بسم الله الرحمن الرحيم

دائرة الشؤون الفلسطينية

الرقم ٧٧٣٧/٣/٤/ق

التاريخ

الموافق ٢٠٢٣/١٠/٢٩

السيد مدير مديرية .....

السيد مدير مكتب الدائرة لمحافظة .....

الموضوع: سياسات وتعليمات

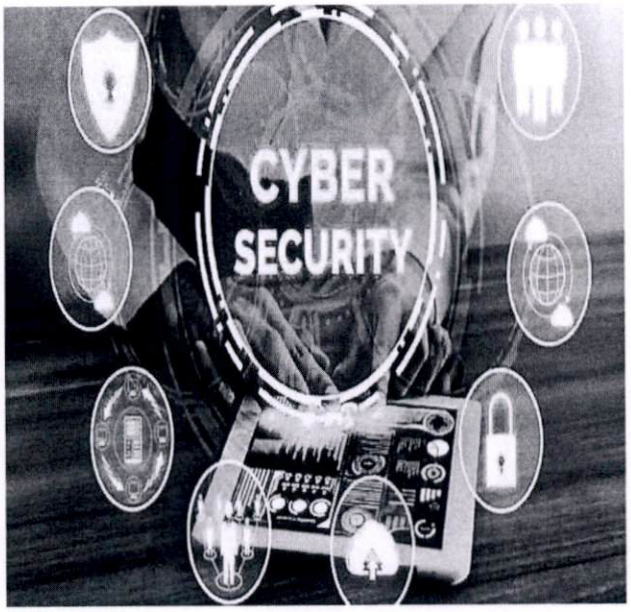
الامن السيبراني

انطلاقا من الإطار الوطني للأمن السيبراني وإيمانا من دائرة الشؤون الفلسطينية بأهمية حماية ممتلكات الدائرة الرقمية والمعلوماتية من التهديدات والمخاطر الداخلية والخارجية، وبما أن المعلومات من الركائز الأساسية والموجودات الهامة التي تبني عليها الدائرة العديد من القرارات التي تساهم بتحقيق الأهداف الوطنية والمؤسسية؛ فقد قامت مديرية تكنولوجيا المعلومات بإعداد سياسات وتعليمات خاصة بالأمن السيبراني، ووضعت خطة لتعزيز ثقافة الحماية من المخاطر السيبرانية وتعميق الوعي بالأمن السيبراني. لذا على جميع الموظفين الالتزام بما ورد في هذه السياسات والتعليمات كلٌّ حسب الصلاحيات الممنوحة له وحسب طبيعة عمله. والعمل على الالتزام والتعاون التام مع مديرية تكنولوجيا المعلومات فيما تُصدر بهذا الخصوص.

واقبلوا الاحترام،،،

المدير العام

المهندس رفيق خرفان



سياسات وتعليمات
الامن السيبراني

دائرة الشؤون الفلسطينية

مديرية تكنولوجيا المعلومات
2023

دائرة الشؤون الفلسطينية
Department of Palestinian Affairs

سياسات وتعليمات الأمن السيبراني

في دائرة الشؤون الفلسطينية

2023

المقدمــة

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بتوثيق متطلبات الأمن السيبراني والتزام دائرة الشؤون الفلسطينية بها، وبحيث تتوافق مع السياسات والتعليمات الصادرة عن المركز الوطني للأمن السيبراني وكذلك السياسات الوطنية لأمن وحماية المعلومات المُعدَّة من قبل اللجنة الوطنية الفنية لأمن وحماية المعلومات والتي أقرها مجلس الوزراء الموقر؛ وذلك بهدف تقليل المخاطر السيبرانية وحماية ممتلكات الدائرة الرقمية والمعلوماتية من التهديدات والمخاطر الداخلية والخارجية، وللحماية من الوصول غير المصرح به إلى مراكز البيانات والأنظمة المحوسبة الأخرى، وتأمين وحماية الأصول الرقمية وأنظمة الدائرة من الاختراق، وتوفير وضعًا أمنيًا جيدًا ضد الهجمات الضارة المصممة للوصول أو تغيير أو حذف أو تدمير أو ابتزاز أنظمة الدائرة أو المستخدمين والبيانات الحساسة ويتم ذلك من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها. ومع تزايد عدد المستخدمين والأجهزة والبرامج في الدائرة وزيادة البيانات التي يعتبر الكثير منها حساس أو سري وبما أن المعلومات من الركائز الأساسية والموجودات الهامة التي تبني عليها الدائرة العديد من القرارات التي تساهم بتحقيق الأهداف المؤسسية والوطنية لها؛ من هنا اتخذت الدائرة قواعد وأسس للتعامل مع المعلومات وحمايتها من الضياع والتلف أو الاستخدام غير المشروع وتقليل التهديدات التي تؤثر على سلامة المعلومات وسريتها وإتاحتها.

