نشرة إرشادية عن أمن البيانات في إدارة البيانات التشغيلية

مارس 2024

بترجمة النشرة الإرشادية هذه بدعم من منظمة كلير قلوبال (CartONG) ساهمت منظمة كارت أو إن جي (Global CLEAR) ووزارة أوروبا والشؤون الخارجية الفرنسية.

مقدمة

يعد أمن البيانات عنصر رئيسي من عناصر مسؤولية الحفاظ على البيانات وهي: الإدارة الآمنة والأخلاقية والفعَّالة للبيانات من أجل الاستجابة التشغيلية. يتضمن مجموعة من التدابير المادية والتقنية والإجرائية التي تحفظ سرية البيانات وسلامتها وإتاحتها وتحول دون فقدانها أو إتلافها أو تعديلها أو الحصول عليها أو الكشف عنها عن طريق الخطأ أو عمدًا أو بشكل غير قانوني أو دون تصريح.

تقدم النشرة الإرشادية هذه مجموعة من الإجراءات الموصى بها لأمن البيانات في إدارة البيانات التشغيلية. ينبغي تنفيذ الإجراءات بما يتوافق مع الولايات المؤسسية والسياسات والأطر القانونية والتنظيمية ذات الصلة.

إدارة آمنة لكلمة المرور

- أمن أجهزتك وحساباتك بكلمات مرور قوية تتضمن أرقام وأحرف كبيرة وصغيرة ورموز وضمِّن لكل كلمة مرور 16 حرف أو رمز على الأقل مكَّن المصادقة متعددة العوامل لجميع الحسابات.
- لا تعيد استخدام نفس كلمة المرور في حسابات أخرى.
- لا تخزن كلمات المرور الخاصة بك في مكان ظاهر(مثل دفتر الملاحظات) أو رقميًا (في ملف على جهازك) ولا تشاركها مع الآخرين.
- لا تفَّعل خاصية « تذكرني» لكلمة المرور في التطبيقات والمتصفحات.
- غيِّر كلمات مرور حساباتك على الإنترنت فورًا إذا فقدت جهازك أو سُرق.

استخدام برامج مكافحة الفيروسات/البرامج الضارة

- تأكد من أن لديك برامج مناسبة لمكافحة الفيروسات/البرامج الضارة على أجهزتك.
- إذا كانت لديك أسئلة حول الأدوات المناسبة أو كيفية تهيئتها فراجع أخصائي تقنية المعلومات في مكتبك.

تحديث البرمجيات وأنظمة التشغيل

- تحقق باستمرار من تحديث جهازك وبرامجك وتطبيقاتك وإضافات المتصفح وفعِّل التحديثات التلقائية لنظام التشغيل.
- استخدم متصفحات إنترنت مثل كروم (Firefox) أو فايرفوكس (Chrome) والتي تتلقى تحديثات أمان تلقائية.
- أغلق أجهزتك في نهاية اليوم لتفعيل التحديثات والحماية من الهجمات الإلكترونية.

تجنب عمليات الاحتيال الإلكتروني والنقر على الروابط المجهولة

- عند تلقي رسائل بريد إلكتروني أو رسائل مشبوهة، تحقق دائمًا من عنوان المرسل/معلومات الاتصال وانقر فقط على الروابط أو المرفقات التي تثق في مرسلها.
- لا ترد على رسائل البريد الإلكتروني المشبوهة أو تعيد إرسالها إلى زملائك.
- أبلغ فريق دعم تقنية المعلومات عن أي نشاط مشبوه.

استخدام الأجهزة المحمولة بحرص ومسؤولية

- استخدم أجهزة منفصلة لأغراض العمل قدر الإمكان. احتفظ بأجهزة عملك بمكان يكون آمن في جميع الأوقات وتجنب حملها والتجول بها دون داعٍ.
- استخدم أدوات المراسلة المعتمدة من قبل مؤسستك والتي توفر التشفير الآمن من طرف إلى طرف.
- أطفئ اتصال البلوتوث قدر الإمكان وقلل الاتصال به.
- معتمدة من مؤسستك عند عملك على الانترنت. سجِّل خروجك من حساباتك إذا كنت تستخدم جهاز حاسب (VPN) استخدم شبكة افتراضية خاصة أو جهاز مشترك.
- عطِّل خواص المؤشرات الحيوية لإلغاء القفل كالتعرف على الوجه - خاصة عند التنقل.

حماية البيانات الحساسة وتقليل استخدام البيانات

- احتفظ **بسجل أصول البيانات الذي يشير إلى مستوى حساسية كل نوع من البيانات التي يديرها مكتبك. استعرض مستويات حساسية المعلومات باستمرار**.
- اجمع الحد الأدنى فقط من البيانات المطلوبة لتحقيق أهداف نشاط معين من أنشطة إدارة البيانات.
- احتفظ فقط بالبيانات الحساسة الضرورية لتحقيق الهدف الذي تدار من أجله وحسب ما تقتضيه التوجيهات والقوانين واللوائح المعمول بها.
- انقل وخزِّن البيانات باستخدام الأدوات والقنوات المعتمدة من مؤسستك (محليًا على خادم المؤسسة أو الحاسب المكتبي أو الحاسب المحمول أو على الخوادم والنظم التي تُشغّل عن بعد من خلال تطبيقات مثل (OneDrive و SharePoint وTeams).
- عيِّن كلمات مرور لحماية ملفات الوورد والبي دي أف والاكسل (Word Excel, PDF) التي تحتوي على بيانات حساسة ، وشارك كلمات مرور المستندات عن طريق قنوات اتصال منفصلة (يعني كإرسال رسالة نصية (تحتوي على كلمة مرور لمستند مرسل عبر البريد الإلكتروني.
- قلل وأدر جيدًا عدد الأشخاص القادرين على الوصول إلى البيانات الحساسة.
- حدد جدول زمني لحفظ واتلاف جميع البيانات المدُارة واستخدم الأدوات المناسبة للإتلاف.
- شفِّر رسائل بريدك الإلكتروني.

المصادر الرئيسية

- **التوجيه التنفيذي للجنة الدائمة المشتركة بين الوكالات بشأن مسؤولية البيانات في العمل الإنساني**
- **مذكرة توجيهية عن إدارة حوادث البيانات**
- **نشرة إرشادية عن الاستخدام المسؤول لأدوات المؤتمرات الإلكترونية**

لمزيد من المعلومات حول إدارة البيانات الحساسة في العمليات الإنسانية، قم بزيارة
صفحة مسؤولية الحفاظ على البيانات الموجودة في موقع المركز على الانترنت أو اتصل بفريقنا على البريد الإلكتروني التالي:
centrehumdata@un.org