وزارة الصحة
Ministry of Health

سياسة الاستخدام المقبول

المشاركة	الأخضر
التصنيف	معلومات عامة
الرقم	CSMS_Policy_01
الحالة	نهائي
النسخة	2.0
التاريخ	٢٠٢٠/١١/٠١
عدد الصفحات	١٣
الجهة المسؤولة	الإدارة العامة للأمن السيبراني
اسم الملف	سياسة الاستخدام المقبول – نهائية 2.0

وزارة الصحة
Ministry of Health

المشاركة والتصنيف

المشاركة	**اللون الأخضر:** مشاركة المعلومات داخل الإدارة أو المجموعة التابعة لوزارة الصحة وبإمكان الشخص المستلم مشاركة المعلومات مع الأطراف خارج وزارة الصحة والذين وقعوا على اتفاقية عدم إفصاح عن المعلومات. مع ذلك، لا يسمح بتبادل هذه المعلومات أو نشرها عبر القنوات العامة.
التصنيف	**معلومات عامة:** لا يؤدي الإفصاح عن المعلومات إلى التسبب بأي ضرر.

تاريخ المراجعة

النسخة	التاريخ	المؤلف	ملخص التعديلات
١,٠	٢٠٢٠/٠٣/٠٣	إدارة الأمن السيبراني	إعداد الهيكل التنظيمي والبنود التفصيلية للسياسة
١,١	٢٠٢٠/٠٣/١٨	إدارة الأمن السيبراني	١. تعديل صياغة السياسة الأولية ٢. تطبيق ملاحظات المدير العام للأمن السيبراني
١,٢	٢٠٢٠/٠٣/٢٥	إدارة الأمن السيبراني	تحديث تفاصيل البريد الإلكتروني المذكورة في القسم ٩
٢,٠	٢٠٢٠/٠٦/٢٥	إدارة الأمن السيبراني	النسخة النهائية (يونيو ٢٠٢٠)

النشر

الاسم والعنوان	القناة
الصحة الإلكترونية	البريد الإلكتروني.
الشؤون القانونية	البريد الإلكتروني.
الموارد البشرية	البريد الإلكتروني او داخلي.

الموافقات

الاسم	المنصب	التوقيع	التاريخ
عبدالله بن عبدالرحمن العيد	إدارة وحوكمة الأمن السيبراني		٢٠ ذو الحجة, ١٤٤١ - ١٠ اغسطس ٢٠٢٠م
باسم بن عبدالله العنقري	مدير عام الإدارة العامة للأمن السيبراني		٢٠ ذو الحجة, ١٤٤١ - ١٠ اغسطس ٢٠٢٠م
اللجنة الاستشارية للأمن السيبراني			٢٠ ذو الحجة, ١٤٤١ - ١٠ اغسطس ٢٠٢٠م

وزارة الصحة
Ministry of Health

قائمة المحتويات

١. المقدمة

تدركُ وزارة الصحة أهمية إدارة مواردها ومعلوماتها بفعالية وكفاءة وأمان لتحقيق أهداف العمل الخاصة بها. تعتبر مراقبة وإدارة موارد معلومات وزارة الصحة بشكل فعال أمرًا ضروريًا لعمليات الأعمال ولتمكين وزارة الصحة من التخفيف من حدة المخاطر على نحوٍ كافٍ.

لم يكن هدف إدارة الأمن السيبراني من نشر سياسة الاستخدام المقبول أن تفرض قيود تتعارض مع ثقافة وزارة الصحة التي أساسها الثقة والنزاهة. تلتزم إدارة الأمن السيبراني بحماية موظفي وزارة الصحة وشركائها والشركة من الأعمال غير القانونية أو المُضرَّة التي يقوم الأشخاص سواءً عن قصد أو دون قصد. إنَّ الأنظمة المتصلة بشبكة الإنترنت والشبكة الداخلية (الإنترانت) والشبكة الخارجية (الإكسترانت)، وتشمل على سبيل المثال لا الحصر: المعدات والبرمجيات الحاسوبية، وأنظمة التشغيل، ووسائط التخزين، وحسابات الشبكة التي تتيح الدخول إلى البريد الإلكتروني وتصفح شبكة الإنترنت العالمية وبروتوكول نقل الملفات جميعها مملوكة لوزارة الصحة.

تُستخدم هذه الأنظمة لأغراض العمل ولخدمة مصالح وزارة الصحة ولتسيير احتياجات أعمالها. يُعد ضمان أمن المعلومات جهدًا جماعيًا ينطوي على مشاركة جميع الموظفين والمنتسبين الذين يتعاملون بالمعلومات و/أو أنظمة المعلومات. وعليه، فإنَّ من مسؤولية كافة مستخدمي المعلومات وأنظمة المعلومات معرفة تفاصيل هذه السياسة وفهمها والالتزام ببنودها والتقيد بها في أعمالهم.

١,١ الغرض

تُحدد هذه السياسة الاستخدام المقبول لموارد و/أو أصول معلومات وزارة الصحة. هذه القواعد موجودة لحماية المستخدمين (بما في ذلك: الموظفين، والمقاولين، وغيرهم) ووزارة الصحة. يمكن أن يُعرِّض الاستخدام غير المناسب وزارة الصحة للمخاطر، وتشمل: هجمات الفيروسات، وتعريض الأنظمة الشبكية والخدمات للخطر، وإلى تحمل التبعات القانونية.

