الوقت نفسه دعائم متينة لثقافة الاستخدام المسؤول للتكنولوجيا.

الشكل رقم1- الحد الأدنى من سياسات تكنولوجيا المعلومات الداخلية

2 أهداف السياسة

تتمثل الأهداف الرئيسية لهذه السياسة فيما يلي:

2.1 الارتقاء بمستوى نضج بيئة سياسات تكنولوجيا المعلومات الداخلية وتعزيز تبني نهج موحد لتطبيق الممارسات الجيدة داخل كل جهة من الجهات الحكومية.

2.2 تحديد خط أساس للحد الأدنى من سياسات تكنولوجيا المعلومات الداخلية المطلوب وضعها أو تعديلها داخل كل جهة من الجهات الحكومية.

2.3 وضع الحد الأدنى من المتطلبات اللازمة لنطاق وتعريف وأهداف كل سياسة من السياسات الداخلية لتكنولوجيا المعلومات.

2.4 تهيئة بيئة أكثر اتساقًا وتناغمًا لسياسات تكنولوجيا المعلومات على مستوى كافة الجهات الحكومية، للمساعدة في تسهيل المبادرات التي يتم إطلاقها على مستوى كافة قطاعات الحكومة ودعم جهود التحول الرقمي المستقبلية.

3 نطاق السياسة وتطبيقها

3.1 تنطبق هذه السياسة على جميع الجهات الحكومية التي تستخدم تكنولوجيا المعلومات، أو تقدم خدمات تتضمن أنظمة تكنولوجيا المعلومات أو أجهزتها، وذلك على الصعيد الداخلي أو للاتصالات التي تتم عبر الإنترنت أو عبر شبكة داخلية (إنترانت) أو شبكات خاصة أو وجهًا لوجه أو عن طريق وسائل أخرى..

3.2 تسري هذه السياسة على أي عملية أو نظام أو كمبيوتر أو موقع إلكتروني أو برنامج أو تطبيق أو جهاز لتكنولوجيا المعلومات يتم استخدامه على الصعيد الداخلي، لأي غرض، بواسطة وداخل أي من الجهات الحكومية المشار إليها البند 3.1.

3.3 تُطبَّق هذه السياسة دون الإخلال بأي متطلبات أكثر صرامةً مما توجبه أي قوانين وسياسات أخرى معمول بها بالفعل، بما في ذلك، على سبيل المثال لا الحصر، أي قوانين وسياسات تخص حماية البيانات والأمن المادي والسيبراني والشؤون الرقمية والاتصالات، وأي قواعد وإجراءات داخلية أكثر صرامة مما تطبقه أي جهة من الجهات الحكومية المعنية، وذلك باستكمالها لذلك كله من خلال مجموعة من القواعد الدنيا المطلوبة.

4 بنود السياسة وأحكامها

تستلزم هذه السياسة من جميع الجهات الحكومية تطبيق الأحكام التالية:

4.1 سياسة الاستخدام المقبول

4.1.1 يجب على كل جهة إعداد سياسة للاستخدام المقبول يكون من شأنها تنظيم الاستخدام المناسب للكمبيوترات وأنظمة المعلومات الأخرى في سياق العمليات اليومية لهذه الجهة، ويتم في هذه السياسة تحديد ما يُشكل استخدامًا داخليًا غير مناسب لأنظمة المعلومات، كما أنها تسلط الضوء على المخاطر المحتملة لمثل هذا الاستخدام على أنظمة الشبكة الخاصة بالجهة وبياناتها، وغيرها من المعلومات والأصول والواجبات والوظائف، وكذلك على الدولة والأطراف الثالثة، فضلًا عن إبرازها للتداعيات القانونية الخطيرة المرتبطة بهذه المخاطر.

4.1.2 يجب أن تستوفي سياسة الاستخدام المقبول الخاصة بكل جهة الحد الأدنى من المتطلبات المنصوص عليها في الملحق 1.1.

4.2 سياسة المصادقة على النفاذ وتوثيقه

4.2.1 يجب على كل جهة إعداد سياسة للمصادقة على النفاذ وتوثيقه، على أن تتضمن هذه السياسة إطارًا أدنى يخص منح الموظفين والوكلاء والمتعهدين وحرمانهم من إمكانية النفاذ إلى ما لدى الجهة من أنظمة تكنولوجيا المعلومات وتطبيقاتها التي تولّد البيانات الحساسة بكافة أنواعها أو تعالجها أو تديرها أو تنقلها أو تحتفظ بها. وتلتزم كل جهة، لدى إعداد سياسة المصادقة على النفاذ وتوثيقه الخاصة بها، بالتأكد من صيانة هذه السياسة للبيانات السرية الخاصة بهذه الجهة وحمايتها ضد الانتهاكات أو الخروقات الناجمة عن إجراءات إدارة النفاذ والتوثيق غير السليمة، كما أن كل جهة تلتزم بجمع البيانات المطلوبة لمسارات التدقيق المرتبطة بالامتثال.

4.2.2 يجب أن تستوفي سياسة المصادقة على النفاذ وتوثيقه لدى كل جهة الحد الأدنى من المتطلبات المنصوص عليها في الملحق 1.2.

4.3 سياسة النسخ الاحتياطي للبيانات واستعادتها

4.3.1 يجب على كل جهة إعداد سياسة للنسخ الاحتياطي للبيانات واستعادتها، على أن تحدد هذه السياسة وتوضح الحد الأدنى مما ينبغي للجهة تنفيذه من إجراءات وعمليات النسخ الاحتياطي للبيانات، لضمان سلامة المعلومات في حالة فقدان البيانات الأصلية أو تلفها. ويجب أن تتوافق هذه السياسة مع أحكام معيار تأمين المعلومات الوطنية وسياسة تصنيف البيانات الوطنية فيما يخص إجراءات وعمليات النسخ الاحتياطي والاستعادة المحددة لكل فئة من فئات البيانات (مثل: البيانات الحساسة، والبيانات المقيدة، وما شابه ذلك.)

4.3.2 يجب أن تستوفي سياسة النسخ الاحتياطي للبيانات واستعادتها الخاصة بكل جهة الحد الأدنى من المتطلبات المنصوص عليها في الملحق 1.3.

4.4 سياسة تصنيف البيانات

4.4.1 يجب على كل جهة إعداد سياسة لتصنيف البيانات تتضمن التزامًا باتباع أسلوب تصنيف البيانات المحدد في سياسة تصنيف البيانات الوطنية، وتتوافق مع التشريعات القائمة في دولة قطر، مثل قانون حماية خصوصية البيانات الشخصية وقانون تنظيم الحق في الحصول على المعلومات، وكذلك السياسات والمعايير الوطنية الأخرى ذات الصلة.

4.4.2 يجب أن تستوفي سياسة تصنيف البيانات لدى كل جهة الحد الأدنى من المتطلبات المنصوص عليها في الملحق 1.4.

4.5 سياسة خصوصية البيانات

4.5.1 يجب على كل جهة إعداد سياسة لخصوصية البيانات تتوافق مع قواعد خصوصية البيانات المعمول بها في دولة قطر وتغطي الجوانب المختلفة لمعالجة البيانات داخل الجهة بما في ذلك، على سبيل المثال لا الحصر، جمعها وتعديلها وتخزينها واستخدامها وتبادلها وتأمينها، وإدراج حقوق بيانات المستخدمين في هذا السياق. يجب على كل جهة، عند إعداد سياسة خصوصية البيانات الخاصة بها، الرجوع إلى سياسة تصنيف البيانات الوطنية وقانون حماية خصوصية البيانات الشخصية، كما أن عليها أن تضع بعين الاعتبار متطلبات الخصوصية المحددة لكل فئة من فئات البيانات (مثل: البيانات الحساسة، والبيانات المقيدة، وما شابه ذلك.)

4.5.2 يجب أن تستوفي سياسة خصوصية البيانات لدى كل جهة الحد الأدنى من المتطلبات المنصوص عليها في الملحق 1.5.

4.6 سياسة البريد الإلكتروني

4.6.1 يجب على كل جهة إعداد سياسة بريد إلكتروني تغطي الجوانب الأمنية المتعلقة بإرسال رسائل البريد الإلكتروني داخليًا، أو داخل الجهة، أو إلى أطراف ثالثة. ويجب أن تتضمن هذه السياسة المبادئ التوجيهية الرسمية المتعلقة بالاستخدام السليم لما لدى الجهة من حسابات البريد الإلكتروني الرسمية، والمعلومات المتعلقة بممارسات الاستخدام المقبول للبريد الإلكتروني الشخصي وذلك أثناء استخدام حسابات البريد الإلكتروني الخاصة بالعمل.

4.6.2 يجب أن تستوفي سياسة البريد الإلكتروني لدى كل جهة الحد الأدنى من المتطلبات المنصوص عليها في الملحق 1.6.

4.7 سياسة إدارة أصول تكنولوجيا المعلومات

4.7.1 يجب على كل جهة إعداد سياسة لإدارة أصول تكنولوجيا المعلومات الخاصة بها، على أن تشمل هذه السياسة مجموعة متكاملة من المبادئ التوجيهية التي تتناول بدقة شديدة كل جانب من جوانب دورة حياة أصول تكنولوجيا المعلومات الخاصة بهذه الجهة، بدءًا من المراحل الأولية للاقتناء والتنفيذ وحتى المراحل المستمرة للاستخدام والصيانة، وكذلك، على نحو من الأهمية، مرحلة التخلص من الأصول في نهاية دورة حياتها أو في حالة تعرضها للسرقة أو التلف من قبل طرف ثالث قبل نهاية دورة حياتها.

4.7.2 يجب أن تستوفي سياسة إدارة أصول تكنولوجيا المعلومات لدى كل جهة الحد الأدنى من المتطلبات المنصوص عليها في الملحق 1.7.

4.8 سياسة إدارة التغيير في تكنولوجيا المعلومات

4.8.1 يجب على كل جهة إعداد سياسة لإدارة التغيير في تكنولوجيا المعلومات لتخطيط وتنفيذ الإغلاق المؤقت لأنظمة تكنولوجيا المعلومات بغرض الصيانة أو الترقيات أو التعديلات المخطط لها. ويجب أن تحدد هذه السياسة الحد الأدنى من المعايير الواجب اتباعها، مع التركيز على تقليل حالات التعطُّل إلى أدنى درجة ممكنة، وضمان سلاسة عمليات الانتقال، وتحسين كفاءة النظام وموثوقيته طوال عملية إدارة التغيير.

4.8.2 يجب أن تستوفي سياسة إدارة التغيير في تكنولوجيا المعلومات لدى كل جهة الحد الأدنى من المتطلبات المنصوص عليها في الملحق 1.8.

4.9 سياسة الاتصالات المحلية

4.9.1 يجب على كل جهة إعداد سياسة للاتصالات المحلية يكون من شأنها تحديد إجراءات تعامل موظفي الجهة مع الاتصالات الداخلية عبر ما لديها من أنظمة للشبكات وطرق تبادل المعلومات.

4.9.2 يجب أن تستوفي سياسة الاتصالات المحلية لدى كل جهة الحد الأدنى من المتطلبات المنصوص عليها في الملحق 1.9.

4.10 سياسة أمن الشبكات

4.10.1 يجب على كل جهة إعداد سياسة لأمن الشبكات تتضمن وتحدد عملية إجراء مراجعات دورية لأنظمة المعلومات وأنشطة الشبكات لضمان سرية البيانات وسلامتها وتوافرها، وذلك من خلال تزويد أنظمة تكنولوجيا المعلومات الخاصة بالجهة بالبرامج والأجهزة وإجراءات التدقيق المناسبة.

4.10.2 يجب أن تستوفي سياسة أمن الشبكات لدى كل جهة الحد الأدنى من المتطلبات المنصوص عليها في الملحق 1.10.

4.11 سياسة الأمن المادي والبيئي

4.11.1 يجب على كل جهة إعداد سياسة للأمن المادي والبيئي يكون من شأنها تحديد المبادئ التوجيهية والإجراءات اللازمة لاستخدام موظفيها لأجهزة تكنولوجيا المعلومات لضمان حماية المعلومات الخاصة بالجهة ومواردها ومبانيها من الضرر أو التلف أو الحذف. كما يجب أن تحدد هذه السياسة الحد الأدنى من متطلبات خطة حماية أصول تكنولوجيا المعلومات الخاصة بالجهة من خلال تطبيق الإجراءات المناسبة بشأن كيفية السماح بالنفاذ المادي إلى هذه الأصول أو تنظيمه أو مراقبته أو منعه.

4.11.2 يجب أن تستوفي سياسة الأمن المادي والبيئي لدى كل جهة الحد الأدنى من المتطلبات المنصوص عليها في الملحق 1.11.

4.12 سياسة النفاذ عن بُعد

4.12.1 يجب على كل جهة إعداد سياسة للنفاذ عن بُعد بهدف تقليل مخاطر أي ضرر ينتج عن الاستخدام غير المصرح به لموارد الجهة من خلال تحديد المبادئ التوجيهية التي تنظم النفاذ إلى موارد الشبكات الداخلية (الإنترانت) وتحديد المتطلبات الأساسية لتشفير الأقراص والنفاذ إلى الشبكة الافتراضية الخاصة (VPN).

