

# **Digital Data Security Management Guidelines**

*These guidelines provide essential practices to protect personal, corporate, and public digital data in an era of growing cyber threats.*

## **1. Access Control**

- Grant the least privilege necessary to every user.**
- Apply multi-**

本指南为在网络威胁日益增长的时代中保护个人、企业及公共数字数据提供关键措施。

#### 1. 访问控制

- 仅授予用户最低必要权限。
- 关键系统必须启用多因素身份验证。
- 定期审查并撤销不必要的访问权限。

#### 2. 数据分类与存储

- 按公共、内部、机密和严格限制四类进行分类。
- 在静态存储与传输中均加密敏感数据。
- 备份应安全存放并与生产环境分离。

#### 3. 网络与系统防护

- 部署防火墙和入侵检测系统以监测异常活动。
- 及时更新操作系统与应用程序补丁。
- 进行网络分段以限制入侵传播范围。

#### 4. 事件响应与监控

- 制定完善的安全事件响应计划。
- 实时监控日志以发现异常模式。
- 发生泄露时立即向主管部门报告。

#### 5. 员工意识与培训

- 定期开展网络安全培训。
- 强调防范钓鱼攻击和安全数据操作。
- 鼓励立即报告可疑事件。

#### 6. 合规与审查

- 遵守 GDPR、网络安全法等相关法规。
- 每年执行安全审计和风险评估。
- 持续更新指南以应对新兴威胁。

通过落实上述措施，可有效降低风险并保障数字信息的长期完整性与可信度。

## ड ड ल                    निस नस

यह दिशानिर्देश बढ़ते साइबर खतरों के युग में व्यक्तिगत, व्यावसायिक और सार्वजनिक डिजिटल डेटा की सुरक्षा के लिए आवश्यक उपाय प्रदान करता है।

### 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 फायरवॉल और घुसपैठ पहचान प्रणाली का उपयोग करें।
- ऑपरेटिंग सिस्टम और अनुप्रयोगों को समय पर अपडेट करें।
- नेटवर्क को खंडित करें ताकि संभावित हमलों का प्रसार सीमित हो।

### 4. घटना प्रतिक्रिया और निगरानी

- लिखित घटना प्रतिक्रिया योजना बनाएँ।
- असामान्य पैटर्न का पता लगाने के लिए लॉग की रीयल-टाइम निगरानी करें।
- डेटा उल्लंघन होने पर संबंधित प्राधिकरण को तुरंत सूचित करें।

### 5. कर्मचारी जागरूकता और प्रशिक्षण

- सभी कर्मचारियों के लिए नियमित साइबर सुरक्षा प्रशिक्षण प्रदान करें।
- फ्रिशिंग से बचाव और सुरक्षित डेटा प्रबंधन पर जोर दें।
- संदिग्ध घटनाओं की अव्याकृत रिपोर्टिंग को प्रोत्साहित करें।

### 6. अनुपालन और समीक्षा

- GDPR और स्थानीय डेटा संरक्षण कानूनों का पालन करें।
- वार्षिक सुरक्षा ऑडिट और जोखिम मूल्यांकन करें।
- नए खतरों को ध्यान में रखते हुए दिशानिर्देश नियमित रूप से अपडेट करें।

इन उपायों को अपनाकरे

## **Guía para la Gestión de la Seguridad de Datos Digitales**

**Esta guía establece prácticas esenciales para proteger datos digitales personales, corporativos y públicos frente al creciente número de amenazas ciberneticas.**

### 1. Control de Acceso

- Otorgar a cada usuario solo el mínimo privilegio necesario.
- Implementar autenticación multifactor para sistemas críticos.
- Revisar y revocar permisos innecesarios con regularidad.

### 2. Clasificación y Almacenamiento de Datos

- Clasificar datos como públicos, internos, confidenciales y restringidos.
- Cifrar datos sensibles en reposo y durante la transmisión.
- Mantener copias de seguridad en lugares seguros y geográficamente separados.

### 3. Protección de Redes y Sistemas

- Utilizar cortafuegos y sistemas de detección de intrusos.
- Mantener los sistemas y aplicaciones actualizados.
- Segmentar redes para limitar la propagación de incidentes.

### 4. Respuesta e Investigación de Incidentes

- Disponer de un plan documentado de respuesta ante incidentes.
- Supervisar registros en tiempo real para detectar patrones anormales.
- Notificar cualquier violación a las autoridades competentes.

### 5. Concienciación y Capacitación del Personal

- Proporcionar formación periódica en ciberseguridad.
- Instruir sobre la detección de phishing y el manejo seguro de datos.
- Fomentar la notificación inmediata de actividades sospechosas.

### 6. Cumplimiento y Revisión

- Cumplir con GDPR y normativas locales de protección de datos.
- Realizar auditorías de seguridad y evaluaciones de riesgos anualmente.
- Actualizar estas directrices según evolucionen las amenazas.

**Implementar estas medidas permite reducir riesgos y mantener la confianza en la protección de la información.**

# Guide de Gestion de la Sécurité des Données Numériques

## 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

-

! ! ! !

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

## التحكم في الوصول 1.

- منح كل مستخدم أدنى مستوى من الصلاحيات الازمة فقط.
- تفعيل المصادقة متعددة العوامل لأنظمة الحساسة.
- مراجعة الأذونات بشكل دوري وإلغاء غير الضروري منها.

## تصنيف وتخزين البيانات 2.

- تصنيف البيانات إلى عامة، داخلية، سرية ومقيدة.
- تشفير البيانات الحساسة أثناء التخزين والنقل.
- حفظ النسخ الاحتياطية في موقع آمنة ومنفصلة جغرافياً.

## حماية الشبكات والأنظمة 3.

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

## الاستجابة للحوادث والمراقبة 4.

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

## توعية وتدريب الموظفين 5.

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

## الامتثال والمراجعة 6.

- 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.