

سياسة الحماية من البرمجيات الخبیثة والمكافحة الذكية للتهدیدات السيبرانية (الاصدار الأول)



المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات


إشارة المشاركة: برتقالي





بروتوكول الإشارة الضوئية (TRAFFIC LIGHT PROTOCOL TLP)




يُستخدم بروتوكول الإشارة الضوئية TLP لتصنيف المعلومات وآلية مشاركة واستخدام هذه المعلومات، ويضم البروتوكول أربعة ألوان (إشارات ضوئية) تفصيلها كالتالي:

أحمر - شخصي وسري لمتلقيها فقط 
لا يجوز لمتلقي المعلومات مشاركتها مع أي أطراف خارج منصة التبادل أو الاجتماع أو المحادثة التي تم الكشف عنها في الأصل.

برتقالي - مشاركة محدودة 
يمكن لمتلقي المعلومات مشاركتها مع الأشخاص المعنيين داخل الجهة فقط، أو مع من تخصه المعلومات لاتخاذ الإجراء الملائم، أو مع الذين يحتاجون إلى معرفة المعلومات لحماية أنفسهم أو منع المزيد من الضرر.

أخضر - مشاركة في نفس الجهة 
يمكن لمتلقي المعلومات مشاركتها داخل وخارج الجهة مع الأشخاص المعنيين، ولا يُسمح بنشرها أو تبادلها من خلال القنوات العامة.

أبيض - مشاركة غير محدودة 
يمكن لمتلقي المعلومات مشاركتها دون أية قيود ومن خلال قنوات الاتصال.



٣	تاريخ مراجعة السياسة
٤	التصديق على هذه السياسة
٤	١. نظرة عامة
٥	١,١ الغرض:
٥	١,٢ انطاق هذه السياسة:
٥	١,٣ التزام الإدارة:
٥	١,٤ لتوافق مع المعايير الدولية:
٦	٢. التعريفات
٧	٣. المهام والمسؤوليات
٩	٤. ضوابط سياسة الحماية من البرمجيات الخبيثة
٩	٤,١ الحماية من البرمجيات الخبيثة
١٠	٤,٢ المعلومات الخاصة بالمكافحة الذكية للتهديدات السيبرانية
١١	٤,٣ الاستثناءات

تاريخ مراجعة السياسة



التاريخ	الإصدار	التوصيف	واضع هذه السياسة
1/6/2022	1.0	تاريخ الإصدار	المركز الوطني للاستعداد لطوارئ (EG-CERT) الحاسبات والشبكات
	1.0	تاريخ سريان هذه السياسة	المركز الوطني للاستعداد لطوارئ (EG-CERT) الحاسبات والشبكات
		تاريخ المراجعة	

التصديق على هذه السياسة



التوقيع	الاسم	التاريخ	المُصدِّقون على هذه السياسة
			الإدارة العليا
			المديرون التنفيذيون
			مدير إدارة الدعم الأمني السبيرانى
			مدير إدارة تكنولوجيا المعلومات
			مدير إدارة التدقيق والمراجعة الداخلية



١. نظرة عامة

تنص هذه الوثيقة على سياسة للحماية من البرمجيات الخبيثة و المكافحة الذكية للتهديدات السيبرانية (Threat Intelligence) والتي تهدف إلى تنفيذ تدابير وإجراءات الحماية والوقاية من البرمجيات الخبيثة وحماية أصول المؤسسة والقيام بجمع وتحليل المعلومات المتعلقة بتهديدات أمن المعلومات وإصدار «المعلومات الخاصة بالتهديدات السيبرانية».

١,١ الغرض:

قام المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات (EG-CERT) بوضع هذه السياسة بهدف الحماية من البرمجيات الخبيثة والتوعية بالتهديدات السيبرانية حتى يمكن اتخاذ الإجراءات اللازمة للتخفيف من حدتها.

١,٢ نطاق هذه السياسة:

تُطبق هذه السياسة على كافة أصول وموارد تقنية المعلومات داخل المؤسسة. يتحمل جميع المتعاملين مع المؤسسة مسؤولية الالتزام بهذه السياسة.

١,٣ التزام الإدارة:

يقوم مدير إدارة تكنولوجيا المعلومات ومدير إدارة الدعم الأمني السيبراني بمراجعة هذه السياسة والموافقة عليها؛ وتدعم الإدارة العليا الغرض الذي تم وضعها من أجله. أي مخالفة لهذه السياسة قد يؤدي إلى اتخاذ إجراءات تأديبية ضد مرتكبيها والتي قد تشمل إيقاف الموظف المخالف عن العمل، أو تقييد وصوله لبعض النظم والمعلومات، أو توقيع عقوبة تشمل، على سبيل المثال لا الحصر، إنهاء خدمته.

١,٤ التوافق مع المعايير الدولية:

تم وضع هذه السياسة بناءً على المنشور الخاص (SP) رقم ٠٣-٨٠٠-٠١ الصادر من المعهد الوطني للمعايير والتقنية (NIST) ومعياري آيزو ٢٧٠٠١ (ISO ٢٧٠٠١) وتتوافق هذه السياسة أيضًا مع أفضل الممارسات الخاصة بضوابط أمن المعلومات (ISO ٢٧٠٠٢) (ISO ٢٧٠٠٢).



خطة استمرارية الأعمال (BUSINESS CONTINUITY) (PLAN)

يُقصد بها عملية توثيق مجموعة محددة مسبقاً من الإرشادات أو الإجراءات التي تنص على كيفية تحقيق استدامة واستمرار أداء مهام أعمال المؤسسة أثناء وبعد حدوث انقطاع أو عطل كبير في الخدمة.



الدفاع في العمق (DEFENSE IN DEPTH)

يُقصد به الدفاع الأمني متعدد المستويات من خلال الضوابط الأمنية المختلفة. وذلك على مستوى الأشخاص والتقنيات والقدرات التشغيلية.



المكافحة الذكية للتهديدات السيبرانية (THREAT INTELLIGENCE)

يُقصد بها المعلومات الخاصة بالتهديدات والمخاطر السيبرانية التي تم جمعها أو تحليلها أو تفسيرها أو تعزيزها حتى يتم توفير السياق والإطار المناسب لعملية صنع القرار.

٣. المهام والمسؤوليات



المهام والمسؤوليات	الموظف المعني
<ul style="list-style-type: none"> الموافقة على هذه السياسة واعتمادها رسميًا. إصدار التعليمات الإدارية الملزمة لكافة العاملين بالمؤسسة بتطبيق السياسات وكذلك وضع لوائح الجزاءات الخاصة بعدم تطبيق هذه السياسات بما لا يتعارض مع اللوائح والقوانين. 	الإدارة العليا
<ul style="list-style-type: none"> مراجعة هذه السياسة واعتمادها رسميًا. 	المسؤولون التنفيذيون
<ul style="list-style-type: none"> وضع الخطط والإجراءات والسياسات والتدابير بالتعاون مع إدارة تكنولوجيا المعلومات. مراجعة هذه السياسة وتحديثها دوريًا. تنفيذ ومراجعة الآليات اللازمة التي تدعم هذه السياسة. الحفاظ على أمن الأنظمة وحماية البيانات. إدارة ومتابعة وتحديث الأدوات الخاصة بالحفاظ على أمن الأنظمة والمعلومات. التعاون مع فريق تكنولوجيا المعلومات وفريق المراجعة الداخلية لتأمين الأصول الرقمية الخاصة بالمؤسسة. الموافقة أو الرفض على أي استثناء لضوابط هذه السياسة. 	فريق الدعم الأمني السيبراني
<ul style="list-style-type: none"> التأكد من معرفة الموظفين بسياسات التأمين الخاصة بالمؤسسة . تحديد المسؤوليات الخاصة بأمن المعلومات وبنود السرية في العقود. 	فريق الموارد البشرية

المهام والمسؤوليات	الموظف المعني
<ul style="list-style-type: none"> • التعاون مع فريق الدعم الأمني السيبراني لإصدار الخطط والإجراءات والتدابير اللازمة لتنفيذ هذه السياسة. • إبلاغ جميع موظفي المؤسسة بمهامهم ومسؤولياتهم الأمنية قبل منحهم إمكانية الوصول إلى البيانات والنظم الحساسة. • تنفيذ الآليات اللازمة التي يطلبها فريق الدعم الأمني السيبراني. 	<p>فريق تكنولوجيا المعلومات</p>
<ul style="list-style-type: none"> • مراجعة داخلية للضوابط الأمنية الخاصة بالسياسة وكفاءتها • تقييم وتعزيز جاهزية المؤسسة لأي هجمات سيبرانية • تقييم وإدارة المخاطر • التأكد من التوافق مع السياسات والمعايير. 	<p>فريق المراجعة الداخلية</p>
<ul style="list-style-type: none"> • التأكد من أن الموظفين المعنيين ملمون بهذه السياسة. 	<p>المديرون</p>
<ul style="list-style-type: none"> • يجب على الموظفين تطبيق هذه السياسة والتصرف وفقاً لها. 	<p>الموظفون</p>

٤. ضوابط سياسة الحماية من البرمجيات الخبيثة



٤,١ الحماية من البرمجيات الخبيثة:

- يجب أن يتم فحص أجهزة الكمبيوتر ووسائط التخزين الإلكترونية ببرامج مكافحة البرمجيات الضارة دورياً.
- يجب أن يتم فحص كل ما يتم تحميله من ملفات وتطبيقات وأي بيانات بتقنيات مكافحة البرمجيات الضارة.
- يجب منع استخدام أي برامج غير مصرح بها باستخدام تقنيات مثل (Application Allow-List).
- يجب كشف زيارة المواقع الضارة (باستخدام التقنيات المناسبة مثل قائمة المواقع المحظورة) ومنع ذلك.
- يتعين تنفيذ وتطبيق اجراءات إدارة الثغرات الإلكترونية.
- يجب مراعاة استخدام استراتيجية الدفاع في العمق ((defense in depth approach).
- يتعين وضع خطط وتحديد اجراءات استمرارية الأعمال والتشغيل للتعافي من هجمات البرمجيات الضارة، ويشمل ذلك عملية أخذ نسخ احتياطية للبيانات واستعادة البيانات والاحتفاظ بنسخ احتياطية غير متصلة بالإنترنت.
- يجب تحديد إجراءات الحماية من البرمجيات الضارة بما في ذلك التدريب على استخدامها.
- يتعين إنشاء قنوات مناسبة للتنبيه والإبلاغ عن أي كود ضار يتم رصده.
- يجب استخدام آليات الحماية من الرسائل المزعجة (SPAM) للحماية من رسائل البريد الضارة.
- يجب تدريب جميع الموظفين على كيفية تحديد البرمجيات الخبيثة والتخفيف من حدة أثارها المحتملة.
- يتعين الاطلاع المستمر على كل المستجدات في مجال البرمجيات الخبيثة وكيفية مكافحتها والوقاية منها.

٤,٢ المعلومات الخاصة بالمكافحة الذكية للتهديدات السيبرانية (Threat Intelligence):



- يجب القيام برصد وجمع وتحليل المعلومات الخاصة بالتهديدات الحالية أو المستجدة.
- يجب أن تكون المعلومات الخاصة بالتهديدات السيبرانية ذات صلة ومتعلقة في نطاق أنشطة المؤسسة والأصول الرقمية الخاصة بها.
- يجب أن توفر المعلومات الخاصة بالتهديدات السيبرانية رؤية ثابتة ودقيقة لوضع التهديدات لكل مؤسسة.
- يتعين على المؤسسة اتخاذ الإجراءات المناسبة وفقًا للمعلومات الخاصة بالتهديدات السيبرانية بسرعة وكفاءة.
- يجب تحديد مصادر المعلومات اللازمة ومتابعتها لإصدار التقارير الخاصة بالتهديدات السيبرانية.
- يتعين التواصل مع الموظفين المختصين واطلاعهم على المعلومات الخاصة بالتهديدات السيبرانية على أن تكون في شكل وتنسيق يسهل عليهم فهمه والتعامل معه.
- يجب إجراء عملية إضافة المعلومات التي تم جمعها من مصادر معلومات التهديدات السيبرانية (Threat Intelligence) إلى عمليات إدارة مخاطر أمن المعلومات كعملية إمداد وتغذية إضافية لضوابط الوقاية والكشف عن البرمجيات الخبيثة.
- يجب التأكد من أن كافة المعلومات المتعلقة بالتهديدات السيبرانية لا يتم تدوالها خارج نطاق المؤسسة الا بتصريح واذن مسبق من الإدارة العليا سواء كان ذلك من خلال الموظفين أو عبر طول الأمن السيبراني.

٤,٣ الاستثناءات:



يجب إبلاغ فريق الدعم الأمني بأي تغييرات مقترحة على النظام؛ يتعين أيضًا توثيق الموافقة على أي استثناء للضوابط والمواد الأساسية المنصوص عليها في هذه السياسة واعتمادها رسميًا من قبل مدير إدارة تكنولوجيا المعلومات. يجب أن يحدد أي استثناء ما يلي:

- طبيعة هذا الاستثناء.
- توضيح فعلي وحقيقي لضرورة الاستثناء.
- أي مخاطر ناتجة عن الاستثناء.
- ما يفيد موافقة مدير إدارة تكنولوجيا المعلومات على هذا الاستثناء.