١,٢ نطاق التطبيق

تنطبق هذه السياسة على جميع المستخدمين في مجال العمل، بما في ذلك: الموظفين، والأطراف الخارجية، والموردين، والشركاء الذين يستخدمون و/أو يتعاملون مع أصول المعلومات المملوكة لوزارة الصحة.

٢. الأدوار والمسؤوليات

فيما يلي الأدوار والمسؤوليات ذات الصلة بهذه السياسة:

- **اللجنة الاستشارية للأمن السيبراني**
  - الجهة المسؤولة عن اتخاذ القرارات النهائية المتعلقة بتوضيح هذه السياسة.
  - مراجعة واعتماد السياسة.
  - مراجعة المخالفات الرئيسية لهذه السياسة.
- **مستخدمو العمل وجميع الوحدات الإدارية وموظفيها في وزارة الصحة، بما في ذلك الأطراف الخارجية والشركاء.**
  - الالتزام بالسياسة وضمان التزام الموظفين والمتعاقدين والشركاء ومقدمي الخدمات كل ضمن اختصاصه.
- **إدارة الأمن السيبراني**
  - تحمل مسؤولية السياسة وتحديثها وتوزيعها على العموم.
  - إدارة الاستثناءات والمخالفات ذات الصلة بالسياسة.
  - ضمان الالتزام بالسياسة داخل وزارة الصحة.

٣. السياسة

٣,١ الاستخدام المقبول

يهدف هذا القسم إلى إبراز المسؤوليات التي تقع على عاتق المستخدم عند استخدام موارد معلومات وزارة الصحة وأصولها.

٣,١,١ تم تزويد المستخدم بأصول معلومات وزارة الصحة لأغراض متعلقة بالوظيفة ويتم منح الامتيازات الضرورية المتعلقة بالنظام عندما يكون هناك احتياجات مشروعة متعلقة بالعمل.

٣,١,٢ لا تسمح وزارة الصحة باستخدام معلوماتها المتعلقة بالعمل وأصولها التقنية لأغراض شخصية، بما في ذلك تخزين البيانات الشخصية.

٣,١,٣ ينبغي على المستخدم عدم الكشف عن معلومات حسابه لأي شخص.

٣,١,٤ يتحمل المستخدم مسؤولية الحفاظ على سرية معلومات وزارة الصحة وأصولها التقنية وفق السياسات والمتطلبات الحالية للأمن السيبراني.

٣,١,٥ سيقتصر وصول واستخدام المستخدم على الأنظمة المصرَّح له باستخدامها.

٣,١,٦ يتعين على المستخدم عدم تعطيل أي خدمات أو أجهزة أو برامج مضادة للفيروسات أو جدران حماية مستخدمة في الحماية ومثبتة على مختلف الأصول التقنية المملوكة لوزارة الصحة وأجهزة المستخدمين المخصصة له.

٣,١,٧ يتعين على المستخدم عدم تخزين أو معالجة أو نقل المواد الإباحية على أي من أنظمة معلومات وزارة الصحة.

٣,١,٨ يتعين على المستخدم عدم نسخ أو تبادل أي معلومات سرية بأي وسيلة، بما في ذلك على سبيل المثال لا الحصر: الأقراص المدمجة ووحدات التخزين المتنقلة ومرفقات رسائل البريد الإلكتروني وغيرها إلاَّ إذا حصل على تصريح بذلك لأغراض رسمية.

٣,١,٩ ينبغي على المستخدم عدم التقاط صور للمعلومات التي خضعت للمعالجة، مثل: السجلات الصحية، باستخدام أجهزة الكاميرا أو كاميرات الهواتف المحمولة دون الحصول على الموافقة المناسبة.

٣,١,١٠ تظل أي برمجيات حاسوبية طورها موظفو وزارة الصحة ضمن نطاق وظيفتهم "ملكية فكرية" للوزارة.

٣,١,١١ تحتفظ وزارة الصحة بالحق في إجراء المراجعة بصفة دورية لضمان الالتزام بهذه السياسة.

٣,٢ استخدام الإنترنت

يهدف هذا القسم إلى إبراز مسؤوليات المستخدم عند تصفح أصول معلومات وزارة الصحة على شبكة الإنترنت.

٣,٢,١ يجب على المستخدم استخدام شبكة الإنترنت لتنفيذ أنشطة العمل في وزارة الصحة بطريقة مريحة ومتسمة بالكفاءة.

٣,٢,٢ يتعين على المستخدم عدم ربط أي جهاز أو أصل معلومات خاص بوزارة الصحة بشبكة الإنترنت إلاَّ بعد الحصول على الموافقة اللازمة من إدارة الأمن السيبراني.

٣,٢,٣ تعود ملكية جميع مصادر المعلومات والمعدات إلى وزارة الصحة. وعليه، يمكن أن تثبت وزارة الصحة برمجية أو تركيب معدات لمراقبة جميع المعلومات والأصول التقنية وحفظ سجل يتعلق بها وحمايتها عندما يستخدمها المستخدم، بما في ذلك: زيارات البريد الإلكتروني والموقع الإلكتروني وتحتفظ وزارة الصحة بحق حفظ سجل بالملفات المخزَّنة على أنظمتها وأصولها وتفتيشها.

