وزارة الصحة
Ministry of Health

سياسة الأمن السيبراني للاستخدام المقبول

المشاركة	أبيض
التصنيف	عام
الرقم	VM.PD - CSD – 001 - CPP
الحالة	نهائي
النسخة	٥,٠
التاريخ	٢٠٢٤/٠٣/٠٦
عدد الصفحات	١٢
الجهة المسؤولة	الإدارة العامة للأمن السيبراني
اسم الملف	سياسة الأمن السيبراني للاستخدام المقبول

المشاركة والتصنيف

المشاركة	**أبيض**: لا يوجد قيود على مشاركة المعلومات ويمكن نشر المعلومات عبر القنوات العامة.
التصنيف	**عام:** البيانات التي لا يوجد أثر من الإفصاح عنها أو الوصول غير المصرح به إليها.

تاريخ المراجعة

النسخة	التاريخ	المؤلف	ملخص التعديلات
١,٠	٢٠٢٠/٠٣/٠٣	الإدارة العامة للأمن السيبراني	إعداد الهيكل التنظيمي والبنود التفصيلية للسياسة
١,١	٢٠٢٠/٠٣/١٨	الإدارة العامة للأمن السيبراني	١. تعديل صياغة السياسة الأولية ٢. تطبيق ملاحظات المدير العام للأمن السيبراني
١,٢	٢٠٢٠/٠٣/٢٥	الإدارة العامة للأمن السيبراني	تحديث تفاصيل البريد الإلكتروني المذكورة في القسم ٩
٢,٠	٢٠٢٠/٠٦/٢٥	الإدارة العامة للأمن السيبراني	النسخة النهائية (يونيو ٢٠٢٠)
٣,٠	٢٠٢١/١٢/٢٩	الإدارة العامة للأمن السيبراني	المراجعة السنوية وإضافة بعض البنود حسب متطلبات الهيئة الوطنية للأمن السيبراني
٣,١	٢٠٢٢/٠١/٢٧	الإدارة العامة للأمن السيبراني	تطبيق ملاحظات الجهات المعنية
٤,٠	٢٠٢٣/٠٢/٠٨	الإدارة العامة للأمن السيبراني	المراجعة السنوية وإضافة بعض البنود حسب متطلبات الهيئة الوطنية للأمن السيبراني وبرقية الديوان
٥,٠	٢٠٢٤/٠١/٣٠	الإدارة العامة للأمن السيبراني	لم يتم تعديل أي جزء

النشر

الاسم والعنوان	القناة
وكالة الوزارة للصحة الإلكترونية والتحول الرقمي	البريد الإلكتروني
الإدارة العامة للشؤون القانونية	البريد الإلكتروني
وكالة الوزارة للموارد البشرية	البريد الإلكتروني / الشبكة الداخلية
وكالة الوزارة للتخطيط والتحول	البريد الإلكتروني

سجل السياسة	
رقم الاصدار	
ملاحظات التعديل	
تاريخ آخر تعديل	

عنوان السياسة	رقم السياسة	جهة اصدار السياسة	بديل للسياسة رقم
سياسة الأمن السيبراني للاستخدام المقبول	VM.PD - CSD - 001- CPP	الإدارة العامة للأمن السيبراني	VM.PD - CSD - 001- CPP
مستوى السياسة (نوع السياسة)	**تاريخ الاعتماد**	**تاريخ التطبيق**	**تاريخ المراجعة القادمة**
سياسة عامة	١٠-أغسطس -٢٠٢٠	٣-نوفمبر-٢٠٢٠	12- فبراير- 2025

١. الغرض

إن الأنظمة المتصلة بشبكة الإنترنت والشبكة الداخلية (الإنترانت) والشبكة الخارجية (الإكسترانت) مملوكة لوزارة الصحة، وتشمل على سبيل المثال لا الحصر: المعدات والبرمجيات وأنظمة التشغيل، ووسائط التخزين، وحسابات الشبكة التي تتيح الدخول إلى البريد الإلكتروني وتصفح شبكة الإنترنت العالمية وبروتوكول نقل الملفات. وبالتالي، تُحدد هذه السياسة الاستخدام المقبول لموارد و/أو أصول معلومات وزارة الصحة. هذه القواعد موجودة لحماية جميع أنواع المستخدمين المعرفين بوزارة الصحة. يمكن أن يُعّرض الاستخدام الغير مناسب وزارة الصحة للمخاطر، مثل هجمات الفيروسات وانتهاك امني للأنظمة والخدمات الشبكية وإلى تحمل تبعات قانونية.

