

حساسية كلمة المرور

أشياء يجب العمل بها:

- دائماً استخدم كلمات مرور معقدة حسب السياسات.
- احفظ كلمات المرور سرية وآمنة.
- قم بتغيير الكلمات المرورية الافتراضية حالاً.
- دائماً تأكد من قفل الجهاز الشخصي عند ترك المكتب.
- احرص على تذكر كلمة المرور بدلاً من تسجيلها في مكان ما.

أشياء لا تقم بعملها:

- لا تقم بكتابة كلمة المرور الخاصة بك بأي مكان.
- لا تقم بمشاركة كلمة المرور الخاصة بك مع أي شخص.
- لا تقم بإرسال كلمات المرور عبر البريد الإلكتروني.
- لا تقم باستخدام كلمات مرور قديمة سبق أن استخدمتها.
- لا تقم باستخدام نفس كلمة المرور لأنظمة متعددة.

سياسة كلمة المرور

جميع المستخدمين يجب أن يتبعوا سياسات كلمة المرور، والأخذ بعين الاعتبار لحساسية إنشاء كلمة مرور بإتباع الخطوات التالية:

- 1- كلمة المرور يجب أن تحتوي على 10 خانات على أقل تقدير.
- 2- كلمة المرور صالحة لمدة 12 شهراً.
- 3- لا يسمح باستخدام آخر 5 كلمات مرور سبق استخدامها.
- 4- لا يمكن احتواء كلمة المرور على اسم المستخدم الخاص بك.
- 5- لا يمكن احتواء كلمة المرور على اسمك أو أجزاء منه.
- 6- يجب أن تكون كلمة المرور مزيجاً من ثلاثة على الأقل من أربعة خيارات مذكورة أدناه:



حرف واحد (كبير) من الحروف الأبجدية الإنجليزية

حرف واحد (صغير) من الحروف الأبجدية الإنجليزية

حرف واحد حرف خاص

يحتوي على رقم واحد

A على الأقل

a على الأقل

&, @ على الأقل

0-9 على الأقل