



جمعية البر الخيرية بأم الدوم
تحت إشراف وزارة الموارد البشرية
والتنمية الاجتماعية برقم 413



سياسة إدارة حزم التحديات والإصلاحات

٢٠٢٠م





الأهداف

تهدف هذه السياسة إلى تحديد متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بإدارة حزم التحديثات والإصلاحات للأنظمة والتطبيقات وقواعد البيانات وأجهزة الشبكة وأجهزة معالجة المعلومات الخاصة بجمعية البر الخيرية بأم الدوم، لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

تتبع هذه السياسة المتطلبات التشريعية والتنظيمية الوطنية وأفضل الممارسات الدولية ذات العلاقة، وهي مطلب تشريعي كما هو مذكور في الضابط رقم ٢-٣-٣-٣ من الضوابط الأساسية للأمن السيبراني (ECC-2018:1) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأنظمة والتطبيقات وقواعد البيانات وأجهزة الشبكة وأجهزة معالجة المعلومات وأجهزة وأنظمة التحكم الصناعي الخاصة بجمعية البر الخيرية بأم الدوم، وتنطبق على جميع العاملين في جمعية البر الخيرية بأم الدوم.

بنود السياسة

1. يجب إدارة حزم التحديثات والإصلاحات (Patch Management) بشكل يضمن حماية الأنظمة والتطبيقات وقواعد البيانات وأجهزة الشبكة وأجهزة معالجة المعلومات.
2. يجب تنزيل حزم التحديثات والإصلاحات من مصادر مرخصة وموثوقة وفقاً للإجراءات المتبعة داخل جمعية البر الخيرية بأم الدوم.
3. يجب استخدام أنظمة تقنية موثوقة وأمنة لإجراء مسح دوري للكشف عن الثغرات وحزم التحديثات ومتابعة تطبيقها.
4. يجب على مسؤول تقنية المعلومات اختبار حزم التحديثات والإصلاحات في البيئة الاختبارية (Test Environment) قبل تثبيتها على الأنظمة والتطبيقات وأجهزة معالجة المعلومات في بيئة الإنتاج (Production Environment)، للتأكد من توافق حزم التحديثات والإصلاحات مع الأنظمة والتطبيقات.





5. يجب وضع خطة للاسترجاع (Rollback Plan) وتطبيقها في حال تأثير حزم التحديثات والإصلاحات سلباً على أداء الأنظمة أو التطبيقات أو الخدمات.
6. يجب على اللجنة الإشرافية للأمن السيبراني التأكد من تطبيق حزم التحديثات والإصلاحات دورياً.
7. يجب منح الأولوية لحزم التحديثات والإصلاحات التي تعالج الثغرات الأمنية حسب مستوى المخاطر المرتبطة بها.
8. يجب جدولة التحديثات والإصلاحات بما يتماشى مع مراحل الإصدارات البرمجية التي يطرحها المورد.
9. يجب تنصيب التحديثات والإصلاحات مرة واحدة شهرياً على الأقل للأنظمة الحساسة المتصلة بالإنترنت، ومرة واحدة كل ثلاثة أشهر للأنظمة الحساسة الداخلية. (3-1-3-2-CSCC)
10. يجب تنصيب التحديثات والإصلاحات لأصول التقنية على النحو التالي:

مدة التكرار لتنصيب التحديثات		نوع الأصل
الأصول المعلوماتية والتقنية للأنظمة الحساسة	الأصول المعلوماتية والتقنية	
شهرياً	شهرياً	أنظمة التشغيل
شهرياً	ثلاثة أشهر	قواعد البيانات
شهرياً	ثلاثة أشهر	أجهزة الشبكة
شهرياً	ثلاثة أشهر	التطبيقات

11. يجب أن تتبع عملية إدارة التحديثات والإصلاحات متطلبات عملية إدارة التغيير.
12. في حال وجود ثغرات أمنية ذات مخاطر عالية، يجب تنصيب حزم التحديثات والإصلاحات الطارئة وفقاً لعملية إدارة التغيير الطارئة (Emergency Change Management).





١٣. يجب تنزيل التحديثات والإصلاحات على خادم مركزي (Server Centralized Patch Management) قبل تنصيبها على الأنظمة والتطبيقات وقواعد البيانات وأجهزة الشبكة وأجهزة معالجة المعلومات، ويُستثنى من ذلك حزم التحديثات والإصلاحات التي لا يتوفر لها أدوات آلية مدعومة.
١٤. بعد تنصيب حزم التحديثات والإصلاحات، يجب استخدام أدوات مستقلة وموثوقة للتأكد من أن الثغرات تمت معالجتها بشكل فعال.
١٥. يجب استخدام مؤشر قياس الأداء (Key Performance Indicator "KPI") لضمان التطوير المستمر لإدارة حزم التحديثات والإصلاحات.
١٦. يجب مراجعة سياسة إدارة حزم التحديثات والإصلاحات وإجراءاتها سنوياً، وتوثيق التغييرات واعتمادها.

الأدوار والمسؤوليات

١. راعي ومالك وثيقة السياسة: مسؤول تقنية المعلومات.
٢. مراجعة السياسة وتحديثها: مسؤول تقنية المعلومات.
٣. تنفيذ السياسة وتطبيقها: مسؤول تقنية المعلومات.

الالتزام بالسياسة

١. يجب على مسؤول تقنية المعلومات ضمان التزام جمعية البر الخيرية بأم الدوم بهذه السياسة بشكل مستمر.
٢. يجب على مسؤول تقنية المعلومات في جمعية البر الخيرية بأم الدوم الالتزام بهذه السياسة.
٣. قد يُعرض أي انتهاك لهذه السياسة صاحب المخالفة، إلى إجراء تأديبي؛ حسب الإجراءات المتبعة في جمعية البر الخيرية بأم الدوم.





المحتويات

الصفحة	الموضوع
٢	الأهداف
٢	نطاق العمل وقابلية التطبيق
٢	بنود السياسة
٤	الأدوار والمسؤوليات
٤	الالتزام بالسياسة