4.12.2 يجب أن تستوفي سياسة النفاذ عن بُعد لدى كل جهة الحد الأدنى من المتطلبات المنصوص عليها في الملحق 1.12.

4.13 التقدُّم المحرَز في التنفيذ والمراجعة

مسؤوليات الجهة الحكومية

4.13.1 يجب على جميع الجهات الحكومية، في غضون [24] شهرًا من نشر هذه السياسة، وضع سياسات تكنولوجيا المعلومات الداخلية الاثنتي عشرة (12) التالية:

- سياسة الاستخدام المقبول
- سياسة المصادقة على النفاذ وتوثيقه
- سياسة النسخ الاحتياطي للبيانات واستعادتها
- سياسة تصنيف البيانات
- سياسة خصوصية البيانات
- سياسة البريد الإلكتروني
- سياسة إدارة أصول تكنولوجيا المعلومات
- سياسة إدارة التغيير في تكنولوجيا المعلومات
- سياسة الاتصالات المحلية
- سياسة أمن الشبكات
- سياسة الأمن المادي والبيئي
- سياسة النفاذ عن بُعد

4.13.2 يجب أن تستوفي كل سياسة من هذه السياسات، بحد أدنى، مجموعة المتطلبات الموضحة تحت العنوان ذي الصلة لتلك السياسة في الملحق 1

4.13.3 يجوز للجهات الحكومية، عند وضعها هذه السياسات في حيّز التنفيذ، الاختيار بين استحداثها من البداية (إذا لم يكن لديها سياسة مقابلة) أو تعديل ما لديها من السياسات القائمة المقابلة وذلك إلى الحد المطلوب لتحقيق الأهداف ذات الصلة في هذه السياسة والحد الأدنى من المتطلبات المنصوص عليها في هذه الوثيقة.

4.13.4 تتولى إدارة المراجعة الداخلية في كل جهة حكومية، أو أي قسم آخر ذي صلة تراه الجهة مناسبًا، مراقبة تنفيذ هذه السياسة والحد الأدنى المطلوب من سياسات تكنولوجيا المعلومات التي تحددها، ضمن نطاق الجهة ذات الصلة.

مسؤوليات وزارة الاتصالات وتكنولوجيا المعلومات

4.13.5 يجوز لوزارة الاتصالات وتكنولوجيا المعلومات إصدار الإجراءات والمبادئ التوجيهية وأفضل الممارسات الإضافية أو التكميلية من وقت لآخر لدعم واحدة أو أكثر من سياسات تكنولوجيا المعلومات الداخلية لدى الجهات الحكومية، كما يجوز لها توسيع نطاق هذه السياسات ليشمل جهات أخرى.

4.13.6 تتولى وزارة الاتصالات وتكنولوجيا المعلومات إجراء مراجعة سنوية لسياسات تكنولوجيا المعلومات هذه. وفي الحالات التي تستدعي إجراء تحديثات نتيجة حدوث تغييرات جوهرية على الصعيد التكنولوجي أو التنظيمي أو المؤسسي، يجوز لوزارة الاتصالات وتكنولوجيا المعلومات تحديث واحدة أو أكثر من سياسات تكنولوجيا المعلومات هذه قبل فترة المراجعة السنوية.

4.13.7 يجوز لوزارة الاتصالات وتكنولوجيا المعلومات في أي وقت أن تطلب معلومات و/أو تقريرًا تفصيليًا (راجِع 3) بشأن تبني هذه السياسة والحد الأدنى المطلوب من سياسات تكنولوجيا المعلومات التي تحددها، من إدارة المراجعة الداخلية بكل جهة حكومية، أو أي طرف آخر ذي صلة تراه الجهة مناسبًا (راجِع البند 4.13.4).

5 قائمة المصطلحات والتعريفات

المصطلح	التعريف
الجهة	يُقصد بها أي جهة حكومية بما في ذلك أي جهات خارجية تدعم الجهة الحكومية في تقديم الخدمات، ويتضح المعنى من خلال السياق المذكور.
البيانات	جميع البيانات والمعلومات الرقمية التي تقوم الجهات الحكومية بالحصول عليها أو استرداداها أو مشاركتها أو معالجتها بهدف تقديم الخدمات الإلكترونية للعامة والزوار والشركات.
الجهة الحكومية	يُقصد بها جميع الوزارات والمؤسسات العامة التابعة لها أو لمجلس الوزراء في دولة قطر، ما لم يرد نص صريح يُفيد بمعنى آخر.
البيانات الشخصية	تشير إلى بيانات فرد تم تحديد هويته أو يمكن تحديدها بشكل معقول، سواء من خلال هذه البيانات الشخصية أو من خلال دمج هذه البيانات مع أي بيانات أخرى.

6 التشريعات والوثائق ذات الصلة

يقدِّم الجدول التالي روابطَ إلكترونيةً لجميع الوثائق والأوراق ذات الصلة أو المُشار إليها في هذه السياسة. وتُبذلُ كلُ الجهود المُمكنة للتأكُّد من صحة هذه الروابط، ولكن قد تكون في بعض الأحيان بعض أو كامل موارد هذه الروابط غيرَ متوفرة نتيجة حذفها أو نقلها أو استبدالها.

التشريعات	القرار الأميري رقم (57) لسنة 2021 (المادة 17) القرار الأميري رقم (47) لسنة 2022 قانون رقم (13) لسنة 2016 بشأن حماية خصوصية البيانات الشخصية قانون رقم (9) لسنة 2022 بتنظيم الحق في الحصول على المعلومات
السياسات أو المعايير أو أطر العمل	سياسة تصنيف البيانات الوطنية (2023) معيار تأمين المعلومات الوطنية (2023) سياسة الحوسبة السحابية أولاً (2024)
الروابط الأخرى	رؤية قطر الوطنية (2030)

الملاحق

الملحق 1: الحد الأدنى من المتطلبات لكل سياسة

يوضح هذا الملحق الحد الأدنى من المتطلبات التي يجب على الجهات الحكومية استيفائها لكل سياسة داخلية لتكنولوجيا المعلومات تنص عليها هذه الوثيقة. يتم توفير النماذج الفردية لسياسات تكنولوجيا المعلومات الداخلية هذه في الملحق 2 وهي متاحة لاستخدام الجهة. يجوز للجهات الحكومية إما تطوير سياساتها الخاصة أو تعديل النماذج المقدمة عن طريق تكييف أو حذف أو إضافة أحكام لمعالجة التداخلات والفجوات والاحتياجات السياقية المحددة لضمان التوافق مع متطلباتها الخاصة.

1.1 سياسة الاستخدام المقبول - الحد الأدنى من المتطلبات

يجب على الجهات الحكومية استيفاء الحد الأدنى من المتطلبات التالية فيما يتعلق بسياسة الاستخدام المقبول لديها:

- تحديد الغرض من السياسة بوصفها سياسةً هدفها ما يلي:
  - حماية توافر موارد تكنولوجيا المعلومات التي تملكها الجهة أو تستخدمها وصيانة سرية هذه الموارد وسلامتها.
  - تشجيع الاستخدام الأخلاقي والمسؤول لهذه الموارد.
- تحديد نطاق الحالات التي تُطبق فيها السياسة، وكذلك، إلى أقصى حد ممكن (من خلال سياقة الأمثلة)، الحالات التي لا تُطبق فيها.
- تحديد معايير الاستخدام المقبول لأجهزة تكنولوجيا المعلومات لدى بالجهة، مثل:
  - الامتثال للقوانين واللوائح المعمول بها.
  - قَصْر استخدام موارد تكنولوجيا المعلومات ضمن نطاق العمل اليومي.
  - مراعاة خصوصية البيانات من خلال تجنب النفاذ غير المصرح به إلى الموارد.
- تحديد معايير الاستخدام غير المقبول لأجهزة تكنولوجيا المعلومات لدى الجهة، مثل:
  - انتهاك حقوق المستخدمين.
  - النسخ غير القانوني للمواد، الذي ينجم عنه قضايا متعلقة بحقوق النشر.
  - تزويد أطراف ثالثة غير مصرح لها بالمعلومات الحكومية.
- تحديد معايير استخدام موظفي الجهة أو وكلائها أو متعهديها لوسائل التواصل الاجتماعي بما في ذلك تضمين هؤلاء لأي إشارة إلى الجهة أو إلى دورهم الحالي أو السابق داخل الجهة أو فيما يتعلق بها.
- تحديد النتائج المترتبة على أي خرق لهذه السياسة، حسب مدى خطورته ومدته، مثل:
  - فرض الغرامات الإدارية أو غيرها من العقوبات.
  - إنهاء عقد الموظف.
  - اتخاذ الإجراءات القانونية ضد الموظف المعني.

- الإشارة إلى أي خدمات سحابية سيتم استخدامها أو قد يتم استخدامها ضمن نطاق فئات العمل المحددة.
- تقييد تثبيت واستخدام أي برنامج من شأنه أن يشكل انتهاكًا للوائح الحكومية أو القوانين الأخرى، مثل قوانين الملكية الفكرية.

1.2 سياسة المصادقة على النفاذ وتوثيقه - الحد الأدنى من المتطلبات

يجب أن تستوفي الجهات الحكومية الحد الأدنى من المتطلبات التالية فيما يتعلق بسياسة المصادقة على النفاذ وتوثيقه الخاصة بها:

- تحديد الغرض من هذه السياسة على أنه يتمثل في وضع إجراءات لحماية المعلومات ومنح الوصول إلى الحسابات السرية وكذلك إلى المعدات والبنية التحتية والخدمات والبرمجيات.
- تحديد نطاق هذه السياسة ليشمل جميع موظفي الجهة ووكلائها ومتعهديها الذين لديهم إمكانية الوصول إلى المعلومات الحكومية وأنظمة تكنولوجيا المعلومات الخاصة بالجهة.
- الاسترشاد بسياسة تصنيف البيانات الوطنية وضمان التوافق الكامل معها.
- وضع ضوابط الوصول من خلال تخصيصها بموجب "مبدأ الامتياز الأقل" ووفقًا لاحتياجات الجهة: لا يُمنح المستخدمون سوى الحد الأدنى من حقوق الوصول والتراخيص وكذلك الموارد اللازمة للأنظمة والخدمات والبيانات والمعلومات المطلوبة لهم بشكل صارم لتنفيذ الأدوار المكلفين بها.
- تضمين إجراءات لمراجعة وصول المستخدمين بشكل دوري بالتنسيق مع أصحاب الأعمال وفريق أمن المعلومات لتحديد الحسابات الزائدة عن الحاجة أو غير النشطة وحذفها، إن وجدت، من خلال تحديد فترة احتفاظ محددة لهذه الحسابات على النحو المنصوص عليه في قانون حماية خصوصية البيانات الشخصية في قطر.
- وضع إجراءات إدارة كلمة المرور على النحو التالي:
  - إلزام المستخدمين باختيار كلمات مرور معقدة وتحديد متطلبات التعقيد تلك من خلال توفير إرشادات قوية عند اختيار كلمة المرور (على سبيل المثال: استخدام كل من الأحرف الصغيرة والأحرف الكبيرة والأحرف الخاصة، وما إلى ذلك).
  - تحديد متطلبات طول كلمة المرور.
  - توعية المستخدمين بالعواقب المترتبة على اختيار كلمة مرور سهلة التوقع أو تضمين معلومات شخصية فيها (على سبيل المثال: استخدام كلمة مرور يسهل اختراقها والتعرض المحتمل لعمليات انتهاك البيانات).
  - تحديد تواتر إعادة تعيين كلمة المرور (على سبيل المثال: 90 يومًا).
  - الأخذ في الحسبان المصادقة متعددة العوامل أثناء إعداد حساب حكومي نيابةً عن الموظفين لإضافة مستوى إضافي من الأمان.

1.3 سياسة النسخ الاحتياطي للبيانات واستعادتها - الحد الأدنى من المتطلبات

يجب أن تستوفي الجهات الحكومية الحد الأدنى من المتطلبات التالية فيما يتعلق بسياسة النسخ الاحتياطي للبيانات واستعادتها الخاصة بها:

- تحديد الغرض من هذه السياسة على أنه يتمثل في ضمان إمكانية استرداد جميع بيانات ومعلومات الجهة في حالة حدوث أي ضرر أو حادث.
- تحديد نطاق السياسة ليشمل جميع موظفي الجهة والأطراف الثالثة التي تتعامل مع بيانات ومعلومات الجهة.
- الاسترشاد بسياسة تصنيف البيانات الوطنية والتأكد من التوافق الكامل معها.
- تحديد معايير النسخ الاحتياطي للبيانات لكل مستوى من مستويات البيانات المختلفة المذكورة في سياسة تصنيف البيانات الوطنية (على سبيل المثال: البيانات العامة والبيانات الداخلية والبيانات المقيدة والبيانات السرية والسرية للغاية).
- تحديد فترات الاحتفاظ بالبيانات للنسخ الاحتياطي (على سبيل المثال: يوميًا، أسبوعيًا، وما إلى ذلك).
- تحديد جدول زمني للنسخ الاحتياطي يشمل وتيرته والوقت المناسب خلال اليوم لإجرائه.
- تحديد إجراءات النسخ الاحتياطي بِحيادٍ تامٍ تجاه أي مورد من الموردين:
  - تحديد النسخ الاحتياطي اليدوي أو التلقائي والإجراءات المنطبقة عليه؛
  - تحديد النسخ الاحتياطي المركزي أو اللامركزي والإجراءات المنطبقة عليه.
- وضع خطة طوارئ لاتخاذ إجراءات في حالة فقدان البيانات.
- اختبار أنظمة النسخ الاحتياطي والاسترداد بانتظام لضمان فاعليتها.

