سياسة الاستخدام المقبول للأصول المعلوماتية

نسخة الوثيقة

النسخة	التاريخ	عدل بواسطة	أسباب التعديل
V1	١٤٤١/١/١ هـ	م. عايض بن هندي هنيدي المجنوني	سياسة الاستعمال المقبول
V2	١٤٤٢/٤/٢٩ هـ	م. عايض بن هندي هنيدي المجنوني	إضافة وتعديل على كافة السياسة

المراجعة والتدقيق

النسخة	التاريخ	بواسطة	الدور
V2	١٤٤٢/٥/١ هـ	مناع بن جمعان الغامدي	مراجعة
	١٤٤٢/٥/١ هـ	سعد بن حسن الشمراني	تدقيق

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني لتقليل المخاطر السيبرانية، المتعلقة باستخدام أنظمة الرئاسة 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 الأصول المعلوماتية والتقنية الخاصة بالرئاسة، وتنطبق هذه السياسة على جميع العاملين بالرئاسة.

بنود السياسة

١- البنود العامة

١-١ يجب التعامل مع المعلومات حسب التصنيف المحدد، وبما يتوافق مع سياسة تصنيف البيانات (سياسة بروتوكول الإشارة الضوئية) الخاصة بالرئاسة بشكل يضمن حماية سرية المعلومات وسلامتها وتوافرها.

١-٢ 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.

١-٣ يجب عدم ترك المطبوعات على الطابعة المشتركة دون رقابة.

١-٤ يمنع استخدام كلمة المرور الخاصة بمستخدمين آخرين بما في ذلك كلمة المرور الخاصة بمدير المستخدم أو مرؤوسيه.

١-٥ يجب الالتزام بسياسة المكتب الآمن والنظيف والتأكد من خلو سطح المكتب وكذلك شاشة العرض من المعلومات المصنفة.

١-٦ يمنع الإفصاح عن أي معلومات تخص الرئاسة، بما في ذلك المعلومات المتعلقة بالأنظمة والشبكات لأي جهة أو طرف غير مصرح له سواءً كان ذلك داخلياً أو خارجياً.

١-٧ يمنع نشر معلومات تخص الرئاسة عبر وسائل الإعلام وشبكات التواصل الاجتماعي دون تصريح مسبق.

١-٨ يمنع استخدام أنظمة الرئاسة وأصولها بغرض تحقيق منفعة وأعمال شخصية، أو تحقيق أي غرض لا يتعلق بنشاط وأعمال الرئاسة.

١-٩ يمنع ربط الأجهزة الشخصية بالشبكات والأنظمة الخاصة بالرئاسة دون الحصول على تصريح مسبق، وبما يتوافق مع سياسة أمن الأجهزة المحمولة (BYOD).

١-١٠ الإدارة العامة للأمن السيبراني مسؤولية تسجيل الحوادث السيبرانية وقياسها وتعقبها وتحليلها وتصعيدها إلى الجهات المختصة إن لزم الأمر.

١-١١ يمنع القيام بأي أنشطة تهدف إلى تجاوز أنظمة الحماية الخاصة بالرئاسة، بما في ذلك برامج مكافحة الفيروسات، وجدار الحماية، والبرمجيات الضارة دون الحصول على تصريح مسبق وبما يتوافق مع الإجراءات المعتمدة لدى الرئاسة.

١-١٢ تحتفظ الإدارة العامة للأمن السيبراني بحقها في مراقبة الأنظمة والشبكات والحسابات الشخصية المتعلقة بالعمل ومراجعتها دورياً لمراقبة الالتزام بسياسات الأمن السيبراني ومعاييره.

١-١٣ يمنع استضافة أشخاص غير مصرح لهم بالدخول للأماكن الحساسة دون الحصول على تصريح مسبق.

١-١٤ يجب ارتداء البطاقة التعريفية في جميع مرافق الرئاسة.

١-١٥ يجب تبليغ الإدارة العامة للأمن السيبراني في حال فقدان المعلومات أو سرقتها أو تسريبها.

١-١٦ يجب مراجعة سياسة الاستخدام المقبول للأصول سنوياً، وتوثيق التغييرات واعتمادها.

٢- حماية أجهزة الحاسب الآلي

٢-١ يمنع استخدام وسائط التخزين الخارجية دون الحصول على تصريح مسبق من الإدارة العامة للأمن السيبراني.

