المملكة العربية السعودية
وزارة الصناعة والثروة المعدنية

سياسة الاستخدام المقبول للأصول

١٤٤٢ هـ - ٢٠٢١ م

تصنيف: مقيد - عام

نسخ الوثيقة

النسخة	التاريخ	أسباب التعديل
1.0	04/12/2021	كتابة السياسة

قائمة المحتويات

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني؛ لتقليل المخاطر السيبرانية، المتعلقة باستخدام أنظمة وزارة الصناعة و الثروة المعدنية وأصولها، وحمايتها من التهديدات الداخلية والخارجية والعناية بالأهداف الأساسية للحماية؛ وهي المحافظة على سرية المعلومة، وسلامتها، وتوافرها .
وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-١-٣ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع ضوابط الأمن السيبراني في وزارة الصناعة والثروة المعدنية وتنطبق على جميع أنظمة الوزارة و العاملين سواء بعقود دائمة أو مؤقتة بما في ذلك الموردين و المقاولين الخارجيين وأي شخص لديه صلاحية الوصول الدائم أوالمؤقت إلى قاعدة وأنظمة وزارة الصناعة و الثروة المعدنية.

بنود السياسة

1- البنود العامة:

1- يجب التعامل مع المعلومات حسب التصنيف المحدد، وبما يتوافق مع سياسة حماية البيانات والمعلومات الخاصة بوزارة الصناعة و الثروة المعدنية بشكل يضمن حماية سرية المعلومات وسلامتها وتوافرها.
2- يحظر انتهاك حقوق أي شخص، أو شركة محمية بحقوق النشر، أو براءة الاختراع، أو أي ملكية فكرية أخرى، أو قوانين أو لوائح مماثلة؛ بما في ذلك، على سبيل المثال لا الحصر، تثبيت برامج غير مصرح بها أو غير قانونية.
3- يجب عدم ترك المطبوعات على الطابعة المشتركة دون رقابة.
4- يجب حفظ وسائط التخزين الخارجية بشكل آمن وملائم، مثل التأكد من ضبط درجة الحرارة بدرجة معينة، وحفظها في مكان معزول وآمن.
5- يمنع استخدام كلمة المرور الخاصة بمستخدمين آخرين، بما في ذلك كلمة المرور الخاصة بمدير المستخدم أو مرؤوسيه.
6- يجب الالتزام بسياسة المكتب الآمن والنظيف، والتأكد من خلو سطح المكتب، وكذلك شاشة العرض من المعلومات المصنفة.
7- يمنع الإفصاح عن أي معلومات تخص وزارة الصناعة و الثروة المعدنية، بما في ذلك المعلومات المتعلقة بالأنظمة والشبكات لأي جهة أو طرف غير مصرح له سواءً كان ذلك داخلياً أو خارجياً.
8- يُمنع نشر معلومات تخص وزارة الصناعة و الثروة المعدنية عبر وسائل الإعلام، وشبكات التواصل الاجتماعي دون تصريح مسبق.
9- يُمنع استخدام أنظمة وزارة الصناعة و الثروة المعدنية وأصولها بغرض تحقيق منفعة وأعمال شخصية، أو تحقيق أي غرض لا يتعلق بنشاط وأعمال وزارة الصناعة و الثروة المعدنية.
10- يُمنع ربط الأجهزة الشخصية بالشبكات، والأنظمة الخاصة بوزارة الصناعة و الثروة المعدنية دون الحصول على تصريح مسبق، وبما يتوافق مع سياسة أمن الأجهزة المحمولة (BYOD).