نطاق العمل

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية والبنية التحتية الرقمية لدائرة الشؤون الفلسطينية وتنطبق على جميع العاملين في الدائرة وفي الميدان.

وتعتبر هذه السياسة هي المحرك الرئيسي لجميع سياسات الأمن السيبراني وإجراءاته ومعاييره ذات المواضيع المختلفة، وكذلك أحد المدخلات لعمليات دائرة الشؤون الفلسطينية الداخلية، مثل عمليات الموارد البشرية وعمليات إدارة الموردين وعمليات إدارة المشاريع وإدارة التغيير وغيرها.

السياسات والتعليمات

سياسة أمن الشبكات والخوادم

تتعلق هذه السياسة بضمان حماية شبكات الانترنت الخاصة بدائرة الشؤون الفلسطينية من المخاطر السيبرانية، وتتضمن:

- استخدام برنامج لمراقبة الشبكة والمواقع الإلكترونية (Web Filtering) وذلك من أجل حماية الشبكة الداخلية من البرامج الخبيثة والبرامج التجسسية التي يمكن أن تهدد أمن وسلامة وإتاحية وخصوصية المعلومات.
- استخدام الجدران النارية (Firewalls).
- استخدام مضاد للفيرروسات وتعميمه على كافة الخوادم وتحديثة باستمرار.
- ربط البنية التحتية لشبكة تكنولوجيا المعلومات في الدائرة مع البنية التحتية لشبكة الحكومة الإلكترونية الآمنة (SGN-Government Network Secured).
- يجب حماية الشبكات اللاسلكية المتوفرة في الدائرة من خلال كلمة سر لحمايتها من الاستخدام لغير المخولين.
- وضع الأجهزة الخادمة الرئيسية وكافة الأجهزة المتعلقة بالشبكة والإنترنت في موقع يمتاز بما يلي:
  - مجهز بأنظمة الحماية ضد الحريق.
  - مزود بأجهزة تكييف لتحافظ على البرودة اللازمة لعمل هذه الأجهزة.
  - يوجد جهاز مزود للطاقة الكهربائية (UPS) موصول بالأجهزة الخادمة الرئيسية لضمان استمرارية عمل هذه الأجهزة عند انقطاع التيار الكهربائي وعدم ضياع البيانات.
  - إن الموقع الخاص بالأجهزة الخادمة الرئيسية ومعدات الشبكة يجب أن يكون مغلق بالمفتاح ولا يسمح للموظفين بالدخول إليها إلا بإذن رسمي. كما أنه لا يسمح للشركات الخاصة بالدخول إلى أي الموقع إلا بإذن رسمي وبمرافقة أحد المخولين بالدخول للموقع.

سياسة حماية أنظمة المعلومات

تتعلق هذه السياسة بضمان حماية الأنظمة المحوسبة والتطبيقات والمنصات الالكترونية والمواقع الالكترونية من المخاطر السيبرانية، وتتضمن:

- إن كافة الأنظمة المحوسبة لا يتم الدخول إليها إلا من خلال اسم مستخدم وكلمة سر ، ولكل مستخدم صلاحيات يتم تحديدها من قبل المسؤول (مدير المديرية أو رئيس القسم المعني)، وذلك لحماية المعلومات من العبث أو الحذف أو التعديل المقصود أو غير المقصود، ولضمان عدم الإطلاع على المعلومات إلا للأشخاص المُصرح لهم بذلك.
- كما أن لمنصة البوابة الإلكترونية اسم مستخدم وكلمة سر لكل موظف.
- أما بالنسبة لمنصة الخدمات الإلكترونية فإنه لا يمكن الدخول للمنصة إلا بعد التسجيل وإرسال رمز تحقق من خلال رقم هاتف المستخدم أو البريد الإلكتروني الخاص به.
- بالنسبة لبرنامج إدارة المحتوى الخاص بالموقع الالكتروني أيضًا لا يتم الوصول له إلا من خلال اسم مستخدم وكلمة سر ، يتم تغييرها باستمرار ، وللمسؤول عن الموقع صلاحيات إنشاء مستخدمين حسب طبيعة عمل كل منهم بحيث يقوم بتحديد الصفحات والعمليات المسموح لهم بإجراؤها بالتنسيق مع المدير / المسؤول المعني.

