السياسات العامة لأمن المعلومات

في الجهات الحكومية

سياسة خصوصية البيانات

م / محمد الجائفي

المحاور

- بنود سياسة خصوصية البيانات
- المقدمة
- الاهداف
- نطاق تطبيق السياسة
- حماية الخصوصية وتشفير البيانات
- منع الإفصاح والكشف او التسريب لبيانات وخصوصية الجهة الحكومية
- الأدوار والمسئوليات

بنود سياسة خصوصية البيانات

يجب على الموظفين عدم الإفصاح لأي شخص عن أي معلومات تتعلق بالأفراد أو الأقسام أو الطرق المستخدمة لمعرفة نقاط الضعف لنظام معين أو أي أنظمة خاصة قد تعرضت للإتلاف بسبب الجرائم أو التجاوزات الحاسوبية

لا يجوز الكشف عن المعلومات المتعلقة بنظم المعلومات التي يمكن أن تمس أمن تلك النظم للمستخدمين أو أي طرف أخر إلا على أساس مبدأ الحاجة للمعرفة وبإذن مسبق من إدارة نظم المعلومات

بنود سياسة خصوصية البيانات

يجب على الموظفين أن لا يفصحوا للأشخاص غير المصرح لهم عن طبيعة وموقع أنظمة المعلومات ولا عن أنظمة الرقابة المستخدمة أو وسائل النفاذ أو نوع وماهية التجهيزات والمكونات المستخدمة

يجب تشفير جميع المعلومات التي تصنف تصنيفاً حساساً (سري أو سري للغاية)

بنود سياسة خصوصية البيانات

يجب على الجهات الحكومية الالتزام بأمن أنظمة المعلومات كافة وعدم الاقتصار على تخزين ونقل ومعالجة وإتلاف المعلومات المصنفة

يجب مراعاة الخصوصية عند التعامل مع البيانات الشخصية للموظفين التابعين لتلك الجهة والبيانات الشخصية للمواطنين

المقدمة

تعد سياسة الخصوصية ضمن سياسة أمن المعلومات في الجهات الحكومية أمرًا أساسيًا وحيويًا في عصر التكنولوجيا الحديثة. تهدف سياسة الخصوصية إلى حماية وضمان خصوصية المعلومات والبيانات الخاصة بالجهة والتي تتعامل معها في أداء مهامها وواجباتها. تعد سياسة الخصوصية أداة مهمة لضمان تعامل الجهات الحكومية مع البيانات بالشكل الآمن والصحيح.

تشمل سياسة الخصوصية التعليمات والمعايير التوجيهية التي يجب اتباعها لأمان أنظمة المعلومات مثل تحديد الشروط والضوابط التي يجب اتباعها عند استخدام او معالجة البيانات او أنظمة المعلومات الخاصة بالجهة، إجراءات الأمان اللازمة لحماية البيانات من الوصول غير المصرح به أو الاستخدام غير القانوني. يتضمن ذلك تطبيق تقنيات التشفير وتنفيذ سياسات الوصول المحدودة وتأمين البنية التحتية للحفاظ على خصوصية الجهة

الأهداف

تهدف هذه السياسة الى:

- حماية وضمان خصوصية المعلومات والبيانات الخاصة بالجهة أو بالموظفين أو الأطراف الأخرى ذات العلاقة والتي تتعامل معها في أداء مهامها وواجباتها، والحفاظ على سرية وسلامة جميع المعلومات المتعلقة بنظم المعلومات التي يمكن أن تمس أمن تلك النظم وتشكل تهديد عليها.
- تحديد الإجراءات المناسبة لتشفير جميع المعلومات الخاصة بالجهة خاصتاً التي تصنف تصنيفاً حساساً (سري أو سري للغاية)
- تحديد القواعد والمبادئ التوجيهية لكيفية التعامل مع البيانات والأنظمة الخاصة بالجهة وكيفية استخدامها بالشكل الذي يضمن سلامتها وسريتها، مع مراعاة الخصوصية عند التعامل مع البيانات الشخصية للموظفين التابعين لتلك الجهة والبيانات الشخصية للمواطنين

