

المركز الوطني  
للأمن السيبراني  
National Cyber  
Security Center



# حماية البيانات والمعلومات



# المحاور

- التعريف بالبيانات والمعلومات.
- أنواع البيانات (شخصية ، عامة).
- تعريف حماية البيانات والمعلومات.
- أهمية حماية البيانات والمعلومات على مستوى المؤسسات والدوائر.
- العناصر الرئيسية لحماية البيانات والمعلومات.
- أفضل الممارسات العامة لحماية البيانات و المعلومات (افعل ولا تفعل).

# تعريف البيانات والمعلومات:

لا بد من الإشارة إلى أن مفهوم البيانات ومفهوم المعلومات هما مفهومان مترابطان للغاية، ويُشار لهما كوحدة واحدة في عملية الحماية الرقمية والأمن السيبراني، إلا أن لكل منهما مفهوم مختلف:

## البيانات:



وهي مجموعة المفردات والأرقام والحقائق الخام التي لم يتم معالجتها أو تنظيمها بحيث تصبح مفهومة وذات معنى.

## المعلومات:



وهي مجموعة بيانات تم معالجتها وتنظيمها ووضعها في سياق معين بحيث أصبحت ذات دلالة واضحة وذات معنى وقيمة.

## مثال:

تاريخ الميلاد (1/1/2000) هو بيانات لأنه بحد ذاته مجرد رقم لا يُشير إلى تاريخ ميلاد شخص معين، لكن إذا قلنا أن تاريخ ميلاد أحمد هارون (1/1/2000) فهذه أصبحت معلومة يُمكن فهمها وذات دلالة.

# أنواع البيانات:

## بيانات

**شخصية:** أي بيانات أو معلومات تتعلق بشخص ما وتدل بصورة مباشرة أو غير مباشرة على أصله أو عرقه أو تدل على آرائه أو انتماءاته السياسية أو معتقداته الدينية أو أي بيانات تتعلق بوضعه المالي أو بحالته الصحية أو الجسدية أو غيرها مما يُشير إليه أو يُعرف عنه بشكل صريح. (قانون حماية البيانات الشخصية الأردني للعام 2023م).



## بيانات

**عامة:** أي تلك المعلومات التي تكون متاحة للجميع ويمكن الوصول إليها من قبل أي كان، وتمتاز بأنه لا تحمل مستوى عالٍ من الخصوصية، كالسجلات الحكومية والمعلومات الموجودة عبر شبكة الإنترنت.



# تعريف حماية البيانات:

## مفهوم حماية البيانات والمعلومات ؟

مجموعة من المبادئ والممارسات التي تهدف إلى حماية بيانات الأفراد والمؤسسات وبطريقة تراعي خصوصيتهم وتضمن عدم التعرض لأيّة مخاطر قد تهددهم نتيجة عدم حماية بياناتهم بشكل كافٍ.

و تتضمن حماية البيانات عدم تلف البيانات وإمكانية الوصول إليها للأغراض المصرح بها فقط بما يتوافق مع المتطلبات القانونية المعمول بها، كما يجب أن تكون البيانات المحمية متاحة و متوفرة عند الحاجة إليها لاستخدامها للغرض المقصود منها.



# أهمية حماية البيانات والمعلومات على مستوى المؤسسات والدوائر:

## ○ حفظ الخصوصية وحقوق المواطنين:

تحتفظ المؤسسات والدوائر الحكومية بالكثير من البيانات المتعلقة بالمواطنين، ومن ضمنها بيانات شخصية حساسة؛ وحماية هذه البيانات تعني ضمان خصوصية المواطنين واحترام حقوقهم.

## ○ حماية سمعة المؤسسة:

يعد اختراق البيانات والإطلاع غير المصرح عليها من الأمور التي تسيء إلى أي مؤسسة أو جهة لذا فإنه يتوجب الحفاظ على سلامة تلك البيانات لحماية سمعة تلك المؤسسات والوزارات.

## ○ حفظ الأمن الوطني:

تسهم حماية المعلومات والبيانات في الحفاظ على الأمن القومي للمملكة الأردنية الهاشمية، كما أنها تُعزز أمن الفضاء الإلكتروني الأردني وتحد من تعرضه للهجمات السيبرانية التي تستهدف مؤسساته المختلفة سواء من قبل أفراد أو جماعات أو حتى دول.

## ○ حماية الموظفين من الملاحقة القانونية:

يخضع نظام حماية البيانات في المملكة الأردنية الهاشمية إلى مبدأ المحاسبة (Accounting) والذي يعني أن كل موظف مسؤول عن حماية حسابه الإلكتروني وما يتضمنه من بيانات ومعلومات، ويُمكن أن يتعرض للملاحقة القانونية إذا تم تسريب بيانات المؤسسة من خلال ذلك الحساب.

## ○ تحسين الخدمات الحكومية:

تعتمد المؤسسات والدوائر على البيانات والمعلومات لتقديم العديد من خدماتها؛ وحماية هذه البيانات يضمن استمرار تقديم الخدمات بصورة صحيحة.