٢-٢ يمنع 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 تمكن المستخدم من الحصول على صلاحيات وامتيازات أعلى.

٢-٣ 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.

٢-٤ يمنع ترك أي معلومات مصنفة في أماكن يسهل الوصول إليها أو الاطلاع عليها من قبل أشخاص غير مصرح لهم.

٢-٥ يمنع تثبيت أدوات خارجية على جهاز الحاسب الآلي دون الحصول على إذن مسبق من الإدارة العامة لتقنية المعلومات.

٢-٦ يجب تبليغ الإدارة العامة للأمن السيبراني عند الاشتباه بأي نشاط قد يتسبب بضرر على أجهزة الحاسب الآلي الخاصة بالرئاسة أو أصولها.

٢-٧ يمنع خروج الأجهزة من مجال الشبكة بدون موافقة مسبقة من الإدارة العامة لتقنية المعلومات.

٢-٨ إنشاء ومعالجة وأرشفة وحذف ملفات المستخدم حسبما تقتضيه طبيعة ومصلحة العمل.

٣- الاستخدام المقبول للإنترنت والبرمجيات

٣-١ يجب إبلاغ الإدارة العامة للأمن السيبراني في حال وجود مواقع مشبوهة ينبغي حجبها أو العكس.

٣-٢ يجب ضمان عدم انتهاك حقوق الملكية الفكرية أثناء تنزيل معلومات أو مستندات لأغراض العمل.

٣-٣ يمنع استخدام البرمجيات غير المرخصة أو غيرها من الممتلكات الفكرية.

٣-٤ يجب استخدام متصفح آمن ومصرح به للوصول إلى الشبكة الداخلية أو شبكة الإنترنت.

٣-٥ يمنع استخدام التقنيات التي تسمح بتجاوز الوسيط (Proxy) أو جدار الحماية (Firewall) للوصول إلى شبكة الإنترنت.

٣-٦ يمنع تنزيل البرمجيات والأدوات أو تثبيتها على أصول الرئاسة دون الحصول على تصريح مسبق من الإدارة العامة لتقنية المعلومات.

٣-٧ يمنع استخدام شبكة الإنترنت في غير أغراض العمل بما في ذلك تنزيل الوسائط والملفات واستخدام برمجيات مشاركة الملفات.

٣-٨ 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.

٣-٩ يمنع إجراء فحص أمني لغرض اكتشاف الثغرات الأمنية ويشمل ذلك إجراء اختبار الاختراقات، أو مراقبة شبكات الرئاسة وأنظمتها، أو الشبكات والأنظمة الخاصة بالجهات الخارجية دون الحصول على تصريح مسبق من الإدارة العامة للأمن السيبراني.

٣-١٠ يمنع استخدام مواقع التواصل الاجتماعي ومواقع مشاركة الملفات دون الحصول على تصريح مسبق من الإدارة العامة للأمن السيبراني.

٣-١١ يمنع زيارة المواقع المشبوهة ذات المحتوى المحظور وفقاً لسياسات الرئاسة.

٤- الاستخدام المقبول للبريد الإلكتروني ونظام الاتصالات

٤-١ يمنع استخدام البريد الإلكتروني أو الهاتف أو الفاكس أو الفاكس الإلكتروني في غير أغراض العمل وبما يتوافق مع سياسات الأمن السيبراني ومعاييره.

٤-٢ يمنع تداول رسائل تتضمن محتوى غير لائق أو غير مقبول بما في ذلك الرسائل المتداولة مع الأطراف الداخلية والخارجية.

٤-٣ يجب استخدام تقنيات التشفير عند إرسال معلومات حساسة عن طريق البريد الإلكتروني أو أنظمة الاتصالات.

٤-٤ يجب عدم تسجيل عنوان البريد الإلكتروني الخاص بالرئاسة في أي موقع ليس له علاقة بالعمل.

٤-٥ يجب تبليغ الإدارة العامة للأمن السيبراني عند الاشتباه بوجود رسائل بريد إلكتروني تتضمن محتوى قد يتسبب بأضرار لأنظمة الرئاسة أو أصولها.

٤-٦ يجب استخدام البريد الإلكتروني الخاص بالرئاسة في مهام العمل اليومية.

٤-٧ تحتفظ الرئاسة بحقها في كشف محتويات رسائل البريد الإلكتروني بعد الحصول على التصاريح اللازمة من صاحب الصلاحية والإدارة العامة للأمن السيبراني وفقاً للإجراءات والتنظيمات ذات العلاقة.