11- يُمنع القيام بأي أنشطة تهدف إلى تجاوز أنظمة الحماية الخاصة بوزارة الصناعة و الثروة المعدنية، بما في ذلك برامج مكافحة الفيروسات، وجدار الحماية، والبرمجيات الضارة دون الحصول على تصريح مسبق، وبما يتوافق مع الإجراءات المعتمدة لدى وزارة الصناعة و الثروة المعدنية
12- تحتفظ الإدارة العامة للأمن السيبراني بحقها في مراقبة الأنظمة والشبكات والحسابات الشخصية المتعلقة بالعمل، ومراجعتها دورياً لمراقبة الالتزام بسياسات الأمن السيبراني ومعاييره.
13- يُمنع استضافة أشخاص غير مصرح لهم بالدخول للأماكن الحساسة دون الحصول على تصريح مسبق.
14- يجب ارتداء البطاقة التعريفية في جميع مرافق وزارة الصناعة و الثروة المعدنية.
15- يجب تبليغ الإدارة العامة للأمن السيبراني في حال فقدان المعلومات أو سرقتها أو تسريبها.
16- يجب أن يعي جميع الموظفين أن أي بيانات مخزنة في أنظمة الوزارة هي مملوكة للوزارة وعلى ذلك فإن أي عملية نقل لهذه المعلومات يترتب عليها تحقيق واتخاذ الاجراءات اللازمة لذلك.
17- يجب على مديري الأنظمة والأشخاص المصرح لهم عدم الإفصاح عن أي تفاصيل متعلقة بالأنظمة والشبكات بما في ذلك الوصول إلى أو الاتصال عن بعد بموارد تقنية المعلومات في الوزارة إلى أي أشخاص غير مصرح لهم بذلك.
18- يجب على جميع الموظفين استخدام نظم وأصول تقنية المعلومات المسندة إليهم بعناية وحرص وستكون سلامة هذه النظم والأصول مسؤوليتهم .
19- يجب عدم نسخ أو نقل أي معلومات صنفت على أنها مقيدة أو سرية أو داخلية بأي طريقة ومنها على سبيل المثال لا الحصر، الأقراص المدمجة والمحمولة، ومرفقات البريد الإلكتروني وما إلى ذلك إلا بإذن من الإدارة العامة للأمن السيبراني.

2- حماية أجهزة الحاسب الآلي

1- يمنع استخدام وسائط التخزين الخارجية لتخزين أو نقل بيانات أو معلومات الوزارة إلا لحاجة العمل دون الحصول على تصريح مسبق من الإدارة العامة للأمن السيبراني، موضحاً فيه سبب الاستخدام، ومع مراعات استخدام وسائط تخزين مشفرة ومحمية .
2- يُمنع القيام بأي نشاط من شأنه التأثير على كفاءة الأنظمة والأصول وسلامتها دون الحصول على إذن مسبق من الإدارة العامة للأمن السيبراني، بما في ذلك الأنشطة التي تُمكّن المستخدم من الحصول على صلاحيات وامتيازات أعلى.
3- يجب تأمين الجهاز قبل مغادرة المكتب وذلك بقفل الشاشة، أو تسجيل الخروج (Sign out or Lock)، سواء كانت المغادرة لفترة قصيرة أو عند انتهاء ساعات العمل.
4- يجب على جميع المستخدمين التأكد من حماية شاشة التوقف بكلمة مرور. كما يجب على إدارة تقنية المعلومات تعيين شاشة توقف محمية بكلمة مرور بحيث تفعل بعد مرور 5 دقائق على عدم استخدام الجهاز .
5- يُمنع ترك أي معلومات مصنفة في أماكن يسهل الوصول إليها، أو الاطلاع عليها من قبل أشخاص غير مصرح لهم.
6- يُمنع تثبيت أدوات خارجية على جهاز الحاسب الآلي دون الحصول على إذن مسبق من إدارة بتقنية المعلومات.

7- يجب تبليغ الإدارة العامة للأمن السيبراني عند الاشتباه بأي نشاط قد يتسبب بضرر على أجهزة الحاسب الآلي الخاصة بوزارة الصناعة و الثروة المعدنية أو أصولها.
8- لا يسمح باستخدام برمجيات الألعاب على أي من أنظمة الوزارة ولا يسمح بتثبيتها أو نقلها في شبكة الوزارة.
9- يجب التحكم بجميع الصلاحيات الإدارية بطريقة آمنة على جميع أجهزة الوزارة ولا يجب تعيينها للاستخدام من قبل أي مستخدم عادي في الوزارة.