# العناصر الأساسية لحماية البيانات والمعلومات:

## الإطلاع على خطط الاستجابة وإدارة الحوادث:

يتوجب أن يكون موظفو المؤسسة أو الدائرة على علم ودراية بكيفية اتباع تعليمات خطط الاستجابة للحوادث السيبرانية وكيفية التعامل مع أي حادثة اختراق قد تحصل.

## إدارة الوصول:

يتوجب أن تخضع المؤسسات لنظام تحديد صلاحيات وصول الموظفين والمستخدمين للأنظمة المختلفة تبعاً لمتطلبات العمل.

## تصنيف البيانات:

من المهم أن يتم تصنيف البيانات والمعلومات في أي مؤسسة تبعاً لمستوى سريتها (عادية، سرية، سرية جداً).

## تحديد البيانات الحساسة:

يتوجب أن يتم تحديد البيانات التي تعتبر حساسة وتستحق حماية خاصة، والتي قد تشتمل على البيانات المالية والمعلومات الخاصة بالدولة وغيرها.



# أفضل الممارسات العامة لحماية البيانات والمعلومات



افعل 

احرص على تحديد البيانات الشخصية التي يتطلب جمعها للقيام بأي مشروع بوضوح.



# أفضل الممارسات العامة لحماية البيانات والمعلومات



## افعل

تأكد من معرفتك التامة و تطبيقك للتعليمات التي يفرضها قسم الأمن السيبراني أو تكنولوجيا المعلومات في مؤسستك، و السياق السياسي ، والسياسات الداخلية الخاصة بالمؤسسة عند تحديد البيانات الشخصية التي يتطلب جمعها.

# أفضل الممارسات العامة لحماية البيانات والمعلومات



افعل 

استخدم كلمات مرور قوية ومركبة على الأنظمة التي تتضمن أي من أنواع البيانات التي تقدمها المؤسسة.

# أفضل الممارسات العامة لحماية البيانات والمعلومات



## افعل

حدد الغرض من جمع البيانات بشكل واضح و مباشر ، مع كيفية استخدامها ، و صلاحيات الاطلاع عليها ، والجهات التي يمكن الاتصال بها للاستفسار عن البيانات التي يتم تجميعها.

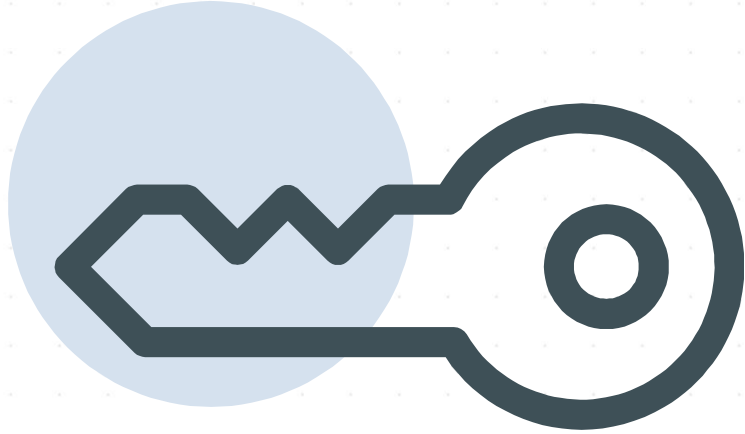
# أفضل الممارسات العامة لحماية البيانات والمعلومات



افعل 

حدد شخصاً مسؤولاً عن استخدام البيانات الشخصية و  
تخزينها و تصحيحها.

# أفضل الممارسات العامة لحماية البيانات والمعلومات



101011

افعل 

قم بتشفير أو وضع كلمات مرور لحماية الملفات و الأجهزة التي تتضمن بيانات شخصية أو معلومات حساسة.

# أفضل الممارسات العامة لحماية البيانات والمعلومات



افعل 

اختر طريقة آمنة للتخلص من البيانات فور أن تنتفي الحاجة إليها.

# أفضل الممارسات العامة لحماية البيانات والمعلومات



افعل 

تأكد من وضع سياسات صارمة و صلاحيات محدودة للموظفين للوصول إلى البيانات بالحد الذي يحتاجون إليه فقط للقيام بأعمالهم.