سياسة إدارة هويات الدخول والصلاحيات

تتعلق هذه السياسة بضمان حماية الأمن السيبراني للوصول المنطقي إلى الأصول المعلوماتية والتقنية للدائرة من أجل منع الوصول غير المصرح به، وتقييد الوصول إلى ماهو مطلوب لإنجاز الأعمال المتعلقة بالدائرة، وتتضمن:

- لكل موظف في الدائرة اسم مستخدم وكلمة سر للدخول على جهاز الحاسوب الشخصي الخاص به والمربوط بالشبكة ولاستخدام البريد الإلكتروني، كما أن كلمة السر تنتهي صلاحيتها كل (40) يوم لإجبار الموظفين على تغييرها باستمرار.

- يوجد كلمات سر لكافة أنظمة المعلومات التطبيقية والمنصات حسب الصلاحيات الممنوحة للمستخدمين من قبل المديرية المعنية.
- تتطلب هذه السياسة حفظ كلمات السر الخاصة بالأجهزة الخادمة الرئيسية وبالأنظمة المحوسبة في مغلف خاص يتم حفظه في مكان خاص لا يمكن الوصول إليه من قبل الأشخاص غير المخولين.
- يجب التقيد بشروط كلمات السر الواردة في هذه السياسة وهي:
  - ألا تكون قد استخدمت مسبقاً من فترة قريبة.
  - ألا تكون سهلة التخمين، مثل اسم الشخص، أو تاريخ ولادته، أو رقم هاتفه، أو اسم سجل الدخول الإلكتروني للمستخدم.
  - ألا تكون من الكلمات المتداولة في القواميس أو اللغات المعروفة.
  - ألا تكون مبنية بحيث تُشكل في مجملها جملة واحدة كاملة من حلروف وأرقام متتابعة ومتسلسلة بشكل منطقي ومعروف للعامة.
  - أن تكون مركبة من الحروف والأرقام والرموز الخاصة، وبدون تكرار.
  - أن تكون طويلة بشكل كافٍ.
  - ألا تحتوي اختصارات معروفة مثل gov,jo,org,inc
  - أن يتم تغييرها بشكل دوري تحدده تعليمات الدائرة.
  - عدم استخدامها في أكثر من نظام.

سياسة أمن الأجهزة المحمولة

تتعلق هذه السياسة بضمان حماية أجهزة الدائرة المحمولة (بما في ذلك أجهزة الحاسب المحمول، والهواتف الذكية، والأجهزة الذكية اللوحية) من المخاطر السيبرانية. ولضمان التعامل بشكل آمن مع المعلومات الحساسة، والمعلومات الخاصة بأعمال الدائرة وحمايتها، أثناء النقل والتخزين، وعند استخدام الأجهزة الشخصية للعاملين في الدائرة.

- يتم منح الأجهزة المحمولة لمدراء المديريات ورؤساء الأقسام والمهندسين. كما لا يتم ربطها مع شبكة الدائرة الداخلية نهائيا إلا من خلال موظف متخصص من الدعم الفني.

سياسة حماية البريد الإلكتروني

تتعلق هذه السياسة بضمان حماية البريد الالكتروني الرسمي للدائرة من المخاطر السيبرانية، وتتضمن:

- يجب عدم استخدام البريد الرسمي إلا لأغراض العمل الرسمية ويمنع استخدامه للأغراض الشخصية.
- يجب شمول البريد الرسمي على أجهزة الحواسيب الشخصية ضمن سياسة النسخ الإحتياطي.

سياسة حماية البيانات والمعلومات

تتعلق هذه السياسة بضمان حماية السرية، وسلامة بيانات ومعلومات الدائرة ودقتها وتوافرها، وذلك وفقاً للسياسات والإجراءات التنظيمية للدائرة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