3- الاستخدام المقبول للإنترنت والبرمجيات

1- يجب عدم استخدام أنظمة الوزارة وشبكته للدخول إلى المواقع غير المتعلقة بالعمل مثل حسابات البريد الإلكتروني العامة، وبوابات الإنترنت، والمواقع التي تتضمن مواد غير قانونية .
2- يسمح باستخدام الوصول إلى شبكة الإنترنت لأغراض العمل فقط. كما يمنع استخدام الوصول إلى شبكة الإنترنت الخاصة بالوزارة لمنافع شخصية أو للترفيه في شبكات التواصل الاجتماعي أو على مواقع الإنترنت والمرئيات (مثل: يوتيوب، فيسبوك، تويتر أو أي مواقع أخرى)
3- يجب على المستخدم عدم تنزيل الوسائط غير المتعلقة بمجال العمل مثل:
   - برمجيات الند بالند (Peer to Peer) وبرمجيات مشاركة الملفات عبر الإنترنت
   - الأفلام، والألعاب، والموسيقى، والبرمجيات، والبرامج النصية، وما إلى ذلك.
4- يجب أن يحصل الموظفين الفنيين أوالمتعاقدين أو الأطراف الأخرى التي تقوم بحل المشاكل التقنية وتنفيذ العمليات على تصريح من قبل الإدارة العامة للأمن السيبراني قبل تثبيت واستخدام البرمجيات في أجهزة العمل مثل برامج المراسلة الفورية أو برامج التحكم بالوصول إلى البيانات. وعلى الأشخاص الراغبين في الحصول على هذه البرمجيات تقديم مبرر مناسب إلى الإدارة العامة للأمن السيبراني للموافقة. يتم بعد ذلك تثبيت البرنامج المطلوب بعد أخذ الموافقة من صاحب المصلحة بمساعدة الشخص المناسب من إدارة تقنية المعلومات.
5- يجب إبلاغ الإدارة العامة للأمن السيبراني في حال وجود مواقع مشبوهة ينبغي حجبها؛ أو العكس.
6- يجب ضمان عدم انتهاك حقوق الملكية الفكرية أثناء تنزيل معلومات أو مستندات لأغراض العمل .
7- يُمنع استخدام أو تثبيت البرمجيات غير المرخصة أو غيرها من الممتلكات الفكرية، (مثل البرمجيات المجانية / المشتركة) بدون موافقة واعتماده من قبل إدارة تقنية المعلومات والإدارة العامة للأمن السيبراني.
8- يجب استخدام متصفح آمن ومصرح به للوصول إلى الشبكة الداخلية أو شبكة الإنترنت.
9- يُمنع استخدام التقنيات التي تسمح بتجاوز الوسيط (Proxy) أو جدار الحماية (Firewall) للوصول إلى شبكة الإنترنت.
10- يُمنع تنزيل البرمجيات والأدوات أو تثبيتها على أصول وزارة الصناعة و الثروة المعدنية دون الحصول على تصريح مسبق من إدارة تقنية المعلومات.
11- يُمنع استخدام شبكة الإنترنت في غير أغراض العمل، بما في ذلك تنزيل الوسائط والملفات واستخدام برمجيات مشاركة الملفات.
12- يجب تبليغ الإدارة العامة للأمن السيبراني عند الاشتباه بوجود مخاطر سيبرانية، كما يجب التعامل بحذر مع الرسائل الأمنية التي قد تظهر خلال تصفح شبكة الإنترنت أو الشبكات الداخلية.

13- يُمنع إجراء فحص أمني لغرض اكتشاف الثغرات الأمنية، ويشمل ذلك إجراء اختبار الاختراقات، أو مراقبة شبكات وزارة الصناعة و الثروة المعدنية وأنظمتها، أو الشبكات والأنظمة الخاصة بالجهات الخارجية دون الحصول على تصريح مسبق من الإدارة العامة للأمن السيبراني.
14- يُمنع استخدام مواقع مشاركة الملفات دون الحصول على تصريح مسبق من الإدارة العامة للأمن السيبراني.
15- يُمنع زيارة المواقع المشبوهة بما في ذلك مواقع تعليم الاختراق.
16- يجب على الموظفين عدم تحميل أو تثبيت أو تنفيذ أي برامج أو خدمات حماية (مثل: الشبكات الخاصة الافتراضية، وكاسر كلمات المرور، وحزمة التنصت، وبرامج ماسحات المنافذ، وما إلى ذلك) التي قد تكشف أو تعرض مواطن الضعف في موارد الحاسب الآلي إلى الاستغلال ما لم يوافق على ذلك الإدارة العامة للأمن السيبراني .
17- يمنع نقل المعلومات السرية من خلال الإنترنت بدون موافقة من مدير عام الإدارة العامة للأمن السيبراني لتأمين الضوابط الأمنية اللازمة.
18- يجب استخدام الحاسب الآلي وأي أنظمة معلومات أخرى بطريقة تحافظ على سريتها وتحمي المعلومات المخزنة فيها .
19- لايسمح للمستخدمين بتعطيل أي خدمة أو جهاز حماية أو برامج الحماية من الفيروسات الموجودة على أي من موارد تقنية المعلومات في الوزرة إلا بموافقة من الإدارة العامة للأمن السيبراني.