٢. نطاق التطبيق

يغطي نطاق هذه السياسة جميع موارد و/أو أصول معلومات وزارة الصحة وينطبق على جميع أنواع المستخدمين المعرفين.

٣. التعاريف

تتماشى تعريفات المصطلحات المستخدمة في هذه الوثيقة مع الهيئة الوطنية للأمن السيبراني والمنظمة الدولية للمعايير (ISO)، ما لم يتم تعريفها على وجه التحديد أدناه.

- **مالك الخدمة**: موظف بوزارة الصحة أو الوحدة التنظيمية التي تتحمل المسؤولية الأساسية عن المعلومات الخاصة بنظام معين.
- **المشغل التقني**: أخصائي تقني في وزارة الصحة أو وحدة تنظيمية مسؤولة عن التطوير التقني لنظام معين وصيانته.
- **المستخدم أو الموظفون**: يشمل جميع منسوبي وزارة الصحة المدراء المباشرين ووكلاء الوزارة والفروع التابعة للوزارة والأطراف الخارجية والمتعاقدين والشركاء ومقدمي الخدمات الذين يمكن لهم الوصول إلى معلومات وزارة الصحة والمرافق الخاصة بمعالجة المعلومات.

٤. نص السياسة

٤,١ الأدوار والمسؤوليات

فيما يلي الأدوار والمسؤوليات ذات الصلة بهذه السياسة:

- **اللجنة الاشرافية للأمن السيبراني**
  - الجهة المسؤولة عن اتخاذ القرارات النهائية المتعلقة بتوضيح هذه السياسة.
  - مراجعة واعتماد السياسة.
  - مراجعة المخالفات الرئيسية لهذه السياسة.
- **الإدارة العامة للأمن السيبراني**

- تحمل مسؤولية السياسة وتحديثها وتوزيعها على العموم.
- إدارة الاستثناءات والمخالفات ذات الصلة بالسياسة.
- ضمان الالتزام بالسياسة داخل وزارة الصحة.

- **المستخدمون أو الموظفون**
  - الالتزام بالسياسة.

٤,٢ الاستخدام المقبول

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

٤,٢,١ تم تزويد المستخدم بأصول معلومات وزارة الصحة لأغراض متعلقة بالوظيفة ويتم منح الامتيازات الضرورية المتعلقة بالنظام عندما يكون هناك احتياجات مشروعة متعلقة بالعمل.

٤,٢,٢ لا تسمح وزارة الصحة باستخدام معلوماتها المتعلقة بالعمل وأصولها التقنية لأغراض شخصية، بما في ذلك تخزين البيانات الشخصية.

٤,٢,٣ ينبغي على المستخدم عدم الكشف عن معلومات حسابه لأي شخص.

٤,٢,٤ يتحمل المستخدم مسؤولية الحفاظ على سرية معلومات وزارة الصحة وأصولها التقنية وفق السياسات والمتطلبات الحالية للأمن السيبراني.

٤,٢,٥ سيقتصر وصول واستخدام المستخدم على الأنظمة المصرَّح له باستخدامها.

٤,٢,٦ 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.

٤,٢,٧ يتعين على المستخدم عدم تخزين أو معالجة أو نقل المواد الإباحية على أي من أنظمة معلومات وزارة الصحة.

٤,٢,٨ 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.

٤,٢,٩ 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.

٤,٢,١٠ تظل أي برمجيات حاسوبية طورها موظفو وزارة الصحة ضمن نطاق وظيفتهم "ملكية فكرية" للوزارة.

٤,٢,١١ تحتفظ وزارة الصحة بالحق في إجراء المراجعة بصفة دورية لضمان الالتزام بهذه السياسة.

٤,٢,١٢ يجب على المستخدمين استخدام أجهزة تمزيق الوثائق الورقية (Cross Shredding)، لإتلاف الوثائق المصنفة على أنها "سري" و "سري للغاية" في حال الانتهاء من استخدامها نهائيًا.

٤,٣ استخدام الإنترنت

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

٤,٣,١ يجب على المستخدم استخدام شبكة الإنترنت لتنفيذ أنشطة العمل في وزارة الصحة بطريقة مريحة ومتسمة بالكفاءة.