1.4 سياسة تصنيف البيانات - الحد الأدنى من المتطلبات

يجب أن تستوفي الجهات الحكومية الحد الأدنى من المتطلبات التالية فيما يتعلق بسياسة تصنيف البيانات الخاصة بها:

- تحديد الغرض من هذه السياسة على أنه يتمثل في وضع نهج لتصنيف البيانات على مستوى الجهة بما يتوافق مع النهج المحدد في سياسة تصنيف البيانات الوطنية.
- تحديد نطاق السياسة ليشمل جميع البيانات التي تجمعها أو تمتلكها أو تستخدمها الجهة.
- ضمان التوافق مع التشريعات المعمول بها في دولة قطر، مثل قانون حماية خصوصية البيانات الشخصية وقانون تنظيم الحق في الوصول إلى المعلومات.
- تحديد الأدوار والمسؤوليات داخل الجهة بشأن تصنيف البيانات وكيفية حماية البيانات.
- وضع وصف مفصل لعملية تصنيف البيانات من خلال تحديد المسؤول في كل مرحلة، وكيفية تقييم حساسية البيانات، والإجراءات التي يجب اتخاذها في حال كانت البيانات لا تندرج ضمن فئة محددة مسبقًا.

1.5 سياسة خصوصية البيانات - الحد الأدنى من المتطلبات

يجب أن تستوفي الجهات الحكومية الحد الأدنى من المتطلبات التالية فيما يتعلق بسياسة خصوصية البيانات الخاصة بها:

- تحديد الغرض من هذه السياسة على أنه يتمثل في ترسيخ حقوق حماية البيانات لمختلف مستويات تصنيف البيانات داخل الجهة الحكومية.
- تحديد نطاق السياسة ليشمل جميع البيانات التي تتم معالجتها أو تخزينها أو تحديثها أو نقلها، وفقًا للوائح الخصوصية الخاصة بالوكالة الوطنية للأمن السيبراني و(بالنسبة للبيانات الشخصية) قانون حماية خصوصية البيانات الشخصية.
- الاسترشاد بمستويات تصنيف البيانات المحددة في سياسة تصنيف البيانات الوطنية (على سبيل المثال: البيانات العامة والبيانات الداخلية والبيانات المقيدة والبيانات السرية والبيانات السرية للغاية) وتعريفات كل منها.
- إنشاء آلية للتحكم في الوصول بناءً على الدور تحدد أدوار ومسؤوليات مالكي البيانات ومستخدميها.
- تحديد إجراءات الاحتفاظ بالبيانات لمالكي البيانات ومستخدميها.
- تحديد فئات البيانات التي سيتم تضمينها في مستويات التصنيف التالية: البيانات الداخلية والبيانات المقيدة والبيانات السرية والبيانات السرية للغاية.
- تحديد أي فئة من فئات البيانات الشخصية التي تملكها أو تعالجها الجهة قد تندرج تحت تصنيف البيانات ذات الطبيعة الخاصة أو تتضمن هذا النوع من البيانات بموجب المادة 16 من قانون حماية خصوصية البيانات الشخصية والإجراءات الخاصة التي تنطبق عليها.
- وضع قواعد لحماية البيانات الداخلية والبيانات المقيدة والبيانات السرية والبيانات السرية للغاية، وتحديد العواقب المترتبة على عدم الامتثال لهذه القواعد.
- تحديد معايير الإفصاح عن البيانات المتعلقة بالجهة الحكومية أو غيرها أو استخدامها على منصات التواصل الاجتماعي من قبل موظفي الجهة أو وكلائها أو متعهديها.

1.6 سياسة البريد الإلكتروني - الحد الأدنى من المتطلبات

يجب أن تستوفي الجهات الحكومية الحد الأدنى من المتطلبات التالية فيما يتعلق بسياسة البريد الإلكتروني الخاصة بها:

- تحديد الغرض من هذه السياسة على أنه يتمثل في وضع إرشادات مناسبة ومحايدة تجاه الموردين للاستخدام الآمن والملائم للبريد الإلكتروني.
- تحديد نطاق السياسة لتشمل استخدام أي موارد لتكنولوجيا المعلومات، بما في ذلك الأجهزة والبرامج والشبكات، التي تستخدمها الجهة الحكومية أو تتوفر لديها لغرض إرسال أو استقبال رسائل البريد الإلكتروني والمرفقات.
- توضيح إمكانية تطبيق سياسة استخدام الأجهزة الشخصية في العمل والاستخدام من قبل الجهات الثالثة.
- تحديد متطلبات الاستخدام المقبول للبريد الإلكتروني للجهة، والتي يجب أن تشمل:
  - استخدام اللغة المهنية المناسبة والالتزام بآداب البريد الإلكتروني؛
  - عدم إرسال أي معلومات حساسة/سرية إلى أطراف ثالثة غير مسموح لها بالحصول على تلك المعلومات؛
  - الالتزام عند إرسال معلومات حساسة/سرية إلى أطراف ثالثة مسموح لها بالحصول على مثل هذه المعلومات بتصنيف تلك المعلومات على النحو المناسب (على سبيل المثال: "سرية"، "لأغراض داخلية بحتة"، وما إلى ذلك).
- وضع قيود للاستخدام الشخصي لنظام البريد الإلكتروني للجهة، لا سيما من خلال التشديد على أن نظام البريد الإلكتروني للوكالة ونطاقها يجب استخدامهما فقط بما يتوافق مع سياسة الاستخدام المقبول للجهة.
- تضمين قواعد الاحتفاظ بالبريد الإلكتروني وإنشاء نسخ احتياطية منه تحسباً لنسيان كلمة المرور أو فقدان أصول تكنولوجيا المعلومات أو سرقتها (على سبيل المثال: الكمبيوتر، الهاتف، الكمبيوتر المتنقل، وما إلى ذلك).
- وضع تدابير أمنية ضد التهديدات السيبرانية من خلال تضمين تحذيرات منتظمة ضد التصيد الاحتيالي.
- توعية جميع المستخدمين بعواقب انتهاك سياسة البريد الإلكتروني للجهة.

1.7 سياسة إدارة أصول تكنولوجيا المعلومات – الحد الأدنى من المتطلبات

يجب أن تستوفي الجهات الحكومية الحد الأدنى من المتطلبات التالية فيما يتعلق بسياسة إدارة أصول تكنولوجيا المعلومات الخاصة بها:

- تحديد الغرض من هذه السياسة على أنه يتمثل في وضع قواعد واضحة للإدارة المناسبة والفعّالة لمعدات تكنولوجيا المعلومات، بدءًا من شرائها وحتى التخلص منها، في الجهة الحكومية.
- تحديد نطاق السياسة ليشمل جميع أصول تكنولوجيا المعلومات التي تحصل عليها الجهة الحكومية والتي تتألف من كل من أصول الأجهزة (على سبيل المثال: أجهزة الكمبيوتر المتنقلة والطابعات والخوادم) وأصول البرامج (على سبيل المثال: البرامج، التراخيص).
- تحديد إجراءات اقتناء أي أصول جديدة لتكنولوجيا المعلومات (على سبيل المثال: البرامج وأجهزة الكمبيوتر والشاشات والأجهزة اللوحية وغيرها). وعلى الرغم من أن الإجراءات ستختلف على الأرجح باختلاف الجهة، إلا أنها يجب أن تتضمن الحصول على موافقة من وزارة الاتصالات وتكنولوجيا المعلومات.
- تحديد متطلبات صيانة الأصول التي تجمع بين متطلبات الصيانة الخاصة بالجهة ومتطلبات الصيانة العامة لوزارة الاتصالات وتكنولوجيا المعلومات.
- توفير مجموعة أصول تكنولوجيا المعلومات المخصصة لأدوار محددة داخل الجهة.
- الحرص على متابعة جرد أصول تكنولوجيا المعلومات التابعة للجهة بصورة فعالة تضمن الحفاظ على الحد الأدنى أو المناسب من المخزون، وذلك ليتسنى تتبع عدد أصول تكنولوجيا المعلومات المختلفة وكمياتها وفترة صلاحيتها للاستخدام.
- وضع إجراءات محددة للتخلص من أصول تكنولوجيا المعلومات التي يتم تحديثها بشكل دوري (على سبيل المثال: أجهزة الكمبيوتر المتنقلة والأجهزة اللوحية وما إلى ذلك) وأصول تكنولوجيا المعلومات الأخرى وذلك في الحالتين التاليتين:
  - عمليات التخلص المخطط له (على سبيل المثال: انتهاء العمر الافتراضي للأصل)؛ و
  - عمليات التخلص غير المخطط له (على سبيل المثال: الأصول المفقودة/ المسروقة).
- تحديد قواعد الوصول لأصول الجهة من قبل أطراف ثالثة، سواءً للوصول المادي أو الوصول إلى تكنولوجيا المعلومات، وتضمين مصفوفات توزيع المسؤوليات التي تحدد أدوار ومسؤوليات الأطراف المعنية.
- استحداث إجراءات لمراجعة تراخيص البرامج بشكل دوري وتحديد الإجراءات المناسبة الواجب اتخاذها بعد المراجعة في حال وجود أي ترخيص منتهي الصلاحية، بما في ذلك:
  - عملية تجديد تراخيص البرامج التي لا تزال ضرورية لأعمال الجهة الحكومية؛
  - عملية إلغاء التراخيص غير المستخدمة التي تم الحصول عليها لصالح وزارة الاتصالات وتكنولوجيا المعلومات بموجب الاتفاقيات الإطارية الحكومية؛
  - عملية التفاوض مع الموردين لإنهاء خدمات الدعم.

1.8 سياسة إدارة التغيير في تكنولوجيا المعلومات - الحد الأدنى من المتطلبات

يجب أن تستوفي الجهات الحكومية الحد الأدنى من المتطلبات التالية فيما يتعلق بسياسة إدارة التغيير في تكنولوجيا المعلومات الخاصة بها:

- تحديد الغرض من هذه السياسة على أنه يتمثل في تقليل حالات التعطل والأخطاء أثناء إجراء تغييرات على خدمات تكنولوجيا المعلومات داخل الجهة.
- تحديد نطاق السياسة ليشمل جميع موظفي الجهة ووكلائها ومتعهديها الذين يضطلعون بأعمال الترقية أو التصحيح أو التعديل لأنظمة تكنولوجيا المعلومات التشغيلية أو المرتبطة بالمشاريع لدى الجهة.
- توثيق جميع الإعدادات الأساسية لأنظمة المعلومات الحالية، بما في ذلك تكوينات المكونات، وضمان حماية قاعدة بيانات إدارة التغيير.
- إنشاء آلية أو أداة إلزامية لبدء عمليات التعديل أو الشروع في تقديم طلبات التغيير.
- تشكيل مجلس استشاري للتغيير يكون مسؤولًا عن إدارة التغيير داخل الجهة، وتحديد أدوار المجلس ومسؤولياته، على أن تشمل ما يلي:
  - تقييم طلبات التغيير والموافقة عليها؛
  - ترتيب طلبات التغيير حسب الأولوية بناءً على مدى تأثيرها وأهميتها؛
  - إبلاغ الجهات المعنية داخل بالجهة بالتغييرات.
- تحديد المعايير المحتملة لرفض طلبات التغيير.
- تحديد الأنواع المختلفة للتغييرات والإجراءات ذات الصلة التي يجب اتباعها لكل منها، مثل التغيير القياسي والتغيير الطارئ وما إلى ذلك.

1.9 سياسة الاتصالات المحلية - الحد الأدنى من المتطلبات

يجب أن تستوفي الجهات الحكومية الحد الأدنى من المتطلبات التالية فيما يتعلق بسياسة الاتصالات المحلية الخاصة بها:

- تحديد الغرض من هذه السياسة على أنه يتمثل في استخدام قنوات الاتصال المختلفة داخل الجهة، بالإضافة إلى أدوار ومسؤوليات الموظفين في الوصول إليها.
- تحديد نطاق السياسة ليشمل جميع موظفي الجهة الذين يتواصلون فيما بينهم من خلال قنوات الاتصال وأجهزة تكنولوجيا المعلومات الخاصة بالجهة.
- الاسترشاد بسياسة تصنيف البيانات الوطنية والتأكد من التوافق الكامل معها.
- تضمين جميع قنوات الاتصال الداخلية المختلفة للجهة.
- وضع مبادئ وإجراءات للتواصل من خلال قنوات الاتصال المدرجة، سواء في ظروف العمل العادية أو في حالات الطوارئ/الأزمات.