النطاق

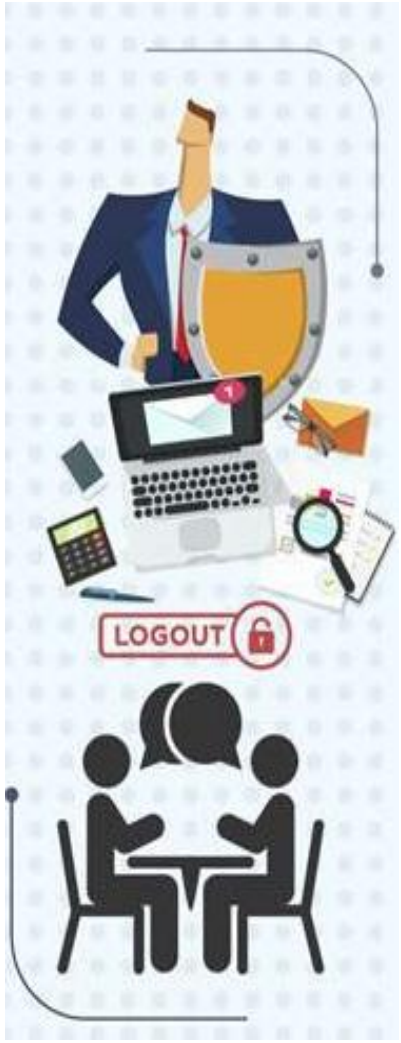
تطبق هذه السياسة على الجهة الحكومية وجميع الأصول المعلوماتية ذات العلاقة والموظفين والعاملين في الجهة بشكل دائم او مؤقت، والموظفين والعاملين في الجهة في حال اتفاقية تعاقد مع جهات أخرى، وأي طرف ذات علاقة.

وزارة الاتصالات وتقنية المعلومات

منع الإفصاح والكشف او التسريب لبيانات وخصوصية الجهة الحكومية

تحديد إجراءات لمنع استخدام أي من الطرق التي تمكن من الكشف او الإفصاح او تسريب البيانات الخاصة بالجهة أو الأشخاص والأطراف ذات العلاقة، على سبيل المثال لا الحصر الطرق التالية:

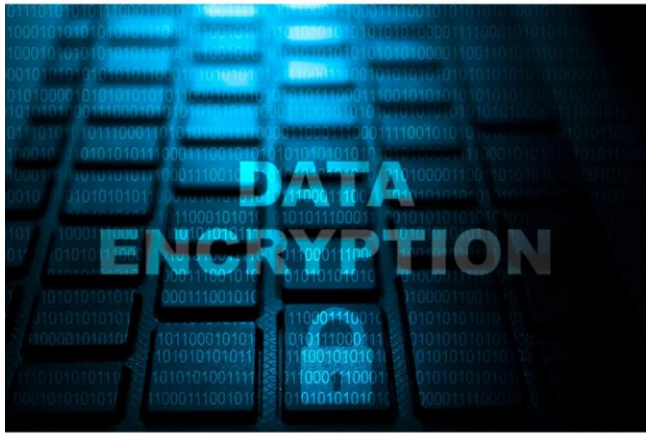
- ترك الأجهزة التي تحتوي على بيانات واعمال الجهة بدون تسجيل خروج او قفل للشاشة
- استخدام كاميرا الهواتف المحمولة لالتقاط صور للبيانات الهامة والحساسة الخاصة ببيانات الجهة
- الحديث بصوت مرتفع في الأمكان المفتوحة عما تحتويه بيانات ومعلومات الجهة الحساسة على سبيل المثال عن طبيعة وموقع أنظمة المعلومات او أنظمة الرقابة المستخدمة أووسائل النفاذ وغيرها



طرق لحماية البيانات من الإفصاح او الكشف او التسريب :