٣,٢,٤ يتعين على المستخدم احترام العملاء وعدم استخدام أو تحميل أو نشر أو مشاركة أو إرسال أو تصفح أو تحميل أي محتوى يضم إهانات عرقية أو ملاحظات تمييزية أو إهانات شخصية أو محتوى يخدش الحياء أو يمثل اهتمامات سياسية أو دينية معينة. كما لا يُسمح لهم بالمشاركة في أي سلوك غير مقبول أو غير مناسب وفق مبادئ وزارة الصحة.

٣,٢,٥ تحتفظ وزارة الصحة بحق تهيئة متصفحات الويب لحفظ ملفات تعريف الارتباط لتوفير قائمة بجميع المواقع الإلكترونية التي زارها المستخدمون.

٣,٢,٦ تحتفظ وزارة الصحة بالحق في فحص ما يلي:

- ملفات التخزين المؤقت في متصفح الويب.
- قائمة المواقع المفضلة وملفات تعريف الارتباط على متصفح الويب.
- الملفات المؤقتة.
- ملفات التنزيلات.
- سجلات مواقع الويب التي زارها المستخدم.

٣,٢,٧ تحتفظ وزارة الصحة بحق فحص سجلات المراسلات ذات الصلة للتحقق من التزام المستخدم بالسياسات الداخلية ومساعدة وزارة الصحة في إجراء التحقيقات الداخلية إذا لَزِمَ الأمر في مرحلة لاحقة.

٣,٢,٨ يتعين على المستخدم استخدام البرمجيات المعتمدة والمحددة للدخول إلى شبكة الإنترنت العالمية لضمان تنفيذ كافة المعالجات الأمنية المعتمدة.

٣,٢,٩ يتعين على المستخدم عدم تحميل أو تثبيت أي برامج أو أنظمة ملحقة، مثل: ActiveX control أو Java scripts، مطلوبة لتصفح أي مواقع يزورها المستخدم. وفي حال كان عمله يتطلب تثبيت هذه البرامج أو الأنظمة الملحقة، فيجب على المستخدم طلب المساعدة من مكتب دعم تكنولوجيا المعلومات.

٣,٢,١٠ يتعين على المستخدم عدم تخزين أو معالجة المعلومات أو الوثائق الحساسة أو السرية أو الخاصة على الأنظمة المرتبطة بشبكة الإنترنت إلاَّ بعد الحصول على موافقة خطية إدارة الأمن السيبراني في الوزارة. بالإضافة إلى ذلك، تحتفظ وزارة الصحة بحق حماية حقوقها في الوصول إلى المعلومات.

٣,٢,١١ يتعين على المستخدم الحصول على الموافقة اللازمة من إدارة العلاقات العامة في الوزارة (الناطق الرسمي المُعيَّن) قبل نشر أي معلومات أو وثائق حول الوزارة على شبكة الإنترنت أو شبكات التواصل الاجتماعي.

٣,٢,١٢ يتعين على المستخدم عدم نشر المعلومات المتعلقة بأعمال الوزارة، وتشمل على سبيل المثال لا الحصر: المعلومات الصحية المحمية إلكترونيًا، والعقود، وأوامر الشراء إلاَّ بعد التحقق من هوية ومصداقية الشخص أو المؤسسة التي طلبتها.

٣,٢,١٣ يتعين على المستخدم تحديد مصدر المعلومات التي حصل عليها من شبكة الإنترنت بعناية لضمان موثوقيتها.

٣,٢,١٤ يتعين على المستخدم عدم تعطيل أو منع المسح التلقائي للملفات التي تم تحميلها من شبكة الإنترنت للكشف عن الفيروسات باستخدام البرمجية المعتمدة للكشف عن الفيروسات.

٣,٢,١٥ تطبق وتتقيد وزارة الصحة بشكل تام باتفاقيات الترخيص المبرمة مع موردي البرمجيات على النحو المحدد في سياسة وزارة الصحة بشأن أمن البرمجيات. وعليه، يتعين على المستخدم عدم تنزيل البرامج غير المصرَّح بها من شبكة الإنترنت، مثل: البرمجيات التجريبية والبرمجيات المجانية، بصورة تتوافق مع رخصة المورد أو إلاَّ بعد حصوله على موافقة خطية من إدارة الأمن السيبراني.

٣,٢,١٦ يتعين على المستخدم الإبلاغ فورًا من خلال القناة المعتمدة للإبلاغ عن الحوادث إذا كان يشتبه بفقدان معلومات حساسة أو سرية و/أو خاصة أو الإفصاح عنها لأطراف غير مصرَّح لهم.

٣,٢,١٧ يتعين على المستخدم عدم تنفيذ أي فحص أمني أو اختبار أو حيازة أو استخدام أدوات لقرصنة رخص البرمجيات وكلمات المرور والأعمال المشابهة.

٣,٢,١٨ يتعين على المستخدم الاهتمام بالتحذيرات الأمنية التي يمكن أن تظهر عند تصفح المواقع على شبكة الإنترنت والتعامل مع كل رسالة بحذر.

٣,٣ استخدام مواقع التواصل الاجتماعي

يهدف هذا القسم إلى تسليط الضوء على مسؤوليات المستخدم عند تصفح مواقع التواصل الاجتماعي.