1.10 سياسة أمن الشبكات - الحد الأدنى من المتطلبات

يجب أن تستوفي الجهات الحكومية الحد الأدنى من المتطلبات التالية فيما يتعلق بسياسة أمن الشبكات الخاصة بها:

- تحديد الغرض من هذه السياسة على أنه يتمثل في حماية أمن شبكة الجهة الحكومية بأكملها (بما في ذلك الشبكات السحابية المستخدمة) من خلال ضمان السرية والنزاهة والتوفّر.
- تحديد نطاق السياسة ليشمل كامل شبكة الجهة الحكومية، وكذلك جميع موظفيها ووكلائها ومتعهديها والأطراف الثالثة التي تتعامل مع هذه الشبكة أو داخلها.
- الاسترشاد بسياسة تصنيف البيانات الوطنية وسياسة الحوسبة السحابية أولاً والتأكد من التوافق الكامل معهما.
- حماية الأمن المادي والبيئي للشبكة.
- تحديد عمليات للمهام الدورية التالية المتعلقة بتأمين أنظمة المعلومات:
  - تدقيق الأحداث مثل المحاولات الفاشلة لتسجيل الدخول، وفتح المعلومات أو إغلاقها، واستخدام الحسابات المميزة؛
  - تسجيل وتوثيق الأحداث (بما في ذلك تاريخ ووقت ومكان الحدوث) مثل الانحرافات في جدران الحماية والنشاط على أجهزة التوجيه والمحولات والأجهزة المضافة أو المحذوفة حديثًا من الشبكة.
- تحديد متطلبات معينة للشبكة لغايات:
  - أمن جهاز التوجيه والتبديل؛
  - الاتصال اللاسلكي؛
  - الشبكة الافتراضية الخاصة (VPN)؛
  - أمن جدار الحماية.
- وضع بروتوكولات النسخ الاحتياطي للبيانات واستعادتها.

1.11 سياسة الأمن المادي والبيئي - الحد الأدنى من المتطلبات

يجب أن تستوفي الجهات الحكومية الحد الأدنى من المتطلبات التالية فيما يتعلق بسياسة الأمن المادي والبيئي الخاصة بها:

- تحديد الغرض من هذه السياسة على أنه يتمثل في صيانة أصول وأنظمة المعلومات من الوصول غير القانوني وحمايتها من المخاطر البيئية، وذلك من خلال تطبيق قيود مادية وبيئية.
- تحديد نطاق السياسة ليشمل جميع موظفي الجهة ووكلائها ومتعهديها (مثل الاستشاريين الذين يزورون الجهة) وأي شخص آخر لديه إمكانية الوصول إلى أي معدات تكنولوجيا المعلومات المادية للجهة.
- تحديد جميع معدات تكنولوجيا المعلومات التي تملكها الجهة أو تستخدمها بأي شكل، سواء داخل مقراتها أو خارجها.
- وضع تدابير أمنية محددة لجميع معدات تكنولوجيا المعلومات المحددة.
- تحديد صلاحيات النفاذ إلى معدات تكنولوجيا المعلومات، بناءً على متطلبات المهام ومستوى التصريح الأمني للموظف.
- تحديد صلاحيات النفاذ إلى معدات تكنولوجيا المعلومات للموظفين الخارجيين والمؤقتين وكذلك المسؤولين عن الصيانة الذين لديهم حق الوصول إلى المواقع.
- بيان المتطلبات المادية والظروف البيئية وضوابط النفاذ اللازمة لتأمين وحماية غرف الخوادم في الجهة.

1.12 سياسة النفاذ عن بُعد - الحد الأدنى من المتطلبات

يجب أن تستوفي الجهات الحكومية الحد الأدنى من المتطلبات التالية فيما يتعلق بسياسة النفاذ عن بُعد الخاصة بها:

- تحديد الغرض من هذه السياسة على أنه يتمثل فيه وضع إرشادات وشروط للاتصال من أي مضيف (أي أجهزة الكمبيوتر المتنقلة والأجهزة اللوحية والهواتف المتنقلة) إلى شبكة الجهة الحكومية.
- تحديد نطاق السياسة ليشمل جميع موظفي الجهة ووكلائها ومتعهديها الذين يستخدمون معدات الجهة الحكومية ويقومون بالنفاذ عن بُعد إلى أنظمة المعلومات الحكومية ونشرها وإدارتها.
- تحديد أنواع الأجهزة المؤهلة للنفاذ عن بُعد (على سبيل المثال: الأجهزة اللوحية، وأجهزة الكمبيوتر)، والتفريق بين سيناريوهات استخدام الأجهزة الشخصية في العمل وسيناريوهات الوصول من قبل الأطراف الثالثة.
- تحديد أنظمة تكنولوجيا المعلومات الخاصة بالجهة التي تتيح النفاذ عن بُعد.
- وضع بروتوكولات لحماية المعلومات الحساسة أثناء النفاذ عن بُعد.
- التنويه بأنه لا يُسمح بالنفاذ عن بُعد إلا للضرورة، ويجب إلغاؤه على الفور عند انتفاء الحاجة إليه، وكذلك التأكد من حذف جميع البيانات المحتفظ بها لغرض هذا النفاذ عن بُعد.
- العلم بأن النفاذ عبر شبكة افتراضية خاصة يجب أن يتم باستخدام بآلية مصادقة مناسبة متعددة العوامل، وأن المحاولات المتعددة سيترتب عليها إصدار تنبيهات.

الملحق 2: نماذج السياسات

يوضح هذا الملحق نماذج السياسة لكل سياسة داخلية لتكنولوجيا المعلومات المنصوص عليها في هذه الوثيقة، بغرض دعم الجهات الحكومية في تطوير كل منها لمنظمتها.

يتم توفير النماذج المحددة لكل سياسة داخلية لتكنولوجيا المعلومات في الأقسام الفرعية التالية. يجوز للجهات تكييف هذه الأقسام أو دمج أقسام إضافية لتلبية احتياجاتها ومتطلباتها الفريدة المتعلقة بسياسات تكنولوجيا المعلومات الداخلية الخاصة بها.

2.1 سياسة الاستخدام المقبول

رقم إصدار السياسة:	*[... 1.0...]*	**عنوان السياسة:**	*[...]*
تاريخ الإصدار:	*[...]*	**تاريخ المراجعة:**	*[...]*
المسؤول عن السياسة/الإدارة:	*[...]*	**اسم معد السياسة:**	*[...]*

مقدمة

توضِّح سياسة الاستخدام المقبول الاستخدام السليم لموارد تكنولوجيا المعلومات داخل الجهات الحكومية. وتفرض هذه السياسة على جميع الموظفين والمتعهدين والمنتسبين استخدام هذه الموارد وفقًا للمعايير الأخلاقية والقانونية وبما يسهم في تحقيق أهداف الجهة. [...]

التعاريف

- *[...]*

الغرض من السياسة وأهدافها

تتمثل أهداف هذه السياسة فيما يلي:

- *حماية توافر موارد تكنولوجيا المعلومات التي تملكها [الجهة] أو تستخدمها وصيانة سرية هذه الموارد وسلامتها.*
- *تشجيع الاستخدام الأخلاقي والمسؤول لموارد تكنولوجيا المعلومات.*
- *[...]*

نطاق السياسة وتطبيقها

تنطبق هذه السياسة على جميع معدات تكنولوجيا المعلومات التي تملكها [الجهة] و/أو تستخدمها، وكذلك الحالات التي يتم فيها استخدام هذه المعدات.

بنود السياسة وأحكامها

فيما يلي بيان بمعايير الاستخدام المقبول لمعدات تكنولوجيا المعلومات التي تملكها [اسم الجهة] وتندرج ضمن نطاق هذه السياسة:

- *يجب أن تكون جميع معدات تكنولوجيا المعلومات والعمليات المتعلقة باستخدامها متوافقة مع القوانين واللوائح المعمول بها في دولة قطر [التي تشمل، على سبيل المثال لا الحصر، (اسم القانون/اللائحة، واسم القانون/اللائحة، ...].*
- *تقتصر استخدامات جميع معدات تكنولوجيا المعلومات والعمليات المتعلقة بها على نطاق العمل اليومي لـ [اسم الجهة] وفقًا للمهام الوظيفية المحددة لموظفيها. وعليه، لا يجوز لأي من موظفي [اسم الجهة] استخدام هذه المعدات والموارد لأغراض شخصية.*
- *لا بد من مراعاة خصوصية البيانات التي تستخدمها موارد تكنولوجيا المعلومات ذات الصلة على مستوى جميع معدات تكنولوجيا المعلومات والعمليات المتعلقة باستخدامها، وذلك من خلال تجنب النفاذ غير المصرح به إلى الموارد.*
- *[...]*

فيما يلي بيان بمعايير الاستخدام غير المقبول لمعدات تكنولوجيا المعلومات التي تملكها [اسم الجهة] وتندرج ضمن نطاق هذه السياسة:

- *يُحظر تثبيت واستخدام أي مورد من موارد تكنولوجيا المعلومات من شأنه أن يشكل انتهاكًا للوائح الحكومية أو القوانين الأخرى، مثل قوانين الملكية الفكرية.*
- *يُحظر انتهاك حقوق المستفيدين من الخدمة بواسطة أي مورد من موارد تكنولوجيا المعلومات، وذلك وفقًا للقوانين واللوائح المعمول بها في دولة قطر [التي تشمل، على سبيل المثال لا الحصر، (اسم القانون/اللائحة، واسم القانون/اللائحة، ...].*
- *يُمنع الوصول غير المصرح به إلى المعلومات الحكومية من قبل أطراف ثالثة، ويُمنح الحق في ذلك للجهات المعنية المحددة في [عنوان سياسة المصادقة على النفاذ وتوثيقه الخاصة بالجهة].*
- *يُحظر النسخ غير القانوني للمواد، الذي ينجم عنه قضايا متعلقة بحقوق النشر.*
- *[...]*

فيما يلي بيان بمعايير استخدام [اسم الجهة] والجهات المعنية لوسائل التواصل الاجتماعي:

- *المعايير الخاصة بموظفي [اسم الجهة]:*
  - *[...]*
- *المعايير الخاصة بالأطراف الثالثة التي تتعاقد معها [اسم الجهة]:*
  - *[...]*

متطلبات الامتثال

- *على جميع الجهات التي تنطبق عليها هذه السياسة أن تضمن امتثالها الكامل للأحكام الواردة في هذه السياسة.*
- *يجوز لـ [اسم الجهة] إجراء مراجعات دورية لمتابعة تطبيق هذه السياسة والامتثال لها.*

- *إذا تبين لـ[اسم الجهة] أن الجهات المعنية يمارسون أنشطة مخالفة لمتطلبات الامتثال، فلها أن تفرض غرامات إدارية، أو تنهي عقد/اتفاقية العمل، أو تتخذ الإجراءات القانونية اللازمة وفقًا للقوانين واللوائح المعمول في دولة قطر، وذلك بناءً على مدى خطورة الانتهاك ومدته.*

الوثائق المرتبطة / المراجع

- *[...]*

2.2 سياسة المصادقة على النفاذ وتوثيقه

رقم إصدار السياسة:	*[... 1.0...]*	**عنوان السياسة:**	*[...]*
تاريخ الإصدار:	*[...]*	**تاريخ المراجعة:**	*[...]*
المسؤول عن السياسة/الإدارة:	*[...]*	**اسم معد السياسة:**	*[...]*

مقدمة

تحدد سياسة المصادقة على النفاذ وتوثيقه التدابير اللازمة لحماية المعلومات مسجلة الملكية الخاصة بـ [اسم الجهة] من الانتهاكات أو الخروقات الناجمة عن إجراءات إدارة النفاذ والتوثيق غير السليمة. وتهدف هذه السياسة إلى ضمان ألا يحصل جميع الموظفين والوكلاء والمتعهدين إلا على حق الوصول إلى ما لدى [اسم الجهة] من الخدمات والبيانات والمعلومات التي تكون ضرورية للغاية لتنفيذ الأدوار المكلفين بها. [...]

التعاريف

- *[...]*

الغرض من السياسة وأهدافها

تتمثل أهداف هذه السياسة فيما يلي:

- *وضع إجراءات لحماية المعلومات ومنح الوصول إلى الحسابات السرية وكذلك إلى المعدات والبنية التحتية والخدمات والبرمجيات.*
- *[...]*

نطاق السياسة وتطبيقها

تنطبق هذه السياسة على جميع موظفي [اسم الجهة] ووكلائها ومتعهديها الذين لديهم إمكانية الوصول إلى المعلومات الحكومية وأنظمة تكنولوجيا المعلومات الخاصة بـ[اسم الجهة].