- وضح سياسة وإجراءات لحماية وتشفير البيانات خاصة الحساسة
- التأكد من التزام جميع المعنيين في الجهة الحكومية بتطبيقها وتنفيذ احكامها
- توعية موظفي الجهة الحكومية بالمخاطر الأمنية وتثقيفهم بالسياسات الأمنية وحثهم على اتباعها
- مر اقبة وتقييم مدى الالتزام بتطبيق السياسة

حماية الخصوصية وتشفير البيانات



- تضمن معايير واجراءات تشفير البيانات حماية بيانات الجهة الحكومية بطريقة أمنة عبر الأنظمة الأساسية والأجهزة المختلفة. يوفر ذلك أيضًا الخصوصية للبيانات والمستخدمين، حيث لا يمكن الوصول إلى رمز التشفير. ويستخدم تشفير البيانات مجموعة متنوعة من خوارزميات التشفير لحماية البيانات
- فوائد تشفير بيانات الجهة الحكومية:
  - ضمان سرية وخصوصية البيانات
  - يحمي البيانات من الوصول إليها من قبل أشخاص غير مصرح لهم
  - حماية البيانات من السرقة، ومن تغيير وتعديل البيانات
- تطبيق إجراءات وتقنيات التشفير للحفاظ على سرية وسلامة البيانات والمعلومات،
- يجب تشفير البيانات في الشبكات لحماية أنظمة المعلومات الحساسة من الوصول غير المصرح به خاصة البيانات الحساسة
- تشفير الأنظمة المعلوماتية وقواعد البيانات الخاصة بها،
- تشفير النسخ الاحتياطية وبيانات الاستعادة
- تشفير عمليات الاتصال ونقل البيانات بين التجهيزات والأنظمة العاملة في الجهة الحكومية

الأدوار والمسئوليات

من أهم مسئوليات الجهة

- اعداد وتطبيق سياسة الخصوصية وجميع التعليمات والاحكام والإجراءات الخاصة بها مع توفير الاحتياجات والمتطلبات لتنفيذها
- وضع التعليمات المناسبة والمعايير التوجيهية التي يجب اتباعها لأمان أنظمة المعلومات مثل تحديد الشروط والضوابط التي يجب اتباعها عند استخدام او معالجة البيانات او أنظمة المعلومات الخاصة بالجهة
- يجب على الجهات الحكومية الالتزام بأمن أنظمة المعلومات كافة وعدم الاقتصار على تخزين ونقل ومعالجة و إتلاف المعلومات المصنفة.
- يجب مراعاة الخصوصية عند التعامل مع البيانات الشخصية للموظفين التابعين لتلك الجهة والبيانات الشخصية للمواطنين
- يجب تشفير جميع المعلومات التي تصنف تصنيفاً حساساً (سري أو سري للغاية).
- عدم الكشف عن المعلومات المتعلقة بنظم المعلومات التي يمكن أن تمس أمن تلك النظم للمستخدمين أو أي طرف أخر إلا على أساس مبدأ الحاجة للمعرفة وبإذن مسبق من إدارة نظم المعلومات.

الأدوار والمسئوليات

من أهم مسئوليات المستخدمين

عدم الإفصاح لأي شخص عن أي معلومات تتعلق بالأفراد أو الأقسام أو الطرق المستخدمة لمعرفة نقاط الضعف لنظام معين أو أي أنظمة خاصة قد تعرضت للإتلاف بسبب الجرائم أو التجاوزات الحاسوبية

عدم الفصاح للأشخاص غير المصرح لهم عن طبيعة وموقع أنظمة المعلومات ولا عن أنظمة الرقابة المستخدمة أووسائل النفاذ أونوع وماهية التجهيزات والمكونات المستخدمة.

عدم الكشف عن المعلومات المتعلقة بنظم المعلومات التي يمكن أن تمس أمن تلك النظم للمستخدمين أو أي طرف أخر إلا على أساس مبدأ الحاجة للمعرفة وبإذن مسبق من إدارة نظم المعلومات.

انتهى