Digital Data Security Management Guidelines

डिजिटल डेटा सुरक्षा प्रबंधन दिशानिर्देश

ए ग

1. अभिगम नियंत्रण

- प्रत्येक उपयोगकर्ता को केवल न्यूनतम आवश्यक अधिकार दें।
- सभी महत्वपूर्ण प्रणालियों के लिए बहु-कारक प्रमाणीकरण लागू करें।
- अनावश्यक अनुमति को समय-समय पर रद्द करें।

2. डेटा वर्गीकरण और भंडारण

- डेटा को सार्वजनिक, आंतरिक, गोपनीय और प्रतिबंधित श्रेणियों में विभाजित करें।
- संवेदनशील डेटा को संग्रह और संचार के दौरान एन्क्रिप्ट करें।
- बैकअप को सुरक्षित और भौगोलिक रूप से अलग स्थानों पर रखें।

3. नेटवर्क और सिस्टम सुरक्षा

- संदिग्ध गतिविधियों की निगरानी के लिए फ़ायरवॉल और घुसपैठ पहचान प्रणाली का उपयोग करें।
- ऑपरेटिंग सिस्टम और अनुप्रयोगों को समय पर अपडेट करें।
- नेटवर्क को खंडित करें ताकि संभावित

Guide de Gestion de la Sécurité des Données Numériques

Ce guide présente des pratiques clés pour protéger les données numériques personnelles, professionnelles et publiques face à l'augmentation des menaces cybernétiques.

1. Contrôle d'Accès
- Accorder à chaque utilisateur le minimum de droits requis.
- Mettre en place une authentification multifacteur pour les systèmes critiques.
- Vérifier régulièrement les accès et supprimer ceux qui sont inutiles.

2. Classification et Stockage des Données
- Classer les données en catégories : publiques, internes, confidentielles, restreintes.
- Chiffrer les données sensibles au repos et lors du transfert.
- Conserver les sauvegardes dans des lieux sécurisés et géographiquement distincts.

3. Protection Réseau et Système
- Installer des pare-feux et systèmes de détection d'intrusion.
- Maintenir les systèmes et applications à jour.
- Segmenter les réseaux pour limiter la propagation d'incidents.

4. Réponse aux Incidents et Surveillance
- Établir un plan de réponse aux incidents.
- Surveiller les journaux en temps réel pour identifier les anomalies.
- Signaler rapidement toute violation aux autorités compétentes.

5. Sensibilisation et Formation du Personnel
- Offrir des formations régulières en cybersécurité.
- Insister sur la détection de hameçonnage et la manipulation sécurisée des données.
- Encourager le signalement immédiat des activités suspectes.

6. Conformité et Révision
- Respecter le RGPD et autres lois locales de protection des données.
- Effectuer un audit de sécurité et une analyse des risques chaque année.
- Mettre à jour le guide pour répondre aux menaces émergentes.

Ces mesures contribuent à réduire les risques et à garantir l'intégrité des informations numériques.

دليل إدارة أمان البيانات الرقمية

يوفر هذا الدليل ممارسات أساسية لحماية البيانات الرقمية الشخصية والتجارية والعامة في ظل التزايد المستمر للتهديدات الإلكترونية.

1. التحكم في الوصول
- منح كل مستخدم أدنى مستوى من الصلاحيات اللازمة فقط.
- تفعيل المصادقة متعددة العوامل للأنظمة الحساسة.
- مراجعة الأذونات بشكل دوري وإلغاء غير الضروري منها.

2. تصنيف وتخزين البيانات
- تصنيف البيانات إلى عامة، داخلية، سرية ومقيدة.
- تشفير البيانات الحساسة أثناء التخزين والنقل.
- حفظ النسخ الاحتياطية في مواقع آمنة ومنفصلة جغرافيًا.

3. حماية الشبكات والأنظمة
- استخدام جدران الحماية وأنظمة كشف التسلل لمراقبة الأنشطة غير العادية.
- تحديث أنظمة التشغيل والتطبيقات بانتظام.
- تقسيم الشبكات للحد من انتشار أي اختراق محتمل.

4. الاستجابة للحوادث والمراقبة
- إعداد خطة موثقة للاستجابة للحوادث.
- مراقبة السجلات في الوقت الحقيقي لاكتشاف الأنماط غير الطبيعية.
- إبلاغ السلطات المختصة فور حدوث أي خرق.

5. توعية وتدريب الموظفين
- تقديم تدريبات دورية على الأمن السيبراني.
- توعية حول اكتشاف محاولات التصيد والتعامل الآمن مع البيانات.
- تشجيع الإبلاغ الفوري عن أي أنشطة مريبة.

6. الامتثال والمراجعة
- الالتزام بالقوانين مثل اللائحة العامة لحماية البيانات وغيرها من التشريعات المحلية.
- إجراء تدقيق أمني وتقييم للمخاطر سنويًا.
- تحديث هذه الإرشادات باستمرار لمواجهة التهديدات المستجدة.

تساعد هذه الإجراءات على تقليل المخاطر وضمان سلامة المعلومات الرقمية على المدى الطويل.