بنود السياسة وأحكامها

فيما يلي ضوابط الوصول التي تندرج ضمن نطاق هذه السياسة:

- *تخضع حقوق الوصول والتراخيص وكذلك الموارد المخصصة لـ"مبدأ الامتياز الأقل".*
- *يُمنح المستخدمون الحد الأدنى من حقوق الوصول إلى الأنظمة والخدمات والبيانات والمعلومات التي تكون ضرورية للغاية لتنفيذ الأدوار المكلفين بها.*

فيما يلي الإجراءات المتعلقة بمراجعة وصول المستخدمين بشكل دوري بالتنسيق مع أصحاب الأعمال وفريق أمن المعلومات، والتي تتوافق مع القوانين واللوائح ذات الصلة المعمول بها في دولة قطر بما في ذلك، على سبيل المثال لا الحصر، قانون حماية خصوصية البيانات الشخصية، و[اسم القانون/ اللائحة، واسم القانون/اللائحة ...]:

- *تحديد الحسابات الزائدة عن الحاجة وحذفها بمجرد انتهاء فترة الاحتفاظ التي تبلغ XXX يومًا.*

- *تحديد الحسابات غير النشطة وحذفها بمجرد انتهاء فترة الاحتفاظ التي تبلغ XXX يومًا.*
- *[...]*

فيما يلي إجراءات إدارة كلمة المرور المتعلقة بالوصول إلى حسابات [اسم الجهة]، والتي تندرج ضمن نطاق هذه السياسة:

- *يجب أن تتضمن كلمة المرور على الأقل أحد العناصر التالية:*
  - *حرف صغير*
  - *حرف كبير*
  - *حرف خاص*
  - *رقم*
  - *[...]*
- *يجب أن تتألف كلمة المرور مما يتراوح بين XXX و XXX أحرف/حرفًا.*
- *يجب إعادة تعيين كلمة المرور كل XXX يومًا.*
- *يجب ألا تتطابق كلمة المرور مع آخر XXX كلمات مرور تم استخدامها.*
- *[...]*

متطلبات الامتثال

- *على جميع الجهات التي تنطبق عليها هذه السياسة أن تضمن امتثالها الكامل للأحكام الواردة في هذه السياسة.*
- *يجوز لـ [اسم الجهة] إجراء مراجعات دورية لمتابعة تطبيق هذه السياسة والامتثال لها.*
- *إذا تبين لـ[اسم الجهة] أن الجهات المعنية يمارسون أنشطة مخالفة لمتطلبات الامتثال، فلها أن تفرض غرامات إدارية، أو تنهي عقد/اتفاقية العمل، أو تتخذ الإجراءات القانونية اللازمة وفقًا للقوانين واللوائح المعمول في دولة قطر، وذلك بناءً على مدى خطورة الانتهاك ومدته.*

الوثائق المرتبطة / المراجع

- *[...]*

2.3 سياسة النسخ الاحتياطي للبيانات واستعادتها

رقم إصدار السياسة:	*[... 1.0...]*	**عنوان السياسة:**	*[...]*
تاريخ الإصدار:	*[...]*	**تاريخ المراجعة:**	*[...]*
المسؤول عن السياسة/الإدارة:	*[...]*	**اسم معد السياسة:**	*[...]*

مقدمة

تتضمن سياسة النسخ الاحتياطي للبيانات واستعادتها الحد الأدنى من إجراءات النسخ الاحتياطي للبيانات المطلوبة التي يجب على [اسم الجهة] اتباعها. وتهدف هذه السياسة إلى ضمان أمن المعلومات في حالة فقدان البيانات الأصلية لدى [اسم الجهة] أو تعرضها للتلف. [...]

التعاريف

- *[...]*

الغرض من السياسة وأهدافها

تتمثل أهداف هذه السياسة فيما يلي:

- *ضمان إمكانية استرداد جميع بيانات ومعلومات [اسم الجهة] في حالة حدوث أي ضرر أو حادث.*
- *[...]*

نطاق السياسة وتطبيقها

تنطبق هذه السياسة على جميع موظفي [اسم الجهة] والأطراف الثالثة التي تتمتع بإمكانية الوصول إلى بيانات ومعلومات [اسم الجهة].

بنود السياسة وأحكامها

يجب أن تتوافق جميع معايير النسخ الاحتياطي للبيانات المطبقة داخل [اسم الجهة] مع مستويات تصنيف البيانات الواردة في سياسة تصنيف البيانات الوطنية، بما في ذلك البيانات العامة (C0)، والبيانات الداخلية (C1)، والبيانات المقيدة (C2)، والبيانات السرية (C3) والبيانات السرية للغاية (C4).

فيما يلي العناصر التي ينبغي أن تتضمنها خطة الاستجابة للطوارئ التي يجري تفعيلها عند وقوع الحوادث التي تعيق الوصول إلى البيانات، وذلك ضمن نطاق هذه السياسة:

- *مصفوفة التصعيد لتسهيل التواصل أثناء حالات الطوارئ:*
  - *[...]*
- *تدابير الطوارئ:*
  - *[...]*

- *خيارات الاسترداد:*
  - *[...]*
- *[...]*

تُحدِّد هذه السياسة الفترات الدورية للاحتفاظ بالنسخ الاحتياطية للبيانات وفقًا لمستويات تصنيفها حسب وتيرة النسخ الاحتياطي للبيانات التالية:

- *النسخ الاحتياطي اليومي.*
- *النسخ الاحتياطي الأسبوعي.*
- *النسخ الاحتياطي الشهري.*
- *[...]*

متطلبات الامتثال

- *على جميع الجهات التي تنطبق عليها هذه السياسة أن تضمن امتثالها الكامل للأحكام الواردة في هذه السياسة.*
- *يجوز لـ [اسم الجهة] إجراء مراجعات دورية لمتابعة تطبيق هذه السياسة والامتثال لها.*
- إذا تبين لـ[اسم الجهة] أن الجهات المعنية يمارسون أنشطة مخالفة لمتطلبات الامتثال، فلها أن تفرض غرامات إدارية، أو تنهي عقد/اتفاقية العمل، أو تتخذ الإجراءات القانونية اللازمة وفقًا للقوانين واللوائح المعمول في دولة قطر، وذلك بناءً على مدى خطورة الانتهاك ومدته.

الوثائق المرتبطة / المراجع

- *[...]*

2.4 سياسة تصنيف البيانات

رقم إصدار السياسة:	*[... 1.0...]*	**عنوان السياسة:**	*[...]*
تاريخ الإصدار:	*[...]*	**تاريخ المراجعة:**	*[...]*
المسؤول عن السياسة/الإدارة:	*[...]*	**اسم معد السياسة:**	*[...]*

مقدمة

تحدِّد سياسة تصنيف البيانات نهج تصنيف البيانات الموضح في سياسة تصنيف البيانات الوطنية وكيفية تطبيقه داخل [اسم الجهة]. وتهدف هذه السياسة إلى ضمان التوافق التام مع القوانين واللوائح ذات الصلة المعمول بها في دولة قطر [بما في ذلك اسم القانون/اللائحة، واسم القانون/اللائحة، ...] [...]

التعاريف

- *[...]*

الغرض من السياسة وأهدافها

تتمثل أهداف هذه السياسة فيما يلي:

- *وضع نهج لتصنيف البيانات على مستوى [اسم الجهة] بما يتوافق مع النهج المحدد في سياسة تصنيف البيانات الوطنية.*
- *[...]*

نطاق السياسة وتطبيقها

تنطبق هذه السياسة على جميع البيانات التي تجمعها أو تمتلكها أو تستخدمها [اسم الجهة].

بنود السياسة وأحكامها

يجب أن تتوافق جميع إجراءات تصنيف وحماية البيانات داخل [اسم الجهة] مع القوانين واللوائح المعمول بها في دولة قطر، بما في ذلك على سبيل المثال لا الحصر:

- *سياسة تصنيف البيانات الوطنية*
- *قانون تنظيم الحق في الحصول على المعلومات*
- *قانون حماية خصوصية البيانات الشخصية*
- *[...]*

يجب على [اسم الجهة] أن تحدد على الأقل مسؤوليات واضحة للأدوار التالية ضمن نطاق هذه السياسة:

- *يقع على عاتق مالكي البيانات مسؤولية تصنيف البيانات بناءً على مدى حساسيتها، وضمان توافر إجراءات الحماية الكافية.*

- *يتولى فريق أمن المعلومات المهام الإشرافية، إلى جانب وضع قواعد التصنيف وضمان الامتثال للقوانين واللوائح.*
- *يجب على أصحاب الأعمال العمل بالتنسيق مع مالكي البيانات والمسؤولين عن حفظها لضمان مطابقة تصنيف البيانات مع المتطلبات التشغيلية والتنظيمية.*

فيما يلي وصف لعملية تصنيف البيانات ضمن نطاق هذه السياسة:

- *التحقق من مدى حساسية البيانات والمعلومات الحكومية من قبل الموظفين المسؤولين.*
- *تصنيف البيانات والمعلومات التي تم التحقق منها من قبل الموظفين المسؤولين، وفقًا لسياسة تصنيف البيانات الوطنية، وذلك ضمن فئات البيانات العامة (C0)، أو البيانات الداخلية (C1)، أو البيانات المقيدة (C2)، أو البيانات السرية ((C3، أو البيانات السرية للغاية (C4).*
- *إجراء مراجعة دورية لفئات البيانات من قبل الموظفين المسؤولين.*

متطلبات الامتثال

- *على جميع الجهات التي تنطبق عليها هذه السياسة أن تضمن امتثالها الكامل للأحكام الواردة في هذه السياسة.*
- *يجوز لـ [اسم الجهة] إجراء مراجعات دورية لمتابعة تطبيق هذه السياسة والامتثال لها.*
- *إذا تبين لـ[اسم الجهة] أن الجهات المعنية يمارسون أنشطة مخالفة لمتطلبات الامتثال، فلها أن تفرض غرامات إدارية، أو تنهي عقد/اتفاقية العمل، أو تتخذ الإجراءات القانونية اللازمة وفقًا للقوانين واللوائح المعمول في دولة قطر، وذلك بناءً على مدى خطورة الانتهاك ومدته.*

الوثائق المرتبطة / المراجع

- *[...]*

2.5 سياسة خصوصية البيانات

رقم إصدار السياسة:	*[... 1.0...]*	**عنوان السياسة:**	*[...]*
تاريخ الإصدار:	*[...]*	**تاريخ المراجعة:**	*[...]*
المسؤول عن السياسة/الإدارة:	*[...]*	**اسم معد السياسة:**	*[...]*

مقدمة

تتضمن سياسة خصوصية البيانات قواعد خصوصية البيانات المعمول بها في دولة قطر. وتهدف هذه السياسة إلى ضمان التوافق التام مع متطلبات الخصوصية المحددة لكل فئة من فئات البيانات بما في ذلك البيانات الحساسة والبيانات المقيدة، [...]، وذلك على النحو المنصوص عليه في سياسة تصنيف البيانات الوطنية وقانون حماية خصوصية البيانات الشخصية. [...]

التعاريف

- *[...]*

الغرض من السياسة وأهدافها

تتمثل أهداف هذه السياسة فيما يلي:

- *ترسيخ حقوق حماية البيانات لمختلف مستويات تصنيف البيانات داخل [اسم الجهة].*
- *[...]*

نطاق السياسة وتطبيقها

تنطبق هذه السياسة على جميع البيانات التي تتولى [اسم الجهة] جمعها أو تخزينها أو تحديثها أو نقلها.

بنود السياسة وأحكامها

يجب أن تتوافق جميع معايير خصوصية البيانات المطبقة داخل [اسم الجهة] مع مستويات تصنيف البيانات الواردة في سياسة تصنيف البيانات الوطنية، بما في ذلك البيانات العامة (C0)، والبيانات الداخلية (C1)، والبيانات المقيدة (C2)، والبيانات السرية (C3) والبيانات السرية للغاية (C4).

فيما يلي معايير الإفصاح عن البيانات المتعلقة بـ[اسم الجهة] أو غيرها من البيانات أو استخدامها على منصات التواصل الاجتماعي أو قنوات التواصل الأخرى من قبل موظفي [اسم الجهة] أو وكلائها أو متعهديها.