4- الاستخدام المقبول للبريد الإلكتروني ونظام الاتصالات

1- يُمنع استخدام البريد الإلكتروني أو الهاتف أو الفاكس أو الفاكس الإلكتروني في غير أغراض العمل وبما يتوافق مع سياسات الأمن السيبراني ومعاييره.
2- يُمنع تداول رسائل تتضمن محتوى غير لائق أو غير مقبول، بما في ذلك الرسائل المتداولة مع الأطراف الداخلية والخارجية .
3- يجب استخدام تقنيات التشفير عند إرسال معلومات حساسة عن طريق البريد الإلكتروني أو أنظمة الاتصالات.
4- يجب عدم تسجيل عنوان البريد الإلكتروني الخاص بوزارة الصناعة و الثروة المعدنية في أي موقع ليس له علاقة بالعمل.
5- يجب تبليغ الإدارة العامة للأمن السيبراني عند الاشتباه بوجود رسائل بريد إلكتروني تتضمن محتوى قد يتسبب بأضرار لأنظمة وزارة الصناعة و الثروة المعدنية أو أصولها.
6- تحتفظ وزارة الصناعة و الثروة المعدنية بحقها في كشف محتويات رسائل البريد الإلكتروني بعد الحصول على التصاريح اللازمة من صاحب الصلاحية و الإدارة العامة للأمن السيبراني وفقاً للإجراءات والتنظيمات ذات العلاقة.
7- يُمنع فتح رسائل البريد الإلكتروني والمرفقات المشبوهة أو غير المتوقعة حتى وإن كانت تبدو من مصادر موثوقة.
8- يجب أن تتم جميع المراسلات البريدية في نطاق الشبكة المغلقة والمصرح بها في الوزارة.

9- يجب على جميع المستخدمين عدم تحويل رسائل البريد الإلكتروني أو إعادة توجيهها من البريد الإلكتروني الخاص بالوزارة إلى أي حساب بريد إلكتروني آخر خارج الوزارة (بما في ذلك حسابات البريد الإلكتروني الشخصية) .
10- يجب على جميع المستخدمين عدم فتح أي بريد إلكتروني مشبوه أو رابط أو ملف مرفق أو أي بريد إلكتروني ليس من المتوقع استلامه حتى وإن كان من مصدر موثوق.
11- الاجتماعات المرئية والاتصالات القائمة على شبكة الإنترنت
12- يُمنع استخدام أدوات أو برمجيات غير مصرح بها لإجراء اتصالات أو عقد اجتماعات مرئية.
13- يُمنع إجراء اتصالات أو عقد اجتماعات مرئية لا تتعلق بالعمل دون الحصول على تصريح مسبق.
14- تتم الموافقة على جميع طلبات الاتصال القائم على بروتوكول الإنترنت ومؤتمرات الفيديو من قبل المدير المباشر لمقدم الطلب أو المشرف عليه.

5- استخدام كلمات المرور

1- يجب اختيار كلمات مرور آمنة بناءً على سياسة كلمة المرور في الوزارة ، والمحافظة على كلمات المرور الخاصة بأنظمة وزارة الصناعة و الثروة المعدنية وأصولها. كما يجب اختيار كلمات مرور مختلفة عن كلمات مرور الحسابات الشخصية، مثل حسابات البريد الشخصي ومواقع التواصل الاجتماعي.
2- يُمنع مشاركة كلمة المرور عبر أي وسيلة كانت، بما في ذلك المراسلات الإلكترونية، والاتصالات الصوتية، والكتابة الورقية. كما يجب على جميع المستخدمين عدم الكشف عن كلمة المرور لأي طرف آخر بما في ذلك زملاء العمل وموظفو إدارة تقنية المعلومات.
3- يجب تغيير كلمة المرور، عند تزويدك بكلمة مرور جديدة من قبل مسؤول النظام.
4- لا يسمح لمستخدمي نظام المعلومات في الوزارة بالحصول على أو امتلاك أي كلمة مرور أو مفاتيح فك الشفرات أو الوصول إلى آليات المراقبة والتي قد تؤدي إلى وصول غير مصرح به .
5- لا يسمح باستخدام نظام المعلومات في الوزارة للأغراض التالية:
   - الكشف عن كلمة المرور عبر الهاتف لأي شخص.
   - الكشف عن كلمة المرور لأي شخص حتى وإن كان مدير نظم معلومات أو فرد من العائلة أو زملاء العمل أو مدراءهم.
   - الكشف عن كلمة المرور عبر الإنترنت
   - كتابة كلمة المرور على ورق او هاتف
   - كتابة كملة المرور أمام أي شخص آخر.
6- المستخدمين معرضين للمساءلة في حال تم ارتكاب أي أنشطة من خلال حساباتهم.