٣,٣,١ إنَّ موظفي وزارة الصحة هم سفراء التجارية للوزارة ويتحملون مسؤولية المحتوى الذي ينشرونه على مواقع التواصل الاجتماعي. يمكن أن يعتقد البعض أنّ المحتوى الذي ينشره موظفو وزارة الصحة بصفتهم الشخصية يمثل وجهة نظر الوزارة. لذلك، يجب على المستخدم ممارسة التقدير السليم عند استخدام مواقع التواصل الاجتماعي.

٣,٣,٢ ينبغي على المستخدم ضمان توافق ملفاتهم التعريفية والمحتوى المرتبط بها مع مدونة قواعد السلوك وسياسات وزارة الصحة عند التطرق إلى مواضيع متصلة بوزارة الصحة على مواقع التواصل الاجتماعي.

٣,٣,٣ تعتبر مواقع التواصل الاجتماعي منتديات عامة. وعليه، يتعين على المستخدم عدم القيام بما يلي:

- الإفصاح عن أي معلومات سرية أو شخصية أو خاصة.
- نشر مواضيع تُعتبر أو قد تُعتبر نوعًا من أنواع التهديد أو المضايقة أو التنمر أو التمييز ضد أي موظف أو متعاقد أو مقدم طلب أو مستفيد من وزارة الصحة، أو غير ذلك.
- نشر مقاطع فيديو و/أو صور للموظفين والمتعاقدين ومقدمي الطلبات والمستفيدين من وزارة الصحة وغيرهم، ما لم يصرح لهم بذلك رسميًا.
- نشر أي موضوع قد يتسبب بإلحاق الضرر بوزارة الصحة أو سمعة الدولة.

٣,٣,٤ لا يُسمح بربط المنشورات الشخصية على مواقع التواصل الاجتماعي بأي شكل من الأشكال (على سبيل المثال، بشكل مباشر أو غير مباشر أو قابل للربط أو مرتبط) مع المعلومات غير العامة المكتسبة من العمل لدى وزارة الصحة أو من الخدمات التي تقدمها.

٣,٣,٥ يجب على المستخدم الاهتمام بشكل كبير عند استخدام مواقع التواصل الاجتماعي بعدم الكشف عن نطاق مهام المؤلف أو أي شخص آخر في وزارة الصحة أو مستوى وضوح أو تفاصيل مجالات مسؤولياته أو الإشارة أو التلميح إليها.

٣,٣,٦ يُحظر تمامًا نشر أي نوع من المحتوى (مثل التسجيلات الصوتية ومقاطع الفيديو والموقع وأي نوع آخر من المواد) التي يتم التقاطها في مرافق وفعاليات وزارة الصحة على الحسابات الشخصية للموظفين.

٣,٣,٧ يُمنع منعًا باتًا استخدام الحسابات الرسمية لوزارة الصحة لأغراض شخصية تتمثل في تصفح مواقع التواصل الاجتماعي أو حضور المؤتمرات العامة أو الاستفادة من خدمات الإنترنت إلاَّ بعد الحصول على موافقة خطية من ممثلي الوزارة.

٣,٤ أمن الأصول المادية

يهدف هذا القسم إلى تسليط الضوء على مسؤوليات المستخدم بالالتزام في تطبيق ضوابط أمن الأصول المادية الخاصة بوزارة الصحة.

٣,٤,١ يتعين على المستخدم إظهار بطاقته التعريفية داخل مباني وزارة الصحة بصورة واضحة.

٣,٤,٢ يتعين على المستخدم الالتزام بمسافة الأمان في مباني وزارة الصحة والاهتمام بذلك.

٣,٤,٣ من مصلحة الجميع ضمان التطبيق الفعال لضوابط الوصول الفعلي إلى مباني وزارة الصحة. يجب أن يتعاون المستخدم ويلتزم بتدابير أمن الأصول المادية الخاصة بوزارة الصحة.

٣,٤,٤ يجب مراقبة الوصول إلى غرفة الحواسيب والمناطق المحظورة ويتعين على المستخدم التقيد بهذه الضوابط طوال الوقت.

٣,٤,٥ لا يُسمح للموظفين غير المُصرَّح لهم بالدخول إلى مباني وزارة الصحة ولا باستخدام أصولها التقنية. وعليه، يتعين على المستخدم التقيد بتطبيق تدابير مراقبة الوصول وعدم تسهيل أو المساعدة في ارتكاب المخالفات.

٣,٤,٦ يجب عدم نقل معلومات وزارة الصحة وأصولها التقنية خارج مبانيها إلاَّ بعد الحصول على الموافقة المطلوبة من المستوى القيادي المناسب و/أو الجهة المسؤولة.

٣,٤,٧ يتعين على المستخدم عدم إدخال أجهزة غير مأذون بها داخل مباني وزارة الصحة أو ربطها مع شبكة الوزارة إلاَّ بعد تبرير حاجة الأعمال إليها والحصول على الموافقة الخطية من إدارة الأمن السيبراني.

٣,٥ أمن المكاتب والحواسيب المحمولة والأجهزة المحمولة

يهدف هذا القسم إلى تسليط الضوء على مسؤوليات المستخدم عند استخدام مكاتب وزارة الصحة وحواسيبها المحمولة وأجهزتها المحمولة.

٣,٥,١ يُسمح للمستخدم فقط بالوصول إلى المكاتب والحواسيب المحمولة في المواقع المخصصة. يتعين على المستخدم عدم الوصول إلى المكاتب والحواسيب المحمولة الأخرى داخل مباني وزارة الصحة دون الحصول على موافقة مسبقة.