- *المعايير الخاصة بموظفي [اسم الجهة]:*
  - *[...]*
- *المعايير الخاصة بالأطراف الثالثة التي تتعاقد معها [اسم الجهة]:*
  - *[...]*

فيما يلي آلية التحكم في الوصول بناءً على الدور التي تحدد أدوار ومسؤوليات مختلف الجهات المعنية التي تتعامل مع بيانات [اسم الجهة]، وذلك ضمن نطاق هذه السياسة:

- *يقع على عاتق مالكي البيانات مسؤولية:*
  - *تحديد حقوق الوصول وعمليات الموافقة بشأن البيانات التي تقع في حوزتهم.*
  - *ضمان إجراء مراجعات دورية لتحديث حقوق وصول المستخدمين حسب الحاجة.*
  - *[...]*
- *يُمنح المستخدمون (أي موظفي [اسم الجهة] أو وكلائها أو متعهديها) حق الوصول إلى البيانات بما يتماشى مع نطاق أعمالهم اليومية داخل [اسم الجهة]، وهم مسؤولون عن:*
  - *استخدام البيانات والموارد فقط ضمن نطاق المهام المخصصة لها.*
  - *الالتزام بمتطلبات حماية وخصوصية البيانات.*
  - *[...]*
- *[...]*

متطلبات الامتثال

- *على جميع الجهات التي تنطبق عليها هذه السياسة أن تضمن امتثالها الكامل للأحكام الواردة في هذه السياسة.*
- *يجوز لـ [اسم الجهة] إجراء مراجعات دورية لمتابعة تطبيق هذه السياسة والامتثال لها.*
- *إذا تبين لـ[اسم الجهة] أن الجهات المعنية يمارسون أنشطة مخالفة لمتطلبات الامتثال، فلها أن تفرض غرامات إدارية، أو تنهي عقد/اتفاقية العمل، أو تتخذ الإجراءات القانونية اللازمة وفقًا للقوانين واللوائح المعمول في دولة قطر، وذلك بناءً على مدى خطورة الانتهاك ومدته.*

الوثائق المرتبطة / المراجع

- *[...]*

2.6 سياسة البريد الإلكتروني

رقم إصدار السياسة:	*[... 1.0...]*	**عنوان السياسة:**	*[...]*
تاريخ الإصدار:	*[...]*	**تاريخ المراجعة:**	*[...]*
المسؤول عن السياسة/الإدارة:	*[...]*	**اسم معد السياسة:**	*[...]*

مقدمة

تتضمن سياسة البريد الإلكتروني الإرشادات المتعلقة بالاستخدام الملائم للبريد الإلكتروني الشخصي فيما يخص حسابات البريد الإلكتروني الخاصة بـ [اسم الجهة]، بالإضافة إلى معايير الاستخدام السليم لحسابات البريد الإلكتروني الرسمية لدى [اسم الجهة]. وتهدف هذه السياسة إلى ضمان أن تكون جميع رسائل البريد الإلكتروني، التي يرسلها موظفو [اسم الجهة] وتتضمن معلومات حول أعمالها، متوافقة مع معايير الأمن والسرية والخصوصية التي تطبّقها [اسم الجهة]. [...]

التعاريف

- *[...]*

الغرض من السياسة وأهدافها

تتمثل أهداف هذه السياسة فيما يلي:

- *وضع إرشادات مناسبة ومحايدة تجاه الموردين للاستخدام الآمن والملائم للبريد الإلكتروني.*
- *[...]*

نطاق السياسة وتطبيقها

تنطبق هذه السياسة على جميع موظفي [اسم الجهة] الذين يستخدمون أي موارد لتكنولوجيا المعلومات، بما في ذلك الأجهزة والبرامج والشبكات، لغرض إرسال أو استقبال رسائل البريد الإلكتروني والمرفقات.

بنود السياسة وأحكامها

فيما يلي معايير الاستخدام المقبول لجميع رسائل البريد الإلكتروني التي يرسلها موظفو [اسم الجهة]، وذلك ضمن نطاق هذه السياسة:

- *على الموظفين الالتزام بالإرشادات المتعلقة بآداب البريد الإلكتروني الخاصة بـ [اسم الجهة] واستخدام اللغة المناسبة في جميع المراسلات عبر البريد الإلكتروني لضمان الحفاظ على المهنية.*
- *يجب استخدام نظام البريد الإلكتروني لـ[اسم الجهة] ونطاقها للأغراض الرسمية فقط، بما يتوافق مع سياسة الاستخدام المقبول للجهة.*
- *يتعين تصنيف المعلومات الحساسة أو المقيدة على النحو المناسب (على سبيل المثال، سرية) عند مشاركتها مع المستلمين المعتمدين لضمان التعامل معها بشكل سليم.*
- *[...]*

فيما يلي معايير الاستخدام غير المقبول لجميع رسائل البريد الإلكتروني التي يرسلها موظفو [اسم الجهة]، وذلك ضمن نطاق هذه السياسة:

- *يُحظر استخدام نظام البريد الإلكتروني الخاص بـ [اسم الجهة] للأغراض الشخصية.*
- *يُحظر تمامًا على الموظفين إرسال معلومات خاصة أو مقيدة إلى أفراد غير مسموح لهم بالحصول على هذه المعلومات.*
- *تشمل الإجراءات التأديبية الناتجة عن انتهاك هذه السياسة، على سبيل المثال لا الحصر، إلغاء حقوق الوصول، والتحذيرات الرسمية، وقد يصل الأمر في الحالات الخطيرة إلى اتخاذ إجراءات قانونية بحق المخالفين.*
- *[...]*

تتضمن أنشطة تعزيز الوعي بالأمن السيبراني لدى [اسم الجهة] ما يلي، على سبيل المثال لا الحصر:

- *يجب أن يخضع كل موظف لتدريب سنوي يهدف إلى تعزيز الوعي بالأمن السيبراني، على أن يتضمن هذا التدريب المواضيع التالية التي تحددها [اسم الجهة]:*
  - *التعرف على رسائل البريد الإلكتروني الاحتيالية والمواقع الإلكترونية الوهمية.*
  - *اتباع الإجراءات الأمنية اللازمة لإدارة البيانات الخاصة.*
  - *الوعي بالمخاطر التي تنجم عن هجمات الهندسة الاجتماعية.*
- *تعمل [اسم الجهة] على إجراء تقييمات دورية لاستعداد الموظفين من خلال اختبارات محاكاة للتصيد الاحتيالي. ويتعين على الموظفين الخضوع لمزيد من التدريب إذا لم يتمكنوا من التعرف على محاولات التصيد الاحتيالي التي يتم محاكاتها.*
- *[...]*

متطلبات الامتثال

- *على جميع الجهات التي تنطبق عليها هذه السياسة أن تضمن امتثالها الكامل للأحكام الواردة في هذه السياسة.*
- *يجوز لـ [اسم الجهة] إجراء مراجعات دورية لمتابعة تطبيق هذه السياسة والامتثال لها.*
- *إذا تبين لـ[اسم الجهة] أن الجهات المعنية يمارسون أنشطة مخالفة لمتطلبات الامتثال، فلها أن تفرض غرامات إدارية، أو تنهي عقد/اتفاقية العمل، أو تتخذ الإجراءات القانونية اللازمة وفقًا للقوانين واللوائح المعمول في دولة قطر، وذلك بناءً على مدى خطورة الانتهاك ومدته.*

الوثائق المرتبطة / المراجع

- *[...]*

2.7 سياسة إدارة أصول تكنولوجيا المعلومات

رقم إصدار السياسة:	*[... 1.0...]*	**عنوان السياسة:**	*[...]*
تاريخ الإصدار:	*[...]*	**تاريخ المراجعة:**	*[...]*
المسؤول عن السياسة/الإدارة:	*[...]*	**اسم معد السياسة:**	*[...]*

مقدمة

تتضمن سياسة إدارة أصول تكنولوجيا المعلومات مجموعة شاملة من قواعد الإدارة الفعالة لمعدات تكنولوجيا المعلومات الخاصة بـ [اسم الجهة]. تهدف هذه السياسة إلى ضمان تغطية جميع مراحل دورة حياة أصول أجهزة أو برامج تكنولوجيا المعلومات لدى [اسم الجهة]، بدءًا من شرائها وتركيبها أو تثبيتها، مرورًا باستخدامها وصيانتها، ووصولًا إلى التخلص منها. [...]

التعاريف

- *[...]*

الغرض من السياسة وأهدافها

تتمثل أهداف هذه السياسة فيما يلي:

- *وضع قواعد واضحة للإدارة المناسبة والفعّالة لمعدات تكنولوجيا المعلومات، بدءًا من شرائها وحتى التخلص منها، في [اسم الجهة]*
- *[...]*

نطاق السياسة وتطبيقها

تنطبق هذه السياسة على جميع أصول تكنولوجيا المعلومات التي تحصل عليها أو تملكها [اسم الجهة]، بما في ذلك أصول الأجهزة والبرامج.

بنود السياسة وأحكامها

فيما يلي إجراءات اقتناء أي أصول جديدة لتكنولوجيا المعلومات، والتي تندرج ضمن نطاق هذه السياسة:

- *تتولى فرق [اسم الجهة] تقييم مدى الحاجة إلى اقتناء أصول جديدة لتكنولوجيا المعلومات وفقًا للمتطلبات التشغيلية أو التحسينات التقنية أو جداول الاستبدال.*
- *تعمل [اسم الجهة] على تفعيل خطة لتخصيص الأصول المحددة بناءً على الأدوار الوظيفية:*
  - *يمكن تخصيص أصول تكنولوجيا المعلومات التالية للموظفين التنفيذيين:*
    - *[...]*

- يمكن تخصيص أصول تكنولوجيا المعلومات التالية للموظفين الإداريين:
  - [...]
- يمكن تخصيص أصول تكنولوجيا المعلومات التالية لـ[...]:
  - [...]

- ينبغي الحصول على الموافقات التالية في جميع عمليات اقتناء الأصول:
  - موافقة رؤساء الأقسام المختصة في [اسم الجهة].
  - موافقة وزارة الاتصالات وتكنولوجيا المعلومات.
- يجب اختيار الموردين وفقًا لمعايير المشتريات المعمول بها، مع مراعاة قائمة الموردين المعتمدين والاتفاقيات الإطارية التي وضعتها وزارة الاتصالات وتكنولوجيا المعلومات.
- [...]

فيما يلي متطلبات صيانة الأصول التي تجمع بين متطلبات الصيانة الخاصة بـ[اسم الجهة] وأفضل ممارسات الصيانة العامة، وذلك ضمن نطاق هذه السياسة:

- تشمل متطلبات الصيانة الوقائية لأصول [اسم الجهة] ما يلي:
  - [...]
- تشمل متطلبات الصيانة التصحيحية لأصول [اسم الجهة] ما يلي:
  - [...]
- تشمل متطلبات صيانة الأصول الخارجية ما يلي:
  - [...]

فيما يلي إجراءات التخلص من أصول تكنولوجيا المعلومات، التي تندرج ضمن نطاق هذه السياسة:

- ترد أدناه متطلبات التخلص المخطط له من أصول تكنولوجيا المعلومات الخاصة بـ[اسم الجهة] عند انتهاء عمرها الافتراضي:
  - [...]
- ترد أدناه متطلبات التخلص غير المخطط له من أصول تكنولوجيا المعلومات (المفقودة أو المسروقة) الخاصة بـ [اسم الجهة]:
  - [...]

فيما يلي قواعد الوصول المادي أو الوصول إلى تكنولوجيا المعلومات من قبل أطراف ثالثة إلى أصول تكنولوجيا المعلومات الخاصة بـ[اسم الجهة]، والتي تندرج ضمن نطاق هذه السياسة:

- لا يجوز إلا للأطراف الثالثة المصرح لها الوصول إلى أصول تكنولوجيا المعلومات أو المواقع المادية، وذلك بعد خضوعهم لعملية تحقق شاملة.

- *يجب مراقبة جميع أنشطة الوصول من قبل الأطراف الثالثة وتوثيقها.*
- *يتعين إعداد مصفوفات توزيع المسؤوليات لجميع الأطراف الثالثة التي يمكنها الوصول إلى أصول تكنولوجيا المعلومات الخاصة بـ [اسم الجهة].*
  - *الموظفون المسؤولون عن الوصول من قبل الأطراف الثالثة هم XXX.*
  - *الموظفون الخاضعون للمساءلة عن الوصول من قبل الأطراف الثالثة هم XXX.*
  - *الموظفون الذين يتم استشارتهم فيما يتعلق بالوصول من قبل الأطراف الثالثة هم XXX.*
  - *الموظفون الذي يجري اطلاعهم على مستجدات كل ما يخص الوصول من قبل الأطراف الثالثة هم XXX.*

متطلبات الامتثال

- *على جميع الجهات التي تنطبق عليها هذه السياسة أن تضمن امتثالها الكامل للأحكام الواردة في هذه السياسة.*
- *يجوز لـ [اسم الجهة] إجراء مراجعات دورية لمتابعة تطبيق هذه السياسة والامتثال لها.*
- *إذا تبين لـ[اسم الجهة] أن الجهات المعنية يمارسون أنشطة مخالفة لمتطلبات الامتثال، فلها أن تفرض غرامات إدارية، أو تنهي عقد/اتفاقية العمل، أو تتخذ الإجراءات القانونية اللازمة وفقًا للقوانين واللوائح المعمول في دولة قطر، وذلك بناءً على مدى خطورة الانتهاك ومدته.*

الوثائق المرتبطة / المراجع

- *[...]*

2.8 سياسة إدارة التغيير في تكنولوجيا المعلومات

رقم إصدار السياسة:	*[... 1.0...]*	**عنوان السياسة:**	*[...]*
تاريخ الإصدار:	*[...]*	**تاريخ المراجعة:**	*[...]*
المسؤول عن السياسة/الإدارة:	*[...]*	**اسم معد السياسة:**	*[...]*

مقدمة

تتضمن سياسة إدارة التغيير في تكنولوجيا المعلومات الإجراءات المتعلقة بالإغلاق المؤقت لأنظمة تكنولوجيا المعلومات أثناء عمليات الصيانة أو الترقيات أو التعديلات المخطط لها. وتهدف هذه السياسة إلى تقليل حالات التعطل والأخطاء أثناء إجراء أنشطة تحسين خدمات تكنولوجيا المعلومات داخل [اسم الجهة]. [...]