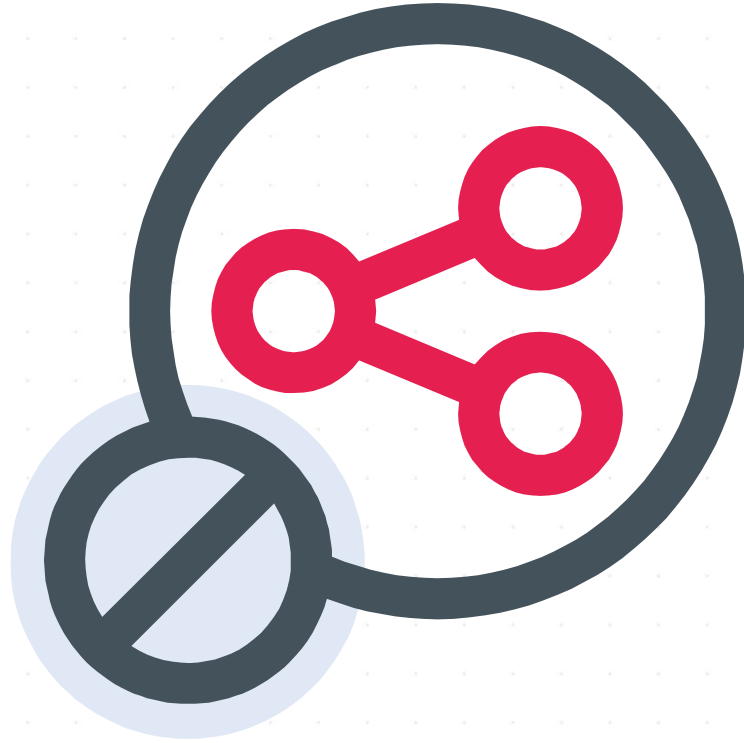
# أفضل الممارسات العامة لحماية البيانات والمعلومات



## افعل

احرص على إعداد اتفاق مكتوب قبل مشاركة أي بيانات شخصية مع أي طرف آخر خارج المؤسسة بعدم مشاركة البيانات وحمايتها والالتزام بالسياسات المطبقة في مؤسستك.

# أفضل الممارسات العامة لحماية البيانات والمعلومات



لا تفعل ..

لا تقم بمشاركة البيانات مع أي جهات حكومية أو أطراف خارجية ، ولا تسمح لهم بالوصول أو الاطلاع عليها دون إضفاء طابع رسمي على شروط القيام بذلك.

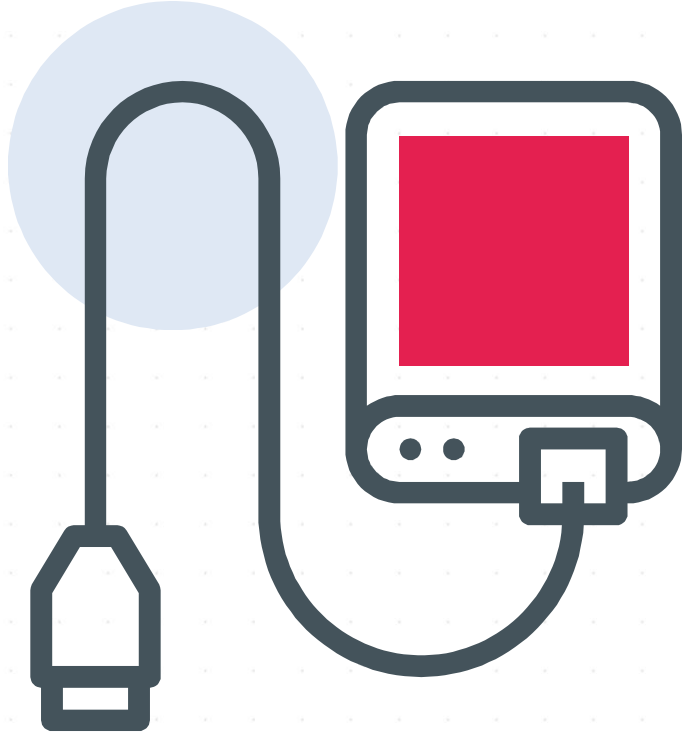
# أفضل الممارسات العامة لحماية البيانات والمعلومات



لا تفعل .. 

لا تقم بترك ملفات ورقية تتضمن بيانات في أماكن مفتوحة واحتفظ بها فقط في الأماكن المخصصة لذلك.

# أفضل الممارسات العامة لحماية البيانات والمعلومات

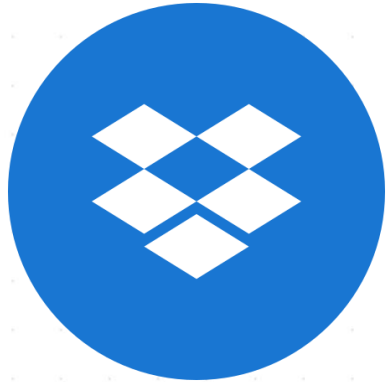


لا تفعل .. 

لا تستخدم وحدات تخزين خارجية لحفظ البيانات ما لم يكن المحتوى محمياً بكلمات مرور أو مشفراً.

# أفضل الممارسات العامة لحماية البيانات والمعلومات

لا تفعل .. 



لا تستخدم منصات تخزين و مشاركة الملفات مثل Google Drive أو Dropbox أو غير ذلك من المنصات الإلكترونية وجعلها متاحة للوصول العام ، و قم باستخدام هذه الملفات بشكل متزامن مع الأطراف المصرح لهم فقط.

نتمنى لكم السلامة في  
العالم  
الرقمي.