٣,٥,٢ يتعين على المستخدم إقفال حاسوبه خلال الاستراحات القصيرة أو إطفاء حاسوبه قبل مغادرة المكتب و/أو في نهاية كل يوم.

٣,٥,٣ يتعين على المستخدم حماية المعلومات الحساسة وتخزينها وحذفها وعدم تركها على مكتبه بمكان يتيح قراءتها أو نسخها أو تغييرها دون علم المستخدم.

٣,٥,٤ يتعين على المستخدم عدم تركيب أي معدات جديدة على الحواسيب المكتبية دون الحصول على التصريح المطلوب من إدارة الصحة الإلكترونية.

٣,٥,٥ يتعين على المستخدم عدم تثبيت أو استخدام البرمجيات غير القانونية و/أو المقرصنة على الجهاز الذي قدمته وزارة الصحة.

٣,٥,٦ يجب على المستخدم استخدام المعدات التي اشترتها ووافقت عليها وزارة الصحة لتسيير الأعمال والعمليات.

٣,٥,٧ لا يُسمح باستخدام برامج الألعاب على أنظمة وشبكات وزارة الصحة. يتعين على المستخدم عدم محاولة تثبيت برامج الألعاب أو نقلها أو استخدامها ضمن شبكة وزارة الصحة.

٣,٥,٨ يتعين على المستخدم الإبلاغ فورًا في حال فقدان حاسوبه المحمول أو حاسوبه الدفتري أو الحواسيب اليدوية الشخصية لضمان أمن هذه الأصول المادية.

٣,٥,٩ يتعين على المستخدم عند استخدام الحاسوب المحمول المُقدَّم من وزارة الصحة ضمان نسخ البيانات المخزَّنة على قرص محلي على خادم ملفات مركزي بصفة دورية من أجل الحصول على نسخة احتياطية ويجب عليه إبلاغ مكتب دعم تقنية المعلومات في حال وجود أي خطأ.

٣,٥,١٠ يجب حمل الحواسيب المحمولة باستخدام حقيبة اليد لتجنب إلحاق الضرر بها أو الدخول إليها بشكل غير مصرَّح به خلال السفر.

٣,٥,١١ يتعين على المستخدم حماية أجهزته التي تحتوي على معلومات سرية متعلقة بالعمل أو عدم تركها في أماكن بارزة (مثل: كرسي السيارة).

٣,٥,١٢ يتعين على المستخدم خلال العمل عن بعد ضمان حماية المعلومات الخاضعة للمعالجة من الوصول إليها بواسطة الأشخاص غير المُصرَّح لهم. يتعين على المستخدم تثبيت فلتر الحجب لضمان الخصوصية وتجنب استراق النظر من فوق أكتاف الأشخاص.

٣,٦ الهواتف المحمولة الشخصية

يهدف هذا القسم إلى تسليط الضوء على مسؤوليات المستخدم فيما يتعلق باستخدام الهواتف المحمولة الشخصية التي تعالج وتخزن معلومات متعلقة بعمل وزارة الصحة.

٣,٦,١ يتعين على المستخدم تفعيل خاصية القفل التلقائي على هاتفه المحمول. (يمكن أن تكون هذه الخاصية مماثلة لإعدادات قفل الشاشة بعد فترة انتظار).

٣,٦,٢ يتعين على المستخدم تجنب استخدام خصائص الإكمال التلقائي التي تتذكر أسماء المستخدمين أو كلمات المرور.

٣,٦,٣ تحتفظ وزارة الصحة بحق مسح هاتف المستخدم المحمول عن بُعد.

٣,٦,٤ يتعين على المستخدم إلغاء تنشيط تقنية البلوتوث في حال لم يكن بحاجة إليها. (سيساعد ذلك في إطالة زمن تشغيل البطارية وتوفير مستوى أفضل من الأمن).

٣,٦,٥ يتعين على المستخدم مواصلة تثبيت التحديثات على هاتفه المحمول والتطبيقات المثبتة عليه. يتعين على المستخدم تطبيق خيار تثبيت التحديثات تلقائيًا إن كان متاحًا.

٣,٦,٦ يتعين على المستخدم تثبيت برنامج مضاد الفيروسات أو برنامج أمن الحاسوب وتهيئته لمسح الجهاز وتحديثه بصورة تلقائية.

٣,٦,٧ يتعين على المستخدم تطبيق إجراءات أمن الأصول المادية الملائمة لمنع سرقة هاتفه المحمول.

٣,٦,٨ يتعين على المستخدم عدم ترك هاتفه المحمول في الأماكن العامة.

٣,٦,٩ يتعين على المستخدم تغيير كلمة مرور هاتفه المحمول فورًا في حال فقدانه. يتعين على المستخدم إبلاغ إدارة الأمن السيبراني بشأن فقدان الهاتف المحمول.

٣,٦,١٠ ينبغي أن يكون المستخدم على علم بالسياسات التي تطبقها شركات اتصالات الهواتف المحمولة وسياسات الأمن السيبراني التي تطبقها وزارة الصحة في حال فقدان الهواتف المحمولة أو سرقتها.

٣,٦,١١ ينبغي أن يكون المستخدم ملمًا بالخطوات المطلوب تنفيذها في حال فقدان هاتفه المحمول وبالخطوات المطلوب تنفيذها لإبلاغ موظفي وزارة الصحة المعنيين عن الحادث.