٤,٣,٢ يتعين على المستخدم عدم ربط أي جهاز أو أصل معلومات خاص بوزارة الصحة بشبكة الإنترنت إلاَّ بعد الحصول على الموافقة اللازمة من الإدارة العامة للأمن السيبراني.

٤,٣,٣ 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.

٤,٣,٤ 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.

٤,٣,٥ تحتفظ وزارة الصحة بحق تهيئة متصفحات الويب لحفظ ملفات تعريف الارتباط لتوفير قائمة بجميع المواقع الإلكترونية التي زارها المستخدمون.

٤,٣,٦ 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.

٤,٣,٧ 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.

٤,٣,٨ يتعين على المستخدم استخدام البرمجيات المعتمدة والمحددة للدخول إلى شبكة الإنترنت العالمية لضمان تنفيذ كافة المعالجات الأمنية المعتمدة.

٤,٣,٩ 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.

٤,٣,١٠ 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 الإدارة العامة للأمن السيبراني في الوزارة. بالإضافة إلى ذلك، تحتفظ وزارة الصحة بحق حماية حقوقها في الوصول إلى المعلومات.

٤,٣,١١ يتعين على المستخدمين التعهد بعدم استخدام تطبيقات التراسل أو التواصل الاجتماعي أو خدمات التخزين السحابية الشخصية لإنشاء أو تخزين أو مشاركة بيانات وزارة الصحة المصنفة على أنها "مقيد" و "سري" و "سري للغاية" في أول مراحل ارتباط المستخدم الوظيفي مع الوزارة وحتى نهاية العلاقة الوظيفية، باستثناء تطبيقات التراسل الآمنة المعتمدة من الجهات ذات العلاقة.

٤,٣,١٢ يتعين على المستخدم الحصول على الموافقة اللازمة من إدارة العلاقات العامة في الوزارة (الناطق الرسمي المُعيَّن) قبل نشر أي معلومات أو وثائق حول الوزارة لم يسبق نشرها على شبكة الإنترنت أو شبكات التواصل الاجتماعي.

٤,٣,١٣ 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.

٤,٣,١٤ يتعين على المستخدم تحديد مصدر المعلومات التي حصل عليها من شبكة الإنترنت بعناية لضمان موثوقيتها.

٤,٣,١٥ 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.

٤,٣,١٦ تطبق وتتقيد وزارة الصحة بشكل تام باتفاقيات الترخيص المبرمة مع موردي البرمجيات على النحو المحدد في سياسة الأمن السيبراني لأمن البرمجيات في وزارة الصحة. 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 الإدارة العامة للأمن السيبراني.

٤,٣,١٧ 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.

٤,٣,١٨ يتعين على المستخدم عدم تنفيذ أي فحص أمني أو اختبار أو حيازة أو استخدام أدوات لقرصنة رخص البرمجيات وكلمات المرور والأعمال المشابهة.

٤,٣,١٩ يتعين على المستخدم الاهتمام بالتحذيرات الأمنية التي يمكن أن تظهر عند تصفح المواقع على شبكة الإنترنت والتعامل مع كل رسالة بحذر.

٤,٤ استخدام مواقع التواصل الاجتماعي

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

٤,٤,١ 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.

٤,٤,٢ 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.

٤,٤,٣ 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.

٤,٤,٤ 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.

٤,٤,٥ يجب على موظفي الوزارة مراعات آداب النشر في شبكات التواصل الاجتماعي وعدم نشر ما يشير الى تعصب أو اتهام أو انطباع سلبي حول ما ينشر أو حول كتاب المحتوى الآخرين والابتعاد عن التلميح بسلبية حول المهام الوظيفية في الوزارة.

٤,٤,٦ يجب على جميع الموظفين العاملين على الوظائف أو الأنظمة الحساسة عدم الإفصاح عن وظائفهم ومهام عملهم في وسائل التواصل الاجتماعي.

٤,٤,٧ 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.

٤,٤,٨ 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.

٤,٥ أمن الأصول المادية

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

٤,٥,١ يتعين على المستخدم إظهار بطاقته التعريفية داخل مباني وزارة الصحة بصورة واضحة.

٤,٥,٢ يتعين على المستخدم الالتزام بمسافة الأمان في مباني وزارة الصحة والاهتمام بذلك.

٤,٥,٣ 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.

٤,٥,٤ يجب مراقبة الوصول إلى غرفة الحواسيب والمناطق المحظورة ويتعين على المستخدم التقيد بهذه الضوابط طوال الوقت.

