

الهيئة الوطنية لأمن وسلامة المعلومات
National Information Security & Safety Authority

كُن الموظف الواعي

لمؤسسات أكثر أماناً

يلعب الموظف دوراً محورياً في حماية أصول المعلومات. هذه الإرشادات توضح بشكلٍ موجز أفضل الممارسات لضمان أمن وسلامة المعلومات وفقاً للسياسات الوطنية لأمن وسلامة المعلومات والمعايير الدولية المتعلقة بالسلوكيات الآمنة للمستخدم.

+218 21 361 4115
+218 21 361 4127
+218 21 361 4177
info@nissa.gov.ly
www.nissa.gov.ly
www.cert.gov.ly

الوعي مسؤوليتك... والأمن مسؤوليتنا جميعًا

كلمات المرور و حماية الخصوصية

كلمة المرور .. إثبات الهوية للموافقة على الوصول لحماية المستخدم وبياناته، و لحفظ الخصوصية له و لمؤسسته .

- استخدم كلمات مرور قوية ويفضل أن تكون "**جملة مرور**" لا يفهمها إلا المستخدم **أنت**.
- من الملزم استخدام تقنية المصادقة متعددة العوامل (Multi-Factor Authentication).

- برامج **إدارة كلمات المرور** تُساعدك على إنشاء وتخزين كلمات مرور قوية وفريدة بأمان، باستخدام كلمة مرور رئيسية **واحدة** فقط.
- لا تشارك **كلمات المرور** الخاصة بك، واقفل جهازك عند مغادرة مكتبك.
- قلل مشاركة **بياناتك الشخصية** والبيانات الحساسة لزملائك، واحترم خصوصية بيانات العملاء والمستفيدين وكل من يتعامل مع مؤسستك.



الاستخدام المقبول والتعامل مع المعلومات

كل موظف مسؤول عن تطبيق معايير الاستخدام الآمن للأجهزة الالكترونية في إطار الوظيفة.

- لا تثبت **برامج** غير آمنة أو من مصادر مجهولة.
- تجنب فتح الروابط أو المرفقات المشبوهة، وتحقق من صحة أي رابط أو بريد قبل إدخال بيانات فيه.
- استخدم **البريد الإلكتروني** الرسمي فقط للأعمال المتعلقة بمؤسستك.
- لا تستخدم **الشبكات** العامة المفتوحة للعمل.

- تجنب **مشاركة بيانات العمل** عبر وسائل التواصل الاجتماعي.
- التزم بأخلاقيات الاستخدام المقبول في مؤسستك.
- عادةً تُصنف المعلومات والبيانات داخل المؤسسات إلى ثلاث تصنيفات أساسية (**مقيدة - داخلية - غير مقيدة**)، هذا التصنيف يمكّن الموظف من تحديد طبيعة تعامله مع تلكم المعلومات والبيانات. تعرف على سياسة تصنيف المعلومات في مؤسستك قبل التعامل معها.
- لا تحتفظ ببيانات أو **معلومات حساسة** تخص مؤسستك على أجهزة شخصية.
- لا تثق بالرسائل التي تطلب بيانات عاجلة أو غير معتادة.
- التزم **بسياسات النسخ الاحتياطي** وحفظ البيانات.

الاستجابة للحوادث و سلوكيات الموظف

كل موظف مسؤول يجب أن يكون عيناً يقظة تساهم في حماية المؤسسة، والتعاون مع فريق الاستجابة يسرّع من احتواء الحادثة.

- أبلغ فوراً عن أي رسالة مشبوهة أو محاولة تصيد.
- لا تتجاهل أي نشاط غريب تلاحظه في جهازك.
- التزم بالإبلاغ عند وقوع حادثة أمنية .
- ثقافة **الأمن السيبراني** تبدأ من قناعاتك الصحيحة، وتتجلى في سلوكياتك اليومية لحماية معلومات مؤسستك.
- التزم **بالسياسات والمعايير** و الإجراءات الصادرة عن مؤسستك.
- احرص على المشاركة في الدورات و**الأنشطة التوعوية** داخل و خارج المؤسسة.
- الأمن السيبراني مسؤولية يشترك فيها جميع الموظفين، وليس قسماً بعينه.
- الهجمات السيبرانية قد تستهدف أي موظف.