٣,٦,١٢ ينبغي على المستخدم الإبلاغ عن الحالة لناقل شبكة الاتصالات في أقرب وقت ممكن حتى يتسنى لهم تعطيل الهاتف المحمول إذا لَزِمَ الأمر.

٣,٧ البرامج الحاسوبية الضارة

يهدف هذا القسم إلى تسليط الضوء على مسؤوليات المستخدم المتعلقة بالتخفيف من حدة مخاطر البرامج الحاسوبية الضارة ضمن شبكة وزارة الصحة.

٣,٧,١ ينبغي على المستخدم عدم فتح المرفقات المرسلة بواسطة مصادر غير محددة أو مشبوهة.

٣,٧,٢ يتعين على المستخدم عدم تغيير إعدادات أو تعطيل مسح الملفات بواسطة مضاد الفيروسات والإعدادات الأخرى.

٣,٧,٣ يتعين على المستخدم اعتبار رسائل البريد الإلكتروني المستلمة من مصادر غير معروفة بأنَّها مشبوهة والإبلاغ عنها لإدارة الأمن السيبراني. كما يتعين على المستخدم إبلاغ إدارة الأمن السيبراني بخصوص رسائل البريد الإلكتروني المستلمة من مصادر معروفة والمحتوية على طلبات غير اعتيادية أو غير مألوفة.

٣,٧,٤ يتعين على المستخدم الاتصال فورًا بإدارة الأمن السيبراني إذا اشتبه أو أصبح على علم بفيروسات حاسوبية أو برامج حاسوبية ضارة.

٣,٨ أمن كلمات المرور

يهدف هذا القسم إلى تسليط الضوء على مسؤوليات المستخدم المتعلقة بإدارة كلمات المرور الخاصة به المستخدمة للدخول إلى حسابات وزارة الصحة.

٣,٨,١ يتعين على المستخدم عدم مشاركة كلمات المرور الخاصة به مع أي شخص.

٣,٨,٢ ينبغي على المستخدم عدم كتابة كلمات المرور الخاصة به أو أي نوع من وسائط التخزين المادية أو الإلكترونية.

٣,٨,٣ يتعين على المستخدم وضع كلمات مرور معقدة بشكل معقول وأن يلتزم بالضوابط المتعلقة بكلمات المرور بما يتوافق مع سياسة التحكم بالوصول.

٣,٩ أنشطة البريد الإلكتروني والاتصالات

يهدف هذا القسم إلى تسليط الضوء على مسؤوليات المستخدم المتعلقة بأنشطة استخدام البريد الإلكتروني والاتصالات في وزارة الصحة.

٣,٩,١ تم توفير نظام البريد الإلكتروني الخاص بوزارة الصحة للاستخدامات ذات الصلة بالعمل بشكل رئيسي. يتعين على المستخدم استغلال البريد الإلكتروني بطريقة مسؤولة ووفق سياسة وزارة الصحة بشأن أمن الاتصالات.

٣,٩,٢ يتعين على المستخدم عدم مشاركة أو تبادل المعلومات والبيانات على شكل ملفات ووثائق مما يؤدي إلى تعريض وزارة الصحة للمسؤولية القانونية أو الضرر.

٣,٩,٣ يتعين على المستخدم عدم استغلال حسابات البريد الإلكتروني الشخصية لتنفيذ أنشطة متعلقة بالعمل.

٣,٩,٤ ينبغي على المستخدم ألا يستغل البريد الإلكتروني لوزارة الصحة لتحقيق أي أغراض شخصية، بما في ذلك على سبيل المثال لا الحصر: التسجيل في المواقع العامة، والحصول على الخدمات عبر الإنترنت، والتسجيل في مواقع التواصل الاجتماعي، وغير ذلك.

٣,٩,٥ يتعين على المستخدم الامتناع عن إرسال رسائل البريد الإلكتروني التي تتضمن محتوى مهين (مثل التعليقات المهينة حول النوع الاجتماعي والتوجه الجنسي والإباحية وغيرها).

٣,٩,٦ يتعين على المستخدم اتخاذ الترتيبات اللازمة عند ذهابه في إجازة، بما في ذلك: تكليف شخص باستلام رسائل البريد الإلكتروني الواردة واتخاذ الإجراءات المطلوبة وفق قواعد العمل ذات الصلة.

٣,٩,٧ يجب على المستخدم تهيئة رسالة بريد إلكتروني تلقائية مفادها بأنَّه "خارج المكتب" عند ذهابه في مغادرة أو إجازة. مع ذلك، يتعين أن يمارس المستخدم ذلك بحذر. يمكن أن يسيء الأشخاص من خارج الوزارة استخدام المعلومات الكثيرة حول الغياب عن العمل. يجب إرسال معلومات كاملة (مثل: تاريخ العودة من الإجازة ورقم الهاتف، وغيرها) باستخدام اسم النطاق الداخلي الخاص بوزارة الصحة. مع ذلك، يمكن إرسال اسم جهة الاتصال وعنوان بريده الإلكتروني إلى خارج نطاق الوزارة.

٣,٩,٨ يجب على المستخدم الإبلاغ عن جميع الثغرات أو المشاكل الأمنية المشتبه بها إذا لاحظتها في نظام البريد الإلكتروني.