الأدوار والمسؤوليات

1- **يجب على الإدارة العامة للأمن السيبراني:**
- الموافقة على السياسة ودعم تنفيذها.
- الإشراف على الإلتزام للسياسة والإنتهاكات الإستثناءات وتسوية المنازعات.
- ضمان التوافق بين هذه السياسة وأعمال الوزارة.
- إدارة استثناءات السياسة والمخالفات.
- توفير الموارد اللازمة لتحديد وشراء وتنفيذ الحلول التقنية وذلك لتنفيذ متطلبات السياسة المقبولة لاستخدام الأصول حيثما أمكن .

2- **يجب على مدراء الأقسام / مالكي أصول البيانات التالي:**
- بتطبيق والالتزام بهذه السياسة على البيانات التي يديرونها.
- متابعة وتسجيل حالات عدم الالتزام المبلغ عنها.
- تزويد الإدارة العامة للأمن السـيبراني وإدارة تقنية المعلومات بتوصـيات لتحديث متطلبات السياسة.

3- **يجب على موظفي الوزارة الالتزام بهذه السياسة والإبلاغ عن أي حادث أمني أو عدم الالتزام بهذه السياسه الى مدير عام الإدارة العامة للأمن السيبراني.**

ملكية السياسة

المسؤول عن هذه السياسة هو مدير عام الإدارة العامة للأمن السيبراني في الوزارة.

تغييرات السياسة

يجب مراجعة هذه السياسة سنوياً، وتوثيق التغييرات واعتمادها من قبل صاحب الصلاحية في الوزارة

الالتزام بالسياسة

1- يجب على مدير عام الإدارة العامة للأمن السيبراني ضمان التزام وزارة الصناعة والثروة المعدنية بهذه السياسة سنوي.
2- يجب على جميع العاملين في وزارة الصناعة والثروة المعدنية الالتزام بهذه السياسة.
3- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة، إلى إجراء تأديبي؛ حسب الإجراءات المتبعة في وزارة الصناعة والثروة المعدنية.
4- يجب على جميع الموظفين والأطراف الخارجية المتعاقدة مع الوزارة أو العاملين بها الإلتزام بمتطلبات السياسة ويجب على مدير عام الإدارة العامة للأمن السيبراني في الوزارة ضمان المراقبة المستمرة للإلتزام وإبلاغ التحديثات لصاحب الصلاحية بشكل دوري.

5- يجب تنفيذ الإجراءات المناسبة لضمان الالتزام ببنود هذه السياسة بإجراء مراجعة سنوياً من قبل الإدارة العامة للأمن السيبراني أو الإدارات ذات العلاقة. وأي انتهاك لهذه السياسة سيؤدي إلى اتخاذ إجراءات تصحيحية من جانب صاحب الصلاحية في الوزارة على أن تكون الإجراءات التأديبية متناسبة مع خطورة الحادثة وفقًا لما يحدده التحقيق، وقد تتضمن على سبيل المثال لا الحصر ما يلي:

- سحب صلاحية الوصول إلى أصول المعلومات.
- توجيه إنذار خطي، أو إنهاء خدمة العامل أو حسب ما تراه الوزارة من إجراءات مناسبة.

6- إن عدم الالتزام بهذه السياسة دون الحصول على استثناء مسبق من الإدارة العامة للأمن السيبراني يستوجب اتخاذ الإجراءات المناسبة وفقًا لسياسات ولوائح الوزارة وقوانينها، أو حسبما يكون مناسبًا، ووفقًا للشروط التعاقدية لاتفاقيات الوزارة مع الشخص أو الجهة المصرح لها.

الاستثناءات

1- تهدف هذه السياسة إلى تطبيق متطلبات الأمن السيبراني. إذا لزم الأمر ، يجب تقديم طلبات الإستثناء رسميًا إلى إدارة الأمن السيبراني، بما في ذلك التبرير والفوائد المنسوبة إلى التنازل.

2- فترة الإعفاء من الوثيقة بحد أقصى ثلاثة أشهر ، ويجب إعادة تقييمها واعتمادها مرة أخرى ، إذا لزم الأمر لمدة ثلاث فترات متتالية كحد أقصى. يجب عدم تقديم أي سياسة تنازل لأكثر من ثلاثة شروط متتالية.