٤,٥,٥ 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.

٤,٥,٦ يجب عدم نقل معلومات وزارة الصحة وأصولها التقنية خارج مبانيها إلاَّ بعد الحصول على الموافقة المطلوبة من المستوى القيادي المناسب و/أو الجهة المسؤولة.

٤,٥,٧ يتعين على المستخدم عدم إدخال أجهزة معالجة المعلومات، مثل: أنظمة الحاسب الآلي أو المضمان (مودم) الإنترنت، غير مأذون بها داخل مباني وزارة الصحة أو ربطها مع شبكة الوزارة إلاَّ بعد تبرير حاجة الأعمال إليها والحصول على الموافقة الخطية من الإدارة العامة للأمن السيبراني.

٤,٦ أمن المكاتب والحواسيب المحمولة والأجهزة المحمولة

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

٤,٦,١ 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.

٤,٦,٢ يتعين على المستخدم إقفال حاسوبه خلال الاستراحات القصيرة أو إطفاء حاسوبه قبل مغادرة المكتب و/أو في نهاية كل يوم.

٤,٦,٣ يتعين على المستخدم حماية المعلومات الحساسة وتخزينها وحذفها وعدم تركها على مكتبه بمكان يتيح قراءتها أو نسخها أو تغييرها دون علم المستخدم.

٤,٦,٤ ينبغي نبغي على المستخدم عدم تثبيت أي أجهزة جديدة على الحواسيب المكتبية دون الحصول على التصريح المطلوب من المشغل التقني.

٤,٦,٥ يتعين على المستخدم عدم تثبيت أو استخدام البرمجيات غير القانونية و/أو المقرصنة على الجهاز الذي قدمته وزارة الصحة.

٤,٦,٦ يجب على المستخدم استخدام المعدات التي اشترتها ووافقت عليها وزارة الصحة لتسيير الأعمال والعمليات.

٤,٦,٧ 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.

٤,٦,٨ يتعين على المستخدم الإبلاغ فورًا في حال فقدان حاسوبه المحمول أو حاسوبه الدفتري أو الحواسيب اليدوية الشخصية لضمان أمن هذه الأصول المادية.

٤,٦,٩ 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.

٤,٦,١٠ يجب حمل الحواسيب المحمولة باستخدام حقيبة اليد لتجنب إلحاق الضرر بها أو الدخول إليها بشكل غير مصرَّح به خلال السفر.

٤,٦,١١ يتعين على المستخدم حماية أجهزته التي تحتوي على معلومات سرية متعلقة بالعمل أو عدم تركها في أماكن بارزة (مثل: كرسي السيارة).

٤,٦,١٢ 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.

٤,٧ 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.

٤,٧,١ يتعين على المستخدم تفعيل خاصية القفل التلقائي على هاتفه المحمول. (يمكن أن تكون هذه الخاصية مماثلة لإعدادات قفل الشاشة بعد فترة انتظار).

٤,٧,٢ يتعين على المستخدم تجنب استخدام خصائص الإكمال التلقائي التي تتذكر أسماء المستخدمين أو كلمات المرور.

٤,٧,٣ يجب تحديد وتقييد استخدام الموظفين لأجهزتهم الشخصية عند استخدامها لأهداف عملية، ويتم تقييدها وفقًا للمتطلبات الوظيفية ذات العلاقة.

٤,٧,٤ إذا تطلب الأمر، تحتفظ وزارة الصحة بحق مسح الهاتف المحمول المقدم من الوزارة عن بعد، أو مسح بيانات الوزارة الموجودة على هواتف المستخدمين الشخصية.

٤,٧,٥ 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).

٤,٧,٦ يتعين على المستخدم مواصلة تثبيت التحديثات على هاتفه المحمول والتطبيقات المثبتة عليه. يتعين على المستخدم تطبيق خيار تثبيت التحديثات تلقائيًا إن كان متاحًا.

٤,٧,٧ يتعين على المستخدم تثبيت برنامج مضاد الفيروسات أو برنامج أمن الحاسوب وتهيئته لمسح الجهاز وتحديثه بصورة تلقائية.

٤,٧,٨ يتعين على المستخدم تطبيق إجراءات أمن الأصول المادية الملائمة لمنع سرقة هاتفه المحمول.

٤,٧,٩ يتعين على المستخدم عدم ترك هاتفه المحمول في الأماكن العامة.