٣,٩,٩ يجب على المستخدم الالتزام بالترميز المتبع لتصنيف المعلومات عند مشاركة المعلومات والبيانات المتعلقة بأعمال وزارة الصحة مع أطراف داخلية أو خارجية.

٣,٩,١٠ تمتلك إدارة وزارة الصحة صلاحية اعتراض مراسلات البريد الإلكتروني أو الكشف عنها أو المساعدة في اعتراضها.

٣,٩,١١ يتعين على المستخدم عدم استغلال أنظمة وزارة الصحة لإعداد أو توزيع رسائل بريد إلكتروني متسلسلة.

٣,٩,١٢ يتعين على المستخدم عدم إعادة إرسال أو تحويل رسائل البريد الإلكتروني من حساب البريد الإلكتروني الخاص بالوزارة إلى حسابات البريد الإلكتروني الشخصية التي تعود للمستخدمين.

٣,١٠ أمن الوثائق

يهدف هذا القسم إلى تسليط الضوء على المسؤوليات التي تقع على عاتق المستخدم فيما يتعلق باستخدام وثائق وزارة الصحة بطريقة آمنة.

٣,١٠,١ سيتولى المستخدم تنفيذ جميع الإجراءات حسب دوره الوظيفي وصفته لحماية الوثائق من الإفصاح عنها بشكل غير مصرَّح به.

٣,١٠,٢ يتعين على المستخدم جمع وتمزيق النشرات أو النسخ التي لم تعد هناك حاجة إليها من الطابعات وآلات النسخ.

٣,١٠,٣ يتعين على المستخدم تطبيق سياسة مكتبية واضحة فيما يتعلق بالأوراق والوثائق السرية من أجل تقليل مخاطر الوصول إليها بشكل غير مصرح به وفقدان المعلومات أو إتلافها بعد انتهاء ساعات العمل.

٣,١٠,٤ يتعين على المستخدم توسيم وترميز والتعامل مع كافة الوثائق التي تحتوي على معلومات حساسة وفق سياسة إدارة أصول الأمن السيبراني.

٣,١٠,٥ يتعين على المستخدم تطبيق العملية المتبعة في وزارة الصحة لإتلاف أو التخلص من الوثائق المحتوية على معلومات سرية والتي انتهت مدة الاحتفاظ بها.

٣,١٠,٦ يتعين على المستخدم اعتبار إخطارات التحذير على صفحات أغلفة جهاز الفاكس بأنَّها رسالة للمستلم فقط كلما أمكن ذلك وبأنَّ استخدام الرسالة بواسطة أي طرف آخر سيكون غير مصرَّح به أو غير قانوني.

٣,١١ الإبلاغ عن الحوادث

يهدف هذا القسم إلى تسليط الضوء على مسؤوليات المستخدم المتعلقة بالإبلاغ عن الحوادث داخل وزارة الصحة.

٣,١١,١ يقع على عاتق جميع مستخدمي وزارة الصحة، بما في ذلك: الموظفين والأطراف الخارجية والمقاولين، مسؤولية إبلاغ إدارة الأمن السيبراني في الوزارة فورًا بأي دليل أو اشتباه بوجود مخالفة أمنية فيما يتعلق بما يلي:

- الوصول غير المصرَّح به إلى شبكات الاتصالات أو الأنظمة الحاسوبية.
- ظهور الفيروسات على أحد الحواسيب بشكل واضح.
- التلاعب الواضح بأي ملف قام المستخدم بتحديد ضوابط تقديرية وتقييدية للتحكم بالوصول إليه.
- مخالفة هذه السياسة أو أي سياسة أو إجراء متعلق بالأمن السيبراني بواسطة أي موظف أو مقاول أو مقدم خدمات خارجي.
- يجب على مستخدمي وزارة الصحة الإبلاغ عن الحادث باستخدام القنوات المناسبة في أقرب وقت ممكن. يمكن أن يؤدي عدم الإبلاغ عن الحوادث إلى ترك آثار سلبية على أنظمة معلومات وزارة الصحة وبياناتها.
- يجب توثيق جميع الحوادث الأمنية عند الإمكان. يجب على المستخدمين جمع أكبر قدر ممكن من المعلومات وتضمينها في تقريرهم.
- يمكن التواصل مع إدارة مخاطر الأمن السيبراني بخصوص الحوادث المتعلقة بهذه السياسة عبر أي من القنوات التالية:
  - يمكن الإبلاغ عن الحوادث عبر البريد الإلكتروني إلى **CS-IR@moh.gov.sa**

٤. الاستثناءات

٤,١ إذا كانت هناك حاجة ملحة للإعفاء من مسؤوليات هذه السياسة مع عدم وجود بديل قابل للتطبيق وآمن، يتعين على مقدم الطلب تعبئة نموذج طلب استثناء السياسة حسب الأصول وتوقيعه وإرساله إلى إدارة الأمن السيبراني.

٤,٢ يقوم مقدم الطلب بإرفاق وصف تفصيلي لنطاق العمل ومبررات الأعمال والفترة الزمنية مع نموذج طلب استثناء السياسة.

٤,٣ تتولى إدارة الأمن السيبراني مسؤولية مراجعة الطلب وتحديد المخاطر والضوابط الإضافية وفقًا لإطار إدارة المخاطر الخاص بوزارة الصحة، وقد تطلب من مقدم الطلب الموافقة على المخاطر المحددة والضوابط الإضافية. علاوة على ذلك، يجوز لإدارة الأمن السيبراني استشارة جهات داخلية وخارجية معنية بالمسائل القانونية والتنظيمية.