٤-٨ يمنع فتح رسائل البريد الإلكتروني والمرفقات المشبوهة أو غير المتوقعة حتى وإن كانت تبدو من مصادر موثوقة.

٤-٩ يمنع استخدام البريد الالكتروني الشخصي مثل (Hotmail. Gmail) في مهام العمل اليومية بالرئاسة.

٥- الاجتماعات المرئية والاتصالات القائمة على شبكة الإنترنت

١-٥ يمنع استخدام أدوات أو برمجيات غير مصرح بها لإجراء اتصالات أو عقد اجتماعات مرئية.

٢-٥ يمنع إجراء اتصالات أو عقد اجتماعات مرئية لا تتعلق بالعمل دون الحصول على تصريح مسبق.

٦- استخدام كلمات المرور

١-٦ يجب اختيار كلمات مرور آمنة، والمحافظة على كلمات المرور الخاصة بأنظمة الرئاسة وأصولها. كما يجب اختيار كلمات مرور مختلفة عن كلمات مرور الحسابات الشخصية، مثل حسابات البريد الشخصي ومواقع التواصل الاجتماعي.

٢-٦ يمنع 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 الإدارة العامة لتقنية المعلومات.

٣-٦ يجب أن تكون كلمة المرور مكونة من ثمانية خانات كحد أدنى، ثلاثة منها على الأقل تحتوي على أحرف وارقام ورموز خاصة.

٤-٦ يجب تغيير كلمة المرور على الفور عند الإفصاح عنها بشكل غير مرخص، سواءً بشكل متعمد أو غير متعمد.

٥-٦ يجب تغيير كلمة المرور عند تزويدك بكلمة مرور جديدة من قبل مسؤول النظام.

٦-٦ يمنع استخدام كلمات مرور رائجة والتي يمكن التكهن بها بسهولة، كالأسماء وتاريخ الميلاد أو أرقام الهواتف.

٧-٦ تعامل مع كلمات المرور على أنها معلومات سرية، وتستمد حساسيتها من حساسية المعلومات للنظام المرتبط بها.

٨-٦ يجب ضمان عدم تفعيل خاصية حفظ كلمة المرور في المتصفح وإدخال البيانات في كل مرة من جديد.

٩-٦ يجب على المستخدمين قدر الإمكان عدم استخدام كلمة المرور نفسها لحسابات مختلفة في الرئاسة.

١٠-٦ كلمات المرور للأنظمة (Root/Administrator) يجب أن تخزن باستعمال برمجيات حفظ كلمات المرور او بطريقة مشفرة.

١١-٦ يمنع الدخول للأنظمة الداخلية والخاصة بالرئاسة بعد ٣ محاولات خاطئة خلال مدة زمنية لا تتجاوز ١٥ دقيقة. ويستمر المنع لمدة أقلها ٣٠ دقيقة وأكثرها ٣ساعات.

١٢-٦ يجب على المستخدم في حالة أن يشتبه أو يلاحظ وجود مشكلة أمنية أو أن كلمة المرور الخاصة به قد تعرضت للاختراق إبلاغ الإدارة العامة للأمن السيبراني وتغيير جميع كلمات المرور.

٧- خصوصية المعلومات

١-٧ يمنع نشر المعلومات السرية والوثائق الخاصة بالرئاسة عبر وسائل التواصل الاجتماعي وغيرها.

٢-٧ يمنع استخدام حساب موظف اخر في الدخول على الأجهزة والأنظمة بالرئاسة.

٣-٧ يجب على المستخدم حماية المعلومات والأجهزة والمحافظة عليها من التلف أو التخريب أو الضياع.

٤-٧ الحفاظ على معلومات الموظفين الشخصية وحمايتها من الإفصاح بشكل غير مرخص.

الأدوار والمسؤوليات

راعي ومالك وثيقة السياسة: الإدارة العامة للأمن السيبراني.

مراجعة السياسة وتحديثها: إدارة الحوكمة والمخاطر والالتزام.

تنفيذ السياسة وتطبيقها: جميع العاملين بالرئاسة.

الالتزام بالسياسة

١- يجب على الإدارة العامة للأمن السيبراني ضمان التزام الرئاسة بهذه السياسة دورياً.

٢- يجب على جميع العاملين في الرئاسة الالتزام بهذه السياسة.

٣- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة، إلى إجراء تأديبي؛ حسب الإجراءات المتبعة في الرئاسة.