٤,٧,١٠ ينبغي على جميع المستخدمين التأكد من أن بيانات وزارة الصحة والمعلومات المخزنة على هواتفهم المتنقلة مفصولة (منطقيًا) عن الملفات الشخصية، ويتم تشفيرها وفقًا لسياسة الأمن السيبراني للتشفير الخاصة بوزارة الصحة.

٤,٧,١١ يتعين على المستخدم تغيير كلمة مرور هاتفه المحمول فورًا في حال فقدانه. يتعين على المستخدم إبلاغ الإدارة العامة للأمن السيبراني بشأن فقدان الهاتف المحمول.

٤,٧,١٢ 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.

٤,٧,١٣ ينبغي أن يكون المستخدم ملمًا بالخطوات المطلوب تنفيذها في حال فقدان هاتفه المحمول وبالخطوات المطلوب تنفيذها لإبلاغ موظفي وزارة الصحة المعنيين عن الحادث.

٤,٧,١٤ ينبغي على المستخدم الإبلاغ عن الحالة لناقل شبكة الاتصالات في أقرب وقت ممكن حتى يتسنى لهم تعطيل الهاتف المحمول إذا لَزِمَ الأمر.

٤,٨ البرامج الحاسوبية الضارة

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

٤,٨,١ ينبغي على المستخدم عدم فتح المرفقات المرسلة بواسطة مصادر غير محددة أو مشبوهة.

٤,٨,٢ يتعين على المستخدم عدم تغيير إعدادات أو تعطيل مسح الملفات بواسطة مضاد الفيروسات والإعدادات الأخرى.

٤,٨,٣ يتعين على المستخدم اعتبار رسائل البريد الإلكتروني المستلمة من مصادر غير معروفة بأنَّها مشبوهة والإبلاغ عنها للإدارة العامة للأمن السيبراني. كما يتعين على المستخدم إبلاغ الإدارة العامة للأمن السيبراني بخصوص رسائل البريد الإلكتروني المستلمة من مصادر معروفة والمحتوية على طلبات غير اعتيادية أو غير مألوفة.

٤,٨,٤ يتعين على المستخدم الاتصال فورًا بالإدارة العامة للأمن السيبراني إذا اشتبه أو أصبح على علم بفيروسات حاسوبية أو برامج حاسوبية ضارة.

٤,٩ أمن كلمات المرور

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

٤,٩,١ يتعين على المستخدم عدم مشاركة كلمات المرور الخاصة به مع أي شخص.

٤,٩,٢ ينبغي على المستخدم عدم كتابة كلمات المرور الخاصة به أو أي نوع من وسائط التخزين المادية أو الإلكترونية.

٤,٩,٣ يتعين على المستخدم وضع كلمات مرور معقدة بشكل معقول وأن يلتزم بالضوابط المتعلقة بكلمات المرور بما يتوافق مع سياسة الأمن السيبراني للتحكم بالوصول.

٤,١٠ أنشطة البريد الإلكتروني والاتصالات

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

٤,١٠,١ تم توفير نظام البريد الإلكتروني الخاص بوزارة الصحة للاستخدامات ذات الصلة بالعمل بشكل رئيسي. يتعين على المستخدم استخدام البريد الإلكتروني بطريقة مسؤولة ووفق سياسة الأمن السيبراني لأمن الشبكات في وزارة الصحة.

٤,١٠,٢ يتعين على المستخدم عدم مشاركة أو تبادل المعلومات والبيانات على شكل ملفات ووثائق مما يؤدي إلى تعريض وزارة الصحة للمسؤولية القانونية أو الضرر.

٤,١٠,٣ يتعين على المستخدم عدم استخدام حسابات البريد الإلكتروني الشخصية لتنفيذ أنشطة متعلقة بالعمل.

٤,١٠,٤ 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.

٤,١٠,٥ يتعين على المستخدم الامتناع عن إرسال رسائل البريد الإلكتروني التي تتضمن محتوى مهين (مثل التعليقات المهينة حول النوع الاجتماعي والتوجه الجنسي والإباحية وغيرها).

٤,١٠,٦ 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.

٤,١٠,٧ 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.

٤,١٠,٨ ينبغي على جميع المستخدمين إبلاغ الإدارة العامة للأمن السيبراني بواسطة البريد الإلكتروني وبشكل فوري عن جميع الثغرات أو الحوادث الأمنية المشبوهة.

