كلمات مرور المستخدم

التعريف والاستخدام و
إجراءات تتعