وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

المبادئ التوجيهية الأمنية لاستخدام البرمجيات مفتوحة المصدر

الإصدار: 1.0

المؤلف: قسم السياسات والمعايير – وزارة المواصلات والاتصالات

تصنيف الوثيقة : عام

تاريخ النشر: مارس 2018

تاريخ الوثيقة:

التاريخ	وصف الاصدار	الاصدار
مارس 2018	نشر النسخة الاولى	1.0

المحتويات

التكليف القانوني:

ينص القرار الأميري رقم (8) لسنة 2016 بشأن تحديد تفويض وزارة المواصلات والاتصالات (المشار إليها فيما بعد باسم "الوزارة"") على أن تتمتع وزارة المواصلات والاتصالات بسُلطة الإشراف على قطاعات تكنولوجيا المعلومات والاتصالات داخل دولة قطر وتنظيمها وتطويرها بطريقة متوافقة مع متطلبات أهداف التنمية الوطنية، وذلك بهدف إيجاد بيئة مناسبة للمنافسة العادلة ودعم تطوير وتحفيز الاستثمار في تلك القطاعات؛ ومن أجل تأمين وزيادة كفاءة المعلومات والهياكل الأساسية التكنولوجية وتنفيذ برامج الحكومة الإلكترونية والإشراف عليها، بالإضافة إلى تحسين الوعي المجتمعي بأهمية تكنولوجيا المعلومات والاتصالات لتحسين حياة الفرد والمجتمع المحلي وبناء مجتمع قائم على المعرفة والاقتصاد الرقمي.

وتنص المادة (22) من القرار الأميري رقم (8) لسنة 2016 على دور الوزارة في حماية الهيكل الأساسي للمعلومات الوطنية الهامة عن طريق اقتراح وإصدار السياسات والمعايير وضمان الامتثال.

وقد أُعدت المبادئ التوجيهية الماثلة بمراعاة القوانين المعمول بها حاليًا في دولة قطر. وفي حالة نشوء أي اختلاف بين هذه الوثيقة وقوانين دولة قطر، تعطى الأسبقية لقوانين دولة قطر. ولذلك الغرض يُحذف ذلك البند من هذه الوثيقة، على أن تظل بقية الوثيقة سارية المفعول بدون التأثير على باقي الأحكام. وفي تلك الحالة ستكون التعديلات ضرورية لضمان الامتثال للقوانين ذات الصلة المعمول بها داخل دولة قطر.

مقدمة:

يعرف "الكود المصدري" في سياق تطبيقات الحاسوب بقائمة الأوامر/ النصوص البرمجية الموضوعة معًا لإنشاء تطبيق. وهو ذلك الجزء من البرنامج غير المرئي على الإطلاق لأغلب مستخدمي الحاسوب.

تُجرى أي تغييرات على منطق التطبيق أو مجموعة خصائصه أو مظهره أو إحساسه عن طريق تعديل "الكود المصدري للبرنامج". وعادة ما يعد هذا الكود سراً دفيناً لمطوري التطبيق كما يعتبر ملكية فكرية للمطورين/ المؤسسة، وغالبًا ما يكون مؤمنًا من خلال حقوق الملكية الفكرية وحقوق التأليف والنشر ...إلخ.

البرمجيات مفتوحة المصدر هي برمجيات يتيح مطوروها (أفراد و/أو مؤسسات) الكود المصدري للعامة بحيث يمكن لأي شخص فحصها وتعديلها وتحسينها وإعادة توزيعها. وتوزع تلك البرمجيات بشكل عام بموجب أنظمة ترخيص خاصة مثل

Common Creatives (CC), GNU General Public License (GNU GPL)...إلخ.

تقدم البرمجيات مفتوحة المصدر عدة فوائد بالإضافة إلى التحديات، ونوضح ذلك بتفاصيل إضافية أدناه.

الهدف:

إن الهدف من هذه المباديء التوجيهية هو تقديم التوجيه الأمني لأصحاب المصلحة التابعين لنا أثناء اختيار حلول برمجية مفتوحة المصدر. حيث ستساعد المؤسسات على فهم وتقييم المخاطر الأمنية المتعلقة بالبرمجيات مفتوحة المصدر وكيفية مجابهتها.

النطاق والجمهور المستهدف:

أي فرد أو مؤسسة تستخدم أو تضع في الاعتبار استخدام البرمجيات مفتوحة المصدر في عملياتها.

المبادئ التوجيهية:

ينطوي اتخاذ القرار إما باختيار البرمجيات مفتوحة المصدر أو البرمجيات مسجلة الملكية على الكثير من التعقيد ويتجاوز مجرد تعلق الأمر بالعوامل المالية. ويجب أن تتخذ المؤسسات قرارًا مستنيرًا مدروساً وتضع في الاعتبار العوامل التالية من بين العوامل الأخرى قبل اختيار البرمجيات مفتوحة المصدر.

أ- **التكلفة الإجمالية للملكية:** لا تعني "مفتوحة المصدر" أنها مجانية بالضرورة. وعلى الرغم من عدم وجود تكاليف للترخيص، فقد توجد رسوم للدعم الإضافي الذي قد تحتاج المؤسسات الحصول عليه وإصلاح الأعطال والتدريبات لتطوير المهارات داخل الفريق والعلاوات التي قد تحتاجها المؤسسات لاستقدام موظفين يتمتعون بتلك المهارات ...إلخ.

- **سهولة الاستخدام:** عادةً ما تكون البرمجيات مفتوحة المصدر غير سهلة الاستخدام، حيث يركز المطورون على المميزات بدلًا من سهولة الاستخدام.

- **الموارد الكُفئة:** يمكن أن تواجه المؤسسات تحديات في استقدام أو إعادة تدريب موظفيهم الحاليين على مجموعة المهارات اللازمة لدعم وتطوير البرمجيات مفتوحة المصدر الداخلية.

ب- **خارطة طريق المستخدم المستهدف:** يمكن أن تختار المؤسسات استخدام المنتج كما هو أو يكون لديها خيار تعديله لتحقيق احتياجات عملها نظرًا لتوافر الكود المصدري. وبدلًا عن ذلك، يمكن للمؤسسات أيضًا استخدام الكود المصدري كقاعدة للتوصل إلى تطوير جديد كامل مما يسمح لهم بتقليل وقت التطوير. ورغم ذلك، تحتاج المؤسسات إلى تقييم رخصة الكود المصدري، حيث تفوض بعض من رخص الاستخدام مفتوحة المصدر بنشر الكود المعدل بموجب رخصة مشابهة.

ج- **الدعم الفني المهني:** عادةً ما تكون البرمجيات مفتوحة المصدر مبادرة مجتمعية/ منتدى مفتوح، حيث لا يوجد أي شخص ملتزم بمساعدتك، وبالتالي يترتب على المؤسسات أن تصلح الأشياء بنفسها أو تنتظر الردود من مجتمع البرمجيات مفتوحة المصدر، ولا يمكن تحديد إطار زمني لاتفاقيات مستوى الخدمات. رغم ذلك، يُتاح الدعم الفني المهني لبعض مبادرات/ منتجات البرمجيات مفتوحة المصدر مثل لينوكس.

د- **الأمن:** من الخطورة أن تفترض أن البرمجيات مفتوحة المصدر مؤمنة ضمنيًا وآمنة الاستخدام. غير أنه، وبما أن الكود المصدري يكون ملكية عامة، فإنه يكون خاضعاً للمراجعة من قبل أي شخص من الشغوفين بالأمن لتحديد مواطن الضعف فيه. يقوم باحثون ومؤسسات أمنية متعددة (مبدأ الأعين المتعددة) بمراجعة الكود النظر إليه من منظوراتهم الخاصة. علاوة على ذلك، وبالنظر إلى أن الكود ملكية عامة، فإن مخاطر احتوائه على فيروسات حصان طروادة أقل بكثير. ومع ذلك، نتيجة لقلة المراقبة المركزية/ السلطة التي تقدم ضمانات الجودة/ الأمن حول الكود الموزع، فمن الممكن أن يقوم المستخدمون الخبثاء بدمج أو إفساد الكود ببرمجيات خبيثة/ فيروسات حصان طروادة نظرًا لتوافر الكود للعامة. علاوة على ذلك، يمكن أن تكون الاستغلالات المحتملة (تجارب إثبات المفاهيم وجاهزية الاستخدام) متوفرة بسهولة على الإنترنت بخصوص نقاط الضعف المعروفة والمنشورة للبرمجيات مفتوحة المصدر.

عند اتخاذ مؤسسة قرارًا بتوزيع واستخدام نظام البرمجيات مفتوحة المصدر، فإن عليها أن تضع في اعتبارها الضوابط الأمنية التالية لتوفير طبقة من الضمان لعملهم.

1- **الحوكمة:** يجب أن تضع المؤسسات سياسة شاملة تحكم استخدام البرمجيات مفتوحة المصدر. ويجب أن تشمل تلك السياسة – من بين أشياء أخرى – استخدام مقبول للبرمجيات مفتوحة المصدر ومستوى مقبول للإقدام على المخاطرة بخصوص البرمجيات مفتوحة المصدر. ويجب أن يكون تقييم المخاطر وفقًا للحد الأدنى لتغطية المخاطر المتعلقة بمتطلبات للترخيص والعمليات (دعم البرمجيات واستقرارها) والأمن (نقاط الضعف والاستغلالات المعروفة).

2- **جرد الأصول:** يجب أن تحتفظ المؤسسات بقائمة مفصلة بالبرمجيات مفتوحة المصدر المستخدمة في المؤسسة؛ بتقديم أمثلة مفصلة (عدد/ كمية) للاستخدام والإصدارات ...إلخ. حيث إن البرمجيات مفتوحة المصدر تستخدم كمكون لتطبيقك الداخلي، يجب توصيل البيانات لتحديد أي المكونات يعد من البرمجيات مفتوحة المصدر وأي الإصدارات مستخدمة حاليًا. ويجب أن تحتوي قائمة الجرد على المكتبات وأطر العمل والبرمجيات الوسيطة والتطبيقات. كما يجب الاحتفاظ بموجز لكل برنامج مفتوح المصدر يحتوي على أصل الكود ومكان الحصول على التحديثات وعدد مرات إطلاق المجتمع لإصدارات جديدة.

3- **التوثيق:** حيث إن البرمجيات مفتوحة المصدر تستخدم كمكون لتطبيقك الداخلي، يجب الاحتفاظ بتوثيق شامل للمكونات المستخدمة. ويتضمن ذلك المكتبات وأطر العمل والبرمجيات الوسيطة والتطبيقات.

4- **سجل كود المصدر:** الاحتفاظ بسجل لكود المصدر الخاص بالبرمجيات مفتوحة المصدر الموزعة في المؤسسة.

5- **البرمجيات مفتوحة المصدر على القائمة البيضاء:** يجب أن تكون برمجيات المصدر المفتوح مؤهلة بعد إجراء اختبارات سهولة الاستخدام والاستقرار والأمان ذات الصلة. وتُستخدم البرمجيات مفتوحة المصدر المعتمدة مسبقًا والمؤهلة وتُوزع في المؤسسة.

6- **ضوابط خط الأساس:** يجب معاملة أي برمجيات مفتوحة المصدر كأي نظام معلومات آخر موزع في مشروع، ويجب الامتثال لخط الأساس المعني بالكامل والضوابط الموصى بها الموضحة في سياسة تأمين المعلومات الوطنية متضمنة تصنيفها.

7- **إدارة المخاطر:** يجب أن تُجري المؤسسات تقييم المخاطر للبرمجيات مفتوحة المصدر، بناءً على أهمية الخدمات التي ستقدمها وتنفيذ الضوابط اللازمة لإدارة أي مخاطر قد تنشأ.

8- **تثبيت البرمجيات مفتوحة المصدر:** يجب أن تمتثل أي برمجيات مفتوحة المصدر مثبتة/ موزعة لإجراء نظام التثبيت في المؤسسة. ويجب أن يضمن ذلك:

أ- توزيع البرمجيات مفتوحة المصدر المدرجة على القائمة البيضاء فقط في المؤسسة.

ب- فحص جميع التوزيعات واعتمادها من خلال نظام توزيع رسمي/ عملية تغيير إداري.

ج- إدراج جميع التوزيعات في سجل الأصول.

د- قيام الأفراد المفوضين فقط مثل إداريي النظام بتثبيت/ توزيع البرمجيات مفتوحة المصدر.

هـ- استخدام البرمجيات مفتوحة المصدر من مواقع موثوقة ومؤتمنة. يُفضل، حينما أمكن، أن يكون كود المصدر ثنائي. ومن الجيد دائمًا تنزيل كود المصدر، والتحقق من المجموعات الاختيارية MD5 المقدمة. ومن أمثلة المواقع الموثوقة على النحو الموصى به من مبادرة المصدر المفتوح: freshmeat.net, sourceforge.net, odir.com, developer.berlios.de, bioinformatics.org

و- التأكد من اختبار البرمجيات مفتوحة المصدر وتحديثها بآخر الإصلاحات.

9-**الأمن:** إجراء التقييم الأمني للتعرف على وتحديث أي نقاط ضعف في البرمجيات مفتوحة المصدر. بخصوص التطبيقات الهامة، يُوصى بإجراء مجموعة من التحليلات الآلية الثابتة (فحص الكود المصدري) والتحليلات الديناميكية للوقوف على نقاط الضعف في التطبيقات الفردية. ويجب على المؤسسة عند تحديد نقاط الضعف أن تقوم بـ:

أ- معرفة ما إذا كان هناك إصلاح أو نسخة محدثة متاحة لإصلاح نقطة الضعف المحددة.

ب- طلب المساعدة من مجتمع المصادر المفتوحة، مع الحذر وتحمل مسؤولية الإفصاح. نشر المشاكل في المجتمع وانتظار مساعدة أحد الأعضاء في حل المشكلة.

ج- إصلاحها بنفسك. استخدم مصادر التطوير الخاصة بك أو بطرف آخر لحل المشاكل.

10- **حماية التطبيق:** مثل أي برنامج آخر، يجب تهيئة البرمجيات مفتوحة المصدر بطريقة آمنة.

أ- إلغاء الخدمات غير المرغوب بها.

ب- يجب إزالة/ تعطيل المكتبات وواجهة برمجة التطبيقات ومكتبة الربط الديناميكي من بيئة التطوير.

ج- ضرورة تقيد تصريحات المستخدمين بأقل الامتيازات والحاجة للحصول على نموذج.

د- استخدام استراتيجية الدفاع في العمق لإدراج جميع الإجراءات الممكنة التي يلزم اتخاذها لجميع البرمجيات مفتوحة المصدر مع المنتجات الأخرى في الشبكة.

11- **إدارة التحديثات:** يجب أن تراقب إدارة التحديثات في الشركة وتحديث حزمة الإصلاحات الصادرة للبرمجيات مفتوحة المصدر.

أ- تفقد المجتمع المتعلق بالكود مفتوح المصدر الخاص بك. حيث تحتوي تلك المجتمعات على أنظمة تتبع الأخطاء البرمجية والقوائم البريدية التي تقدم معلومات حول المشاكل الأمنية المعروفة بالإضافة إلى آخر الأخبار والاستغلالات.

ب- عند تحديد نقطة ضعف جديدة، يجب أن تستكشف المؤسسة استراتيجيات تخفيف جديدة يمكن تنفيذها حتى يتوفر تحديث لها.

ج- عند إطلاق تحديث، قم باختبار ذلك التحديث من حيث استقراره وإمكانية تطبيقه في بيئة الاختبار الخاصة بك قبل توزيعه على أنظمة الإنتاج الخاصة بك.

د- الاحتفاظ بنهج مقيد بإطار زمني لتحديث جميع نقاط الضعف الخاصة بالبرمجيات مفتوحة المصدر القائمة.

12- **الامتثال:** يجب التحقق – من وقت لآخر – من قوائم جرد البرمجيات مفتوحة المصدر لضمان الامتثال لسياسة استخدام البرمجيات مفتوحة المصدر. ويمكن استخدام منتجات التحليل التركيبي للبرمجيات مفتوحة المصدر لتحليل تركيب التطبيق للكشف عن المكونات المعروف عنها احتوائها على نقاط ضعف أمنية و/أو وظيفية أو التي تتطلب ترخيص ملائم.

13- **استمرارية الأعمال/ بناء القدرات:** يجب أن تضمن المؤسسات تمتع موظفيها بالمهارات المتعلقة اللازمة للاحتفاظ ببرمجيات مفتوحة المصدر. حيث يجب تقديم التدريبات بانتظام وتوزيع المهارات لتجنب حدوث أي عطل. كما يجب تطوير قواعد المعرفة الخاصة بالبرمجيات مفتوحة المصدر والاحتفاظ بها في المؤسسة.

ملحق أ- ترخيص البرمجيات مفتوحة المصدر:

تُصنف البرمجيات مفتوحة المصدر بشكل عام كاختيارية أو تبادلية (تقييدية) أو في موقع متوسط بين هذين النوعين، وذلك بناءً على طبيعة التقييدات والالتزامات الواردة في الرخصة.

الرخص الاختيارية مفتوحة المصدر: وتتميز تلك الرخص بشكل عام بواجبات أكثر تساهلًا، وقد تشمل السماح بالتوزيع الثانوي ما دام الموزع يقدم الإسناد لذلك أو السماح بالبدائل البرمجية الثانوية أو التحسينات حتى تظل مسجلة الملكية. وتسهل المرونة قدرة المستخدمين النهائيين أو المرخصين على دمج البرمجيات المرخص بها في المنتجات المشتقة.

أمثلة: رخصة إم آي تي، رخصة أباتشي للبرمجيات، توزيعة برمجيات بيركلي.

الرخص التبادلية أو التقييدية مفتوحة المصدر: تتسم تلك الرخص بشكل عام بفرض قيود والتزامات أكثر صرامة على المستخدمين النهائيين أو مرخصي البرمجيات مفتوحة المصدر. وتتمثل السمات المميزة للرخصة التبادلية مفتوحة المصدر في ما يدعى بشرط "الحقوق المتروكة". ويلزم شرط الحقوق المتروكة من يقومون بإنشاء الكود وتوزيعه فيما بعد بأن يقوموا بذلك بموجب نفس الشروط والأحكام للإصدار الأصلي من البرنامج مفتوح المصدر، حتى عند تعديل ذلك البرنامج. بالإضافة إلى ذلك، سوف تتطلب الرخص مفتوحة المصدر – التي تحتوي على التزامات الحقوق المتروكة– عادةً من المرخصين كشف كود المصدر الأساسي أو إتاحته عند طلب ذلك من الآخرين. ويمكن أن تؤدي التزامات الحقوق المتروكة إلى التعرض لمخاطر فشل المرخص له في مراقبة الشروط والأحكام التي تحكم المكونات مفتوحة المصدر المدمجة في كود برنامج المرخص له.

مثال: رخصة GNU's Not Unix General Public License