٤,١٠,٩ يجب على المستخدم الإبلاغ عن جميع الثغرات أو المشاكل الأمنية المشتبه بها إذا لاحظتها في نظام البريد الإلكتروني.

٤,١٠,١٠ يجب على المستخدم الالتزام بالترميز المتبع لتصنيف المعلومات عند مشاركة المعلومات والبيانات المتعلقة بأعمال وزارة الصحة مع أطراف داخلية أو خارجية.

٤,١٠,١١ تمتلك إدارة وزارة الصحة صلاحية اعتراض مراسلات البريد الإلكتروني أو الكشف عنها أو المساعدة في اعتراضها.

٤,١٠,١٢ يتعين على المستخدم عدم استخدام أنظمة وزارة الصحة لإعداد أو توزيع رسائل بريد إلكتروني متسلسلة.

٤,١٠,١٣ 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.

٤,١١ أمن الوثائق

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

٤,١١,١ سيتولى المستخدم تنفيذ جميع الإجراءات حسب دوره الوظيفي وصفته لحماية الوثائق من الإفصاح عنها بشكل غير مصرَّح به.

٤,١١,٢ يتعين على المستخدم جمع وتمزيق النشرات أو النسخ التي لم تعد هناك حاجة إليها من الطابعات وآلات النسخ.

٤,١١,٣ يتعين على المستخدم تطبيق سياسة الأمن السيبراني لتأمين المكاتب والشاشات فيما يتعلق بالأوراق والوثائق السرية من أجل تقليل مخاطر الوصول إليها بشكل غير مصرح به وفقدان المعلومات أو إتلافها بعد انتهاء ساعات العمل.

٤,١١,٤ يتعين على المستخدم توسيم وترميز والتعامل مع كافة الوثائق التي تحتوي على معلومات حساسة وفق سياسة الأمن السيبراني لإدارة الأصول.

٤,١١,٥ يتعين على المستخدم تطبيق العملية المتبعة في وزارة الصحة لإتلاف أو التخلص من الوثائق المحتوية على معلومات سرية والتي انتهت مدة الاحتفاظ بها.

٤,١١,٦ 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.

٤,١٢ الإبلاغ عن الحوادث

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

٤,١٢,١ يقع على عاتق جميع مستخدمي وزارة الصحة، بما في ذلك: الموظفين والأطراف الخارجية والمتعاقدين، مسؤولية إبلاغ الإدارة العامة للأمن 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 متعاقد 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

٤,١٣ الاستثناءات

٤,١٣,١ 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 الإدارة العامة للأمن السيبراني.

٤,١٣,٢ يقوم مقدم الطلب بإرفاق وصف تفصيلي لنطاق العمل ومبررات الأعمال والفترة الزمنية مع نموذج طلب استثناء السياسة.

٤,١٣,٣ تتولى الإدارة العامة للأمن 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 للإدارة العامة للأمن السيبراني استشارة جهات داخلية معنية بالمسائل القانونية وجهات داخلية وخارجية معنية بالمسائل التنظيمية.

٤,١٣,٤ يجب على مقدم الطلب عدم تنفيذ الاستثناء إلا عند الحصول على الموافقة من مدير عام الإدارة العامة للأمن السيبراني..

٤,١٣,٥ تتولى الإدارة العامة للأمن السيبراني مسؤولية متابعة الاستثناءات المعتمدة وإلغائها بعد زوال الأسباب التي تستدعي وجودها.

٤,١٤ الالتزام

٤,١٤,١ الالتزام بسياسات الأمن السيبراني الخاصة بوزارة الصحة والضوابط المرتبطة بها يعد أمراً إلزامياً في مهام وزارة الصحة، وعلى موظفيها، ومتعاقديها، وشركائها، ومقدمي الخدمات الذين يمكنهم الوصول إلى المعلومات ومرافق معالجة المعلومات بوزارة الصحة.

٤,١٤,٢ يتعين على المدراء المباشرين في وزارة الصحة تطبيق العناية الواجبة لضمان الالتزام عن طريق الإنفاذ المستمر والتقييم الذاتي ضمن نطاق مسؤولياتهم.

٤,١٤,٣ تتولى الإدارة العامة للأمن 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 الإدارة العامة للأمن السيبراني مسؤولية متابعة التزام وزارة الصحة والإشراف على تنفيذ الأطراف المعنية للإجراءات التصحيحية.