- يجب على الدائرة تصنيف المعلومات التي تتعامل بها وتتناقلها من حيث درجة السرية.
- عند اتلاف المعلومات فإنه يجب اتلافها بطريقة تتفق مع القوانين والتشريعات الحكومية.
- التدقيق الخاص بأمن المعلومات: يجب إجراء تدقيق داخلي على جميع الموارد المعلوماتية والسجلات، وتقوم وحدة الرقابة الداخلية بإجراء تدقيق داخلي إدارياً ومالياً.
- يجب على الدائرة إعداد تعهد "عدم الإفصاح عن المعلومات" للموظفين والتوقيع عليها.
- يجب توقيع الموظف على تعهد أو إقرار بأنه لا يحتفظ بأية معلومات سرية عند إنهاء الخدمة.
- على الموظف الالتزام بما يلي:
  - عدم تخطي الصلاحيات الممنوحة له في التعامل مع الموارد المعلوماتية في الدائرة.
  - عدم استغلال الموارد المعلوماتية في الدائرة لمنفعة أي جهة خارجية لغير غايات العمل الرسمي.
  - عدم انتحال هويات الموظفين الآخرين – عن طريق استعمال بطاقات مرورهم مثلاً – من أجل المنفعة الشخصية أو محاولة التسبب بإيذاء جهة ما أو منفعة جهة أخرى بشكل غير قانوني.

- المحافظة على الموارد المعلوماتية في الدائرة من سوء الاستعمال أو أية تهديدات أو مخاطر محتملة، بقدر الاستطاعة والحذر، وبالتوافق مع سياسة الاستعمال المقبول.
- تعليق بطاقة التعريف التي تُعبر عن هويته والصلاحيات المناطة به.
- تسليم كل ما بحوزته من بطاقات مرور ومفاتيح وكلمات مرور وأجهزة ووثائق عند انتهاء وظيفته أو سفره (أو مغادرته في إجازة) للجهة المسؤولة عن ذلك في الدائرة.
- التوقيع على تعهد للدائرة – عند انتهاء عقده – بأنه لا يحتفظ بأيٍّ من الموارد المعلوماتية المملوكة للدائرة وأنه يتحمل المسؤولية في حال ثبوت غير ذلك.
- عدم التعريف عن الوصف الوظيفي لأي جهة خارج الدائرة لغير ضرورة.

سياسة التشفير

تتعلق هذه السياسة بضمان الاستخدام السليم والفعال للتشفير بتشفير المعلومات السرية أثناء نقلها وتخزينها باستخدام إحدى خوارزميات التشفير المثبتة والمعتمدة عالمياً؛ لحماية الأصول المعلوماتية الإلكترونية للدائرة، وذلك وفقاً للسياسات، والإجراءات التنظيمية والمتطلبات التشريعية والتنظيمية ذات العلاقة.

سياسة إدارة النسخ الاحتياطية

تتعلق هذه السياسة بضمان حماية بيانات الدائرة ومعلوماتها، وكذلك حماية الإعدادات التقنية للأنظمة والتطبيقات الخاصة من الأضرار الناجمة عن المخاطر السيبرانية، وذلك وفقاً للسياسات والإجراءات والمتطلبات التشريعية والتنظيمية ذات العلاقة، وتتضمن:

- تزويد وزارة الاقتصاد الرقمي والريادة بخطة النسخ الاحتياطي الخاصة بالخوادم الرئيسية لدائرة الشؤون الفلسطينية والمُستضافة على السحابة الحكومية الالكترونية.
- شمول أنظمة المعلومات والبيانات وأجهزة الحواسيب الشخصية والبريد الالكتروني بآلية النسخ الاحتياطي.

سياسة إدارة الثغرات وتهديدات الأمن السيبراني

تتعلق هذه السياسة بضمان اكتشاف الثغرات التقنية في الوقت المناسب، ومعالجتها بشكل فعال، وذلك لمنع احتمالية استغلال هذه الثغرات من قبل الهجمات السيبرانية وتقليل ذلك، وكذلك تقليل الآثار المترتبة على أعمال الدائرة، وذلك من خلال التنسيق مع المركز الوطني للأمن السيبراني والاستجابة للتقارير الدورية الصادرة عنهم ومعالجة الثغرات الأمنية الموصى بها بالتنسيق مع وزارة الاقتصاد الرقمي والريادة والأطراف الخارجية المسؤولة عن البرمجيات والأنظمة ذات العلاقة بمحتويات التقارير (إن وُجدت).