٤,٤ يتعين على مقدم الطلب تنفيذ الاستثناء بعد الحصول على موافقة رئيس إدارة الأمن السيبراني.

٤,٥ تتولى إدارة الأمن السيبراني مسؤولية متابعة الاستثناءات المعتمدة وإلغائها بعد زوال الأسباب التي تستدعي وجودها.

٥. الالتزام

٥,١ يُعدّ الالتزام بسياسات الأمن السيبراني الخاصة بوزارة الصحة والضوابط المرتبطة بها أمرًا إلزاميًا بين جميع الفرق وموظفيها والمقاولين والشركاء ومقدمي خدمات الرعاية الصحية الذين يحق لهم الاطلاع على معلومات وزارة الصحة ومرافق تجهيز المعلومات.

٥,٢ يتعين على المدراء المباشرين في وزارة الصحة تطبيق العناية الواجبة لضمان الالتزام عن طريق الإنفاذ المستمر والتقييم الذاتي ضمن نطاق مسؤولياتهم.

٥,٣ تتولى إدارة الأمن السيبراني مسؤولية إجراء تقييمات الالتزام بشكل منتظم ومستقل من أجل قياس وتحليل وتقييم مدى التزام وزارة الصحة بسياسات الأمن السيبراني والضوابط الأمنية المرتبطة بها. تتولى إدارة الأمن السيبراني مسؤولية متابعة التزام وزارة الصحة والإشراف على تنفيذ الأطراف المعنية للإجراءات التصحيحية.

٦. المخالفات

٦,١ تتولى إدارة الأمن السيبراني مسؤولية التحقق من المخالفات وتطبيق الإجراءات التأديبية والقانونية على الجهة المخالفة وفقًا للسياسات الخاصة بوزارة الصحة والأنظمة السعودية.

٦,٢ ينبغي أن تتوافق الإجراءات التأديبية مع درجة خطورة المخالفات، بحسب ما تُظهره التحقيقات، وقد تشمل، على سبيل المثال لا الحصر، ما يلي:

- فقدان حقوق الوصول إلى أصول المعلومات.
- استكمال التوعية بالأمن السيبراني.
- الغرامات المالية.
- إنهاء خدمات الموظف.

٧. مراجعة السياسة

٧,١ تتولى إدارة الأمن السيبراني مسؤولية مراجعة وتحديث هذه الوثيقة سنويًا، بالإضافة إلى ضمان التوافق المستمر مع التعديلات على المتطلبات وأفضل الممارسات واللوائح التنظيمية والالتزامات.

٧,٢ إذا كانت هناك حاجة ملحة لتعديل هذه السياسة، يتعين على مقدم الطلب تعبئة نموذج طلب تعديل وثيقة السياسة الأمنية حسب الأصول وتوقيعه وإرساله إلى إدارة الأمن السيبراني.

٨. التواصل

يمكن التواصل مع إدارة مخاطر الأمن السيبراني بخصوص الاستفسارات والملاحظات والحوادث المتعلقة بهذه السياسة عبر أي من القنوات التالية:

- يمكن إرسال الاستفسارات والملاحظات عبر البريد الإلكتروني إلى **CS-Policies@moh.gov.sa**
- يمكن الإبلاغ عن الحوادث عبر البريد الإلكتروني إلى **CS-IR@moh.gov.sa**

٩. المراجع

٩,١ المراجع التنظيمية الحكومية:

- الضوابط الأساسية للأمن السيبراني[١].
- ضوابط استخدام تقنيات المعلومات والاتصالات.[٢] (قرار رقم: ٥٥٥, تاريخ: ١٤٤٠/٩/٢٣ هـ)
- نظام مكافحة الجرائم الإلكترونية.

٩,٢ المراجع الدولية:

- آيزو/آي إي سي ٢٧٠٠١.
- آيزو/آي إي سي ٢٧٠٠٢.

٩,٣ المراجع الداخلية:

- سياسة التحكم بالوصول.
- سياسة أمن الأصول المادية والأمن البيئي.
- سياسة الاستخدام المقبول.
- سياسة إدارة حوادث الأمن السيبراني.
- إدارة دورة حياة الأصول التقنية.
- معيار تصنيف المعلومات.
- قائمة جرد أصول المعلومات.
- معيار طرق تسمية الأصول.
- معيار ترميز المعلومات.
- معيار التعامل مع الأصول.
- معيار إدارة الوسائط القابلة للنقل.
- إجراء التخلص الآمن.
- معيار نقل الوسائط المادية.
- القائمة المرجعية لإنهاء خدمات الموظف أو تغيير الوظيفة.

---

[١] *الضوابط الأساسية للأمن السيبراني*. الرياض: الهيئة الوطنية للأمن السيبراني، ٢٠١٨. PDF. <https://www.ncsc.gov.sa/>.

[٢] *ضوابط استخدام تقنيات المعلومات والاتصالات في الجهات الحكومية file:///X:/CS%20Governance/Governance/ضوابط%٢٠استخدام%٢٠تقنيات%٢٠المعلومات%٢٠والاتصالات%٢٠في%٢٠الجهات%٢٠الحكومية.pdf*