التعاريف

- *[...]*

الغرض من السياسة وأهدافها

تتمثل أهداف هذه السياسة فيما يلي:

- *تقليل حالات التعطل والأخطاء أثناء إجراء تغييرات على خدمات تكنولوجيا المعلومات داخل [اسم الجهة].*
- *[...]*

نطاق السياسة وتطبيقها

تنطبق هذه السياسة على جميع موظفي الجهة ووكلائها ومتعهديها الذين يضطلعون بأعمال الترقية أو التصحيح أو التعديل لأنظمة تكنولوجيا المعلومات التشغيلية أو المرتبطة بالمشاريع لدى الجهة.

بنود السياسة وأحكامها

يجب إبقاء قاعدة بيانات إدارة التغيير محدثة باستمرار لتسجيل وتتبع الإعدادات والتغييرات، وذلك من خلال اتخاذ التدابير الأمنية اللازمة لحمايتها من الوصول غير المصرح به والتعديلات غير المرغوب فيها.

يتولى المجلس الاستشاري للتغيير مسؤولية الإشراف على عملية إدارة التغيير داخل [اسم الجهة]، والتي تتألف من المراحل التالية في إطار نطاق هذه السياسة:

- *يجب على فرق [اسم الجهة] تقديم طلب تغيير إلى المجلس الاستشاري للتغيير فيما يخص أي أصل من أصول تكنولوجيا المعلومات يحتاج إلى التجديد داخل فرقهم.*
- *يتولى المجلس الاستشاري للتغيير تقييم طلبات التغيير والموافقة عليها وتحديد أولوياتها بناءً على مدى تأثيرها وأهميتها.*
- *يعمل المجلس الاستشاري للتغيير على إبلاغ الجهات المعنية داخل [اسم الجهة] بالتغييرات.*

- *[...]*

فيما يلي معايير الرفض لطلبات إدارة التغيير في تكنولوجيا المعلومات التي تندرج ضمن نطاق هذه السياسة:

- *إذا كان الطلب يتجاوز حدود ميزانية [اسم الجهة] المخصصة لمعدات تكنولوجيا المعلومات أو يتطلب إنفاق جزء كبير منها.*
- *إذا كان الطلب لا يتوافق مع الاستراتيجية العامة لـ [اسم الجهة].*
- *إذا رفضت الطلب وزارة الاتصالات وتكنولوجيا المعلومات.*
- *[...]*

متطلبات الامتثال

- *على جميع الجهات التي تنطبق عليها هذه السياسة أن تضمن امتثالها الكامل للأحكام الواردة في هذه السياسة.*
- *يجوز لـ [اسم الجهة] إجراء مراجعات دورية لمتابعة تطبيق هذه السياسة والامتثال لها.*
- *إذا تبين لـ[اسم الجهة] أن الجهات المعنية يمارسون أنشطة مخالفة لمتطلبات الامتثال، فلها أن تفرض غرامات إدارية، أو تنهي عقد/اتفاقية العمل، أو تتخذ الإجراءات القانونية اللازمة وفقًا للقوانين واللوائح المعمول في دولة قطر، وذلك بناءً على مدى خطورة الانتهاك ومدته.*

الوثائق المرتبطة / المراجع

- *[...]*

2.9 سياسة الاتصالات المحلية

رقم إصدار السياسة:	*[... 1.0...]*	**عنوان السياسة:**	*[...]*
تاريخ الإصدار:	*[...]*	**تاريخ المراجعة:**	*[...]*
المسؤول عن السياسة/الإدارة:	*[...]*	**اسم معد السياسة:**	*[...]*

مقدمة

تنص سياسة الاتصالات المحلية على الإجراءات التي ينبغي لموظفي [اسم الجهة] اتباعها عند التعامل مع الاتصالات الداخلية عبر أنظمة الشبكات لدى [اسم الجهة]، فضلًا عن طرق تبادل المعلومات داخل الجهة. وتهدف هذه السياسة إلى ضمان التوافق الكامل مع المبادئ الموضحة في سياسة تصنيف البيانات الوطنية. [...]

التعاريف

- *[...]*

الغرض من السياسة وأهدافها

تتمثل أهداف هذه السياسة فيما يلي:

- *تحديد قنوات الاتصال المختلفة المستخدمة داخل [اسم الجهة]، بالإضافة إلى أدوار ومسؤوليات الموظفين في الوصول إليها.*
- *[...]*

نطاق السياسة وتطبيقها

تنطبق هذه السياسة على جميع موظفي [اسم الجهة] الذين يتواصلون فيما بينهم من خلال قنوات الاتصال وأجهزة تكنولوجيا المعلومات الخاصة بـ[اسم الجهة].

بنود السياسة وأحكامها

يجب أن تتوافق جميع إجراءات الاتصالات المحلية داخل [اسم الجهة] مع القوانين واللوائح المعمول بها في دولة قطر، (بما في ذلك اسم القانون/اللائحة، واسم القانون/اللائحة، ...].

فيما يلي قنوات الاتصالات المحلية التي يتم التعامل معها ضمن نطاق هذه السياسة:

- *منصة البريد الإلكتروني ومساحات العمل التعاونية الخاصة بـ [اسم الجهة]*
- *بوابة الإنترنت الخاصة بـ[اسم الجهة].*
- *هواتف [اسم الجهة].*
- *أدوات الرسائل النصية الرسمية التي تستخدمها [اسم الجهة].*
- *[...]*

فيما يلي مبادئ وإجراءات التواصل من خلال قنوات الاتصالات المشمولة ضمن هذه السياسة:

- *يجب أن تتسم جميع رسائل التواصل بالدقة والإيجاز واللباقة، وأن تكون مصاغة بلغة مهنية تتوافق مع مبادئ [اسم الجهة].*
- *يتعين على الموظفين تحديد قناة الاتصال المناسبة وفقاً لنوع الرسالة ودرجة أهميتها.*
- *لا يجوز تبادل المواد الحساسة إلا عبر الوسائل الآمنة (مثل رسائل البريد الإلكتروني المشفرة)، وأن يكون الوصول إليها مقصورًا على الأفراد المصرح لهم.*
- *[...]*

متطلبات الامتثال

- *على جميع الجهات التي تنطبق عليها هذه السياسة أن تضمن امتثالها الكامل للأحكام الواردة في هذه السياسة.*
- *يجوز لـ [اسم الجهة] إجراء مراجعات دورية لمتابعة تطبيق هذه السياسة والامتثال لها.*
- إذا تبين لـ[اسم الجهة] أن الجهات المعنية يمارسون أنشطة مخالفة لمتطلبات الامتثال، فلها أن تفرض غرامات إدارية، أو تنهي عقد/اتفاقية العمل، أو تتخذ الإجراءات القانونية اللازمة وفقًا للقوانين واللوائح المعمول في دولة قطر، وذلك بناءً على مدى خطورة الانتهاك ومدته.

الوثائق المرتبطة / المراجع

- *[...]*

2.10 سياسة أمن الشبكات

رقم إصدار السياسة:	*[... 1.0...]*	**عنوان السياسة:**	*[...]*
تاريخ الإصدار:	*[...]*	**تاريخ المراجعة:**	*[...]*
المسؤول عن السياسة/الإدارة:	*[...]*	**اسم معد السياسة:**	*[...]*

مقدمة

تنص سياسة أمن الشبكات على الإجراءات الواجب اتباعها لمراقبة أنظمة تكنولوجيا المعلومات والشبكات التابعة لـ[اسم الجهة] بشكل دوري. وتهدف هذه السياسة إلى ضمان أمن البيانات وسلامتها وتوافرها، وذلك من خلال تزويد أنظمة تكنولوجيا المعلومات والشبكات الخاصة بـ[اسم الجهة] بالبرامج والأجهزة وإجراءات التدقيق المناسبة. [...]

التعاريف

- *[...]*

الغرض من السياسة وأهدافها

تتمثل أهداف هذه السياسة فيما يلي:

- *حماية أمن شبكة الجهة الحكومية بأكملها (بما في ذلك الشبكات السحابية المستخدمة) من خلال ضمان السرية والنزاهة والتوفّر.*
- *[...]*

نطاق السياسة وتطبيقها

تنطبق هذه السياسة على جميع موظفي [اسم الجهة] ووكلائها ومتعهديها والأطراف الثالثة التي تتعامل مع الشبكة الحكومية أو داخلها.

بنود السياسة وأحكامها

يجب أن تتوافق جميع إجراءات أمن الشبكات داخل [اسم الجهة] مع القوانين واللوائح المعمول بها في دولة قطر، (بما في ذلك اسم القانون/اللائحة، واسم القانون/اللائحة، ...].

تتضمن قواعد الأمن المادي والبيئي داخل [اسم الجهة] ما يلي، على سبيل المثال لا الحصر:

- *ينبغي أن يكون الوصول المادي إلى معدات الشبكات مقيدًا باستخدام آليات آمنة (على سبيل المثال، سجلات الوصول الخاضع للمراقبة).*
- *من الضروري تطبيق ضوابط بيئية تضمن الحفاظ على درجة الحرارة والرطوبة المناسبة في غرف الشبكات من أجل تجنب حدوث أعطال في المعدات.*
- *[...]*

فيما يلي متطلبات أمن الشبكات داخل [اسم الجهة]:

- *متطلبات أمن أجهزة التوجيه والمحولات:*
  - *[...]*
- *متطلبات أمن الاتصال اللاسلكي:*
  - *[...]*
- *متطلبات أمن الشبكة الافتراضية الخاصة (VPN):*
  - *[...]*
- *متطلبات أمن جدار الحماية:*
  - *[...]*

متطلبات الامتثال

- *على جميع الجهات التي تنطبق عليها هذه السياسة أن تضمن امتثالها الكامل للأحكام الواردة في هذه السياسة.*
- *يجوز لـ [اسم الجهة] إجراء مراجعات دورية لمتابعة تطبيق هذه السياسة والامتثال لها.*
- *إذا تبين لـ[اسم الجهة] أن الجهات المعنية يمارسون أنشطة مخالفة لمتطلبات الامتثال، فلها أن تفرض غرامات إدارية، أو تنهي عقد/اتفاقية العمل، أو تتخذ الإجراءات القانونية اللازمة وفقًا للقوانين واللوائح المعمول في دولة قطر، وذلك بناءً على مدى خطورة الانتهاك ومدته.*

الوثائق المرتبطة / المراجع

- *[...]*

2.11 سياسة الأمن المادي والبيئي

رقم إصدار السياسة:	*[... 1.0...]*	**عنوان السياسة:**	*[...]*
تاريخ الإصدار:	*[...]*	**تاريخ المراجعة:**	*[...]*
المسؤول عن السياسة/الإدارة:	*[...]*	**اسم معد السياسة:**	*[...]*

مقدمة

تنص سياسة الأمن المادي والبيئي على الإجراءات التي يجب على موظفي [اسم الجهة] اتباعها عند استخدام معدات تكنولوجيا المعلومات الخاصة بـ [اسم الجهة]. وتهدف هذه السياسة إلى ضمان الحماية الكاملة لمعلومات [اسم الجهة] ومواردها ومقراتها من الأضرار المحتملة أو التلف أو الحذف. [...]

التعاريف

- *[...]*

الغرض من السياسة وأهدافها

تتمثل أهداف هذه السياسة فيما يلي:

- *صيانة أصول وأنظمة المعلومات من الوصول غير القانوني وحمايتها من المخاطر البيئية، وذلك من خلال تطبيق قيود مادية وبيئية.*
- *[...]*

نطاق السياسة وتطبيقها

تنطبق هذه السياسة على جميع موظفي [اسم الجهة] ووكلائها ومتعهديها وأي شخص آخر لديه إمكانية الوصول إلى أي من معدات تكنولوجيا المعلومات المادية للجهة.