سياسة الأمن السيبراني المتعلقة بالأطراف الخارجية

تتعلق هذه السياسة بضمان حماية أصول الدائرة من مخاطر الأمن السيبراني المتعلقة بالأطراف الخارجية (بما في ذلك خدمات الإسناد لتقنية المعلومات "Outsourcing" والخدمات المدارة "Managed Services") وفقاً للسياسات والإجراءات التنظيمية والمتطلبات التشريعية والتنظيمية ذات العلاقة، وتتضمن:

- عند الاستعانة بمزود خارجي لتوفير خدمات معينة للدائرة فإنه يجب على الدائرة إعداد اتفاقية "مستوى الخدمة" بحيث تشمل بند واضح عن "عدم الإفصاح بشكل غير مرخص عن المعلومات" وتوقيع المزود الخارجي عليها.
- عدم السماح للفنيين المعنيين من الطرف الخارجي باستخدام الأجهزة الخاصة بالدائرة بدون إذن رسمي وبدون رقابة من قبل المعنيين.
- عدم السماح للطرف الخارجي بالحصول على نسخ من الوثائق أو المستندات أو قواعد البيانات لأي سبب دوذ إذن رسمي مسبق يتضمن سبب الحصول على الوثائق أو البيانات وتعهد بعدم التصريح بها والتخلص منها حسب الأصول عند انتهاء الغاية التي أُخذت من أجلها.

سياسة الأمن السيبراني المتعلقة بالحوسبة السحابية والاستضافة

تتعلق هذه السياسة بضمان معالجة المخاطر السيبرانية، وتنفيذ متطلبات الأمن السيبراني للحوسبة السحابية، والاستضافة بشكل ملائم وفعّال، وتتضمن:

- التنسيق مع المعنيين من وزارة الاقتصاد الرقمي والريادة بحيث يتم إعطاء صلاحيات الوصول للأجهزة الخادمة الرئيسية المُستضافة على السحابة الحكومية الالكترونية من خلال IP address للموظفين المحددين من قبل مدير مديرية تكنولوجيا المعلومات وبكلمات سر مُحددة للمخولين فقط.
- يتم متابعة إجراء التحديثات الموصى بها من المركز الوطني للأمن السيبراني والخاصة بأنظمة التشغيل والبرمجيات والأدوات المستخدمة باستمرار.
- التأكد من وجود نسخة مُحدثة وفعالة من برنامج مضاد الفيروسات على جميع الأجهزة الخادمة الافتراضية.
- التأكد من شمول كافة الأجهزة بنظام النسخ الاحتياطي المذكور في سياسة إدارة النسخ الاحتياطية.

سياسة الحماية من البرمجيات الضارة

تتعلق هذه السياسة بضمان استخدام البرمجيات الخاصة بالحماية من البرمجيات الضارة والفيروسات، وتتضمن:

- تستخدم الدائرة برنامج خاص للحماية من الفيروسات، وتقوم بتنزيل أحدث الإصدارات بشكل مستمر، كما أن أجهزة جميع الموظفين مربوطة بجهاز خادم رئيسي خاص ببرنامج مضاد الفيروسات ليتم تحديث الملفات الخاصة به بشكل أوتوماتيكي دون الحاجة لتحديثه من قبل الموظف نفسه.
- إصدار تعميم يقضي بمنع استخدام أي وسيلة تخرين (فلاش أو CD) على أجهزة الدائرة إلا بعد فحصها من قبل أحد موظفي قسم الدعم الفني.

سياسة أمن أجهزة المستخدمين

تتعلق هذه السياسة بضمان حماية أجهزة المستخدمين من المخاطر السيبرانية، وتتضمن:

- التعامل مع أجهزة الحاسوب المكتبية بشكل يتوافق مع سياسات أمن وحماية المعلومات وتعليمات الدائرة.
- المستخدم مسؤول عن حفظ كلمة المرور الخاصة بالدخول إلى حاسوبه المكتبي بالتوافق مع سياسات كلمات المرور.
- المستخدم مسؤول عن إبلاغ الدعم الفني بأي مشكلة تصيب حاسوبه المكتبي، وعليه عدم محاولة إصلاحه بنفسه.
- عدم ربط أي جهاز أو وسيط تخزين أو معدات لاسلكية – مثل البلوتوث والـ (واي–فاي) – مع الشبكة المعلوماتية للدائرة، أو مع أيٍ من الأجهزة والمعدات الأخرى، أو استخدام المودم، بدون الحصول على موافقة مسبقة ومكتوبة من الإدارة العليا في الدائرة.
- عدم إحضار أو ربط أجهزة الحاسوب المكتبية التي يملكها المستخدم بالشبكة المعلوماتية الخاصة بالدائرة.
- عدم استخدام وسائط التخزين المتنقلة بدون فحصها ببرامج مكافحة الفيروسات.
- حفظ المعلومات والملفات على الأجهزة التي يحددها مدير النظام مثل خوادم الملفات بالتوافق مع سياسة أمن الشبكات.