٤,١٥ المخالفات

٤,١٥,١ تتولى الإدارة العامة للأمن السيبراني مسؤولية التحقق التقني من المخالفات وتتولى الإدارة العامة للشؤون القانونية مسؤولية استكمال الإجراءات التأديبية والقانونية على الجهة المخالفة.

٤,١٥,٢ ينبغي أن تتوافق الإجراءات التأديبية مع درجة خطورة المخالفات، بحسب ما تُظهره التحقيقات، وما تنص عليها الأنظمة والقوانين ذات العلاقة.

٤,١٦ مراجعة السياسة

٤,١٦,١ تتولى الإدارة العامة للأمن السيبراني مسؤولية مراجعة وتحديث هذه الوثيقة سنويًا، بالإضافة إلى ضمان التوافق المستمر مع التعديلات على المتطلبات وأفضل الممارسات واللوائح التنظيمية والالتزامات.

٤,١٦,٢ إذا كانت هناك حاجة ملحة لتعديل هذه السياسة، يتعين على مقدم الطلب تعبئة نموذج طلب تعديل وثيقة السياسة الأمنية حسب الأصول وتوقيعه وإرساله إلى الإدارة العامة للأمن السيبراني.

٤,١٧ التواصل

٤,١٧,١ يمكن التواصل مع الإدارة العامة للأمن 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

٤,١٨ الاجراءات

غير مطلوب.

٤,١٩ مقياس الأداء (المؤشرات)

مراجعة جميع إصدارات الهيئة الوطنية للأمن السيبراني (NCA) والتأكد من تضمينها في السياسة.

٥. المراجع

٧,١ المراجع التنظيمية الحكومية:

- الضوابط الأساسية للأمن السيبراني.
- ضوابط استخدام تقنيات المعلومات والاتصالات. (قرار رقم: ٥٥٥, تاريخ: ١٤٤٠/٩/٢٣ هـ)
- ضوابط الأمن السيبراني للأنظمة الحساسة (CSCC).
- نظام مكافحة الجرائم الإلكترونية.

٧,٢ المراجع الدولية:

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

٧,٣ المراجع الداخلية:

- سياسة الأمن السيبراني للتحكم بالوصول.
- سياسة الأمن السيبراني للأمن المادي والبيئي.
- سياسة الأمن السيبراني للاستجابة الحوادث.
- إدارة دورة حياة الأصول التقنية.
- معيار طرق تسمية الأصول.
- معيار تصنيف المعلومات.
- قائمة جرد أصول المعلومات.
- معيار التعامل مع الأصول.
- معيار إدارة الوسائط القابلة للنقل.
- القائمة المرجعية لإنهاء خدمات الموظف أو تغيير الوظيفة

٦. المرفقات

٨,١ المراجع التنظيمية الحكومية:

- ضوابط استخدام تقنيات المعلومات والاتصالات.٢ (قرار رقم: ٥٥٥, تاريخ: ١٤٤٠/٩/٢٣ هـ)
- الضوابط الأساسية للأمن السيبراني;

- ضوابط الأمن السيبراني للأنظمة الحساسة (CSCC).
- نظام مكافحة الجرائم الإلكترونية.

عنوان السياسة	رقم السياسة	جهة اصدار السياسة	بديل للسياسة رقم
سياسة الأمن السيبراني للاستخدام المقبول	VM.PD - CSD - 001- CPP	الإدارة العامة للأمن السيبراني	VM.PD - CSD - 001- CPP
مستوى السياسة	**تاريخ الاعتماد**	**تاريخ التطبيق**	**تاريخ المراجعة القادمة**
[redacted] **سياسة عامة**	١٠-أغسطس -٢٠٢٠	٣-نوفمبر-٢٠٢٠	12- فبراير- 2025

الإعداد			
الاسم	المنصب	التوقيع	التاريخ
باسم عبدالله العنقري	مدير عام الإدارة العامة للأمن السيبراني		١١- فبراير -٢٠٢٤
مراجعة			
	المنصب	التوقيع	التاريخ
سوزان أسعد راشد	مدير عام الإدارة العامة للتميز المؤسسي		١١- فبراير -٢٠٢٤
فهد الغوينم	مدير عام الإدارة العامة للشؤون القانونية		١٢- فبراير -٢٠٢٤
الاعتماد			
الاسم	المنصب	التوقيع	التاريخ
اللجنة الإشرافية للأمن السيبراني	اللجنة الإشرافية للأمن السيبراني		٠٥- مارس -٢٠٢٤