بنود السياسة وأحكامها

فيما يلي فئات معدات تكنولوجيا المعلومات التي تستخدمها [اسم الجهة] في أعمالها، سواء كانت موجودة داخل مقراتها أو خارجها، وذلك ضمن نطاق هذه السياسة:

- *أنظمة الحوسبة مثل:*
  - *أجهزة الكمبيوتر الشخصية*
  - *الشاشات*
  - *أجهزة الكمبيوتر المتنقلة*
  - *[...]*

- *البنية التحتية للبوابة مثل:*
  - *جدران الحماية*
  - *أجهزة التوجيه*
  - *المحولات*
  - *[...]*
- *[...]*

فيما يلي التدابير الأمنية المحددة لجميع معدات تكنولوجيا المعلومات الخاصة بـ [اسم الجهة]، والتي تندرج ضمن نطاق هذه السياسة:

- *تتضمن التدابير الأمنية المحددة لأنظمة الحوسبة ما يلي:*
  - *[...]*
- *تتضمن التدابير الأمنية المحددة للبنية التحتية للبوابة ما يلي:*
  - *[...]*
- *[...]*

فيما يلي صلاحيات النفاذ المحددة إلى معدات تكنولوجيا المعلومات للموظفين الخارجيين والمؤقتين وكذلك المسؤولين عن الصيانة الذين لديهم حق الوصول إلى مقرات [اسم الجهة]، بناءً على متطلبات المهام ومستوى التصريح الأمني للموظف، وذلك ضمن نطاق هذه السياسة:

- *تشمل صلاحيات النفاذ المحددة إلى معدات تكنولوجيا المعلومات الخاصة بأنظمة الحوسبة ما يلي:*
  - *[...]*
- *تشمل صلاحيات النفاذ المحددة إلى معدات تكنولوجيا المعلومات الخاصة بالبنية التحتية للبوابة ما يلي:*
  - *[...]*
- *[...]*

متطلبات الامتثال

- *على جميع الجهات التي تنطبق عليها هذه السياسة أن تضمن امتثالها الكامل للأحكام الواردة في هذه السياسة.*
- *يجوز لـ [اسم الجهة] إجراء مراجعات دورية لمتابعة تطبيق هذه السياسة والامتثال لها.*
- *إذا تبين لـ[اسم الجهة] أن الجهات المعنية يمارسون أنشطة مخالفة لمتطلبات الامتثال، فلها أن تفرض غرامات إدارية، أو تنهي عقد/اتفاقية العمل، أو تتخذ الإجراءات القانونية اللازمة وفقًا للقوانين واللوائح المعمول في دولة قطر، وذلك بناءً على مدى خطورة الانتهاك ومدته.*

الوثائق المرتبطة / المراجع

- *[...]*

2.12 سياسة النفاذ عن بُعد

رقم إصدار السياسة:	*[... 1.0...]*	**عنوان السياسة:**	*[...]*
تاريخ الإصدار:	*[...]*	**تاريخ المراجعة:**	*[...]*
المسؤول عن السياسة/الإدارة:	*[...]*	**اسم معد السياسة:**	*[...]*

مقدمة

تنص سياسة النفاذ عن بُعد على الإجراءات الخاصة بالنفاذ إلى موارد الشبكات الداخلية (الإنترانت) لدى [اسم الجهة]، بالإضافة إلى متطلبات تشفير الأقراص والنفاذ إلى الشبكة الافتراضية الخاصة (VPN)، [...]. تهدف هذه السياسة إلى ضمان تقليل الأضرار المحتملة الناجمة عن الاستخدام غير المصرح به لموارد [اسم الجهة]. [...]

التعاريف

- *[...]*

الغرض من السياسة وأهدافها

تتمثل أهداف هذه السياسة فيما يلي:

- *وضع إرشادات وشروط للاتصال من أي مضيف (أي أجهزة الكمبيوتر المتنقلة والأجهزة اللوحية والهواتف المتنقلة) إلى شبكة [اسم الجهة].*
- *[...]*

نطاق السياسة وتطبيقها

تنطبق هذه السياسة على جميع موظفي الجهة ووكلائها ومتعهديها الذين يستخدمون معدات [اسم الجهة] ويقومون بالنفاذ عن بُعد إلى أنظمة المعلومات الحكومية ونشرها وإدارتها.

بنود السياسة وأحكامها

فيما يلي الأجهزة المؤهلة للنفاذ عن بُعد التي تندرج ضمن نطاق هذه السياسة:

- *الأجهزة التي تملكها [اسم الجهة]، بما في ذلك أجهزة الكمبيوتر المتنقلة والشاشات والأجهزة اللوحية التي توفرها [اسم الجهة].*
- *الأجهزة الشخصية المعتمدة من قبل [اسم الجهة] للنفاذ عن بُعد التي تتوافق مع المعايير الأمنية والأحكام المنصوص عليها في سياسة استخدام الأجهزة الشخصية في العمل[3].*
- *الأجهزة المملوكة للوكلاء أو المتعهدين التي لا يمكن النفاذ إليها إلا في ظل ظروف معينة ووفقًا لتدابير أمنية صارمة.*

[3] https://qcert.ncsa.gov.qa/sites/default/files/public/documents/cs-csps_byod_policy_v1.1.pdf

- *[...]*

فيما يلي أنواع أنظمة تكنولوجيا المعلومات التي تتيح النفاذ عن بُعد والتي تندرج ضمن نطاق هذه السياسة:

- *منصة البريد الإلكتروني ومساحات العمل التعاونية الخاصة بـ [اسم الجهة]*
- *تطبيقات داخلية محددة بناءً على الأدوار الوظيفية والاحتياجات.*
- *يمنح مالك البيانات حق النفاذ إلى الملفات والمستندات المخزنة.*
- *[...]*

فيما يلي متطلبات استخدام الشبكة الافتراضية الخاصة في إطار هذه السياسة:

- *يجب إجراء النفاذ عن بُعد باستخدام الشبكة الافتراضية الخاصة المعتمدة لدى [اسم الجهة].*
- *يتطلب النفاذ إلى الشبكة الافتراضية الخاصة مصادقة متعددة العوامل.*
- *[...]*

متطلبات الامتثال

- *على جميع الجهات التي تنطبق عليها هذه السياسة أن تضمن امتثالها الكامل للأحكام الواردة في هذه السياسة.*
- *يجوز لـ [اسم الجهة] إجراء مراجعات دورية لمتابعة تطبيق هذه السياسة والامتثال لها.*
- *إذا تبين لـ[اسم الجهة] أن الجهات المعنية يمارسون أنشطة مخالفة لمتطلبات الامتثال، فلها أن تفرض غرامات إدارية، أو تنهي عقد/اتفاقية العمل، أو تتخذ الإجراءات القانونية اللازمة وفقًا للقوانين واللوائح المعمول في دولة قطر، وذلك بناءً على مدى خطورة الانتهاك ومدته.*

الوثائق المرتبطة / المراجع

- *[...]*

الملحق 3: تقارير اعتماد السياسات

يعرض هذا القسم أمثلة على المعلومات التي قد تطلبها وزارة الاتصالات وتكنولوجيا المعلومات لتحديد ما إذا كان قد تم اتخاذ الإجراءات المناسبة لاعتماد هذه السياسة. ستشمل المعلومات المطلوبة، على سبيل المثال لا الحصر، ما يلي:

قائمة المراجعة للحد الأدنى المطلوب من سياسات تكنولوجيا المعلومات الداخلية لسياسة الجهات الحكومية	*الإجابة*
سياسة الاستخدام المقبول	
هل اعتمدت الجهة سياسة من هذا القبيل؟	☐ نعم ☐ لا
إذا كانت الإجابة "نعم" على السؤال السابق، فهل تلبي السياسة المعنية الحد الأدنى من المتطلبات المحددة في الملحق 1 من هذه السياسة؟	☐ نعم ☐ لا ☐ لا ينطبق
في حال كانت الإجابة "لا" على السؤال السابق، فيرجى ذكر المتطلبات الناقصة: • XXX	
سياسة المصادقة على النفاذ وتوثيقه	
هل اعتمدت الجهة سياسة من هذا القبيل؟	☐ نعم ☐ لا
إذا كانت الإجابة "نعم" على السؤال السابق، فهل تلبي السياسة المعنية الحد الأدنى من المتطلبات المحددة في الملحق 1 من هذه السياسة؟	☐ نعم ☐ لا ☐ لا ينطبق
في حال كانت الإجابة "لا" على السؤال السابق، فيرجى ذكر المتطلبات الناقصة: • XXX	
سياسة النسخ الاحتياطي للبيانات واستعادتها	
هل اعتمدت الجهة سياسة من هذا القبيل؟	☐ نعم ☐ لا
إذا كانت الإجابة "نعم" على السؤال السابق، فهل تلبي السياسة المعنية الحد الأدنى من المتطلبات المحددة في الملحق 1 من هذه السياسة؟	☐ نعم ☐ لا ☐ لا ينطبق
في حال كانت الإجابة "لا" على السؤال السابق، فيرجى ذكر المتطلبات الناقصة: • XXX	

قائمة المراجعة للحد الأدنى المطلوب من سياسات تكنولوجيا المعلومات الداخلية لسياسة الجهات الحكومية	*الإجابة*
سياسة تصنيف البيانات	
هل اعتمدت الجهة سياسة من هذا القبيل؟	☐ نعم ☐ لا
إذا كانت الإجابة "نعم" على السؤال السابق، فهل تلبي السياسة المعنية الحد الأدنى من المتطلبات المحددة في الملحق 1 من هذه السياسة؟	☐ نعم ☐ لا ☐ لا ينطبق
في حال كانت الإجابة "لا" على السؤال السابق، فيرجى ذكر المتطلبات الناقصة: • XXX	
سياسة خصوصية البيانات	
هل اعتمدت الجهة سياسة من هذا القبيل؟	☐ نعم ☐ لا
إذا كانت الإجابة "نعم" على السؤال السابق، فهل تلبي السياسة المعنية الحد الأدنى من المتطلبات المحددة في الملحق 1 من هذه السياسة؟	☐ نعم ☐ لا ☐ لا ينطبق
في حال كانت الإجابة "لا" على السؤال السابق، فيرجى ذكر المتطلبات الناقصة: • XXX	
سياسة البريد الإلكتروني	
هل اعتمدت الجهة سياسة من هذا القبيل؟	☐ نعم ☐ لا
إذا كانت الإجابة "نعم" على السؤال السابق، فهل تلبي السياسة المعنية الحد الأدنى من المتطلبات المحددة في الملحق 1 من هذه السياسة؟	☐ نعم ☐ لا ☐ لا ينطبق
في حال كانت الإجابة "لا" على السؤال السابق، فيرجى ذكر المتطلبات الناقصة: • XXX	
سياسة إدارة أصول تكنولوجيا المعلومات	
هل اعتمدت الجهة سياسة من هذا القبيل؟	☐ نعم ☐ لا
إذا كانت الإجابة "نعم" على السؤال السابق، فهل تلبي السياسة المعنية الحد الأدنى من المتطلبات المحددة في الملحق 1 من هذه السياسة؟	☐ نعم ☐ لا ☐ لا ينطبق

قائمة المراجعة للحد الأدنى المطلوب من سياسات تكنولوجيا المعلومات الداخلية لسياسة الجهات الحكومية	الإجابة
في حال كانت الإجابة "لا" على السؤال السابق، فيرجى ذكر المتطلبات الناقصة: • XXX	
سياسة إدارة التغيير في تكنولوجيا المعلومات	
هل اعتمدت الجهة سياسة من هذا القبيل؟	☐ نعم ☐ لا
إذا كانت الإجابة "نعم" على السؤال السابق، فهل تلبي السياسة المعنية الحد الأدنى من المتطلبات المحددة في الملحق 1 من هذه السياسة؟	☐ نعم ☐ لا ☐ لا ينطبق
في حال كانت الإجابة "لا" على السؤال السابق، فيرجى ذكر المتطلبات الناقصة: • XXX	
سياسة الاتصالات المحلية	
هل اعتمدت الجهة سياسة من هذا القبيل؟	☐ نعم ☐ لا
إذا كانت الإجابة "نعم" على السؤال السابق، فهل تلبي السياسة المعنية الحد الأدنى من المتطلبات المحددة في الملحق 1 من هذه السياسة؟	☐ نعم ☐ لا ☐ لا ينطبق
في حال كانت الإجابة "لا" على السؤال السابق، فيرجى ذكر المتطلبات الناقصة: • XXX	
سياسة أمن الشبكات	
هل اعتمدت الجهة سياسة من هذا القبيل؟	☐ نعم ☐ لا
إذا كانت الإجابة "نعم" على السؤال السابق، فهل تلبي السياسة المعنية الحد الأدنى من المتطلبات المحددة في الملحق 1 من هذه السياسة؟	☐ نعم ☐ لا ☐ لا ينطبق
في حال كانت الإجابة "لا" على السؤال السابق، فيرجى ذكر المتطلبات الناقصة: • XXX	
سياسة الأمن المادي والبيئي	
هل اعتمدت الجهة سياسة من هذا القبيل؟	☐ نعم ☐ لا

قائمة المراجعة للحد الأدنى المطلوب من سياسات تكنولوجيا المعلومات الداخلية لسياسة الجهات الحكومية	*الإجابة*
إذا كانت الإجابة "نعم" على السؤال السابق، فهل تلبي السياسة المعنية الحد الأدنى من المتطلبات المحددة في الملحق 1 من هذه السياسة؟	☐ نعم ☐ لا ☐ لا ينطبق
في حال كانت الإجابة "لا" على السؤال السابق، فيرجى ذكر المتطلبات الناقصة: • XXX	
سياسة النفاذ عن بُعد	
هل اعتمدت الجهة سياسة من هذا القبيل؟	☐ نعم ☐ لا
إذا كانت الإجابة "نعم" على السؤال السابق، فهل تلبي السياسة المعنية الحد الأدنى من المتطلبات المحددة في الملحق 1 من هذه السياسة؟	☐ نعم ☐ لا ☐ لا ينطبق
في حال كانت الإجابة "لا" على السؤال السابق، فيرجى ذكر المتطلبات الناقصة: • XXX	

مراقبة الوثيقة

النسخة	التاريخ	التعديلات	المؤلّف
1.0.0	2025\03\01	إصدار السياسة	وزارة الاتصالات وتكنولوجيا المعلومات

تم إعدادها من قبل
إدارة سياسات ومعايير الحكومة الرقمية
وزارة الاتصالات وتكنولوجيا المعلومات
النسخة 1.0.0 لسنة 2025

البريد الإلكتروني: policy@mcit.gov.qa
www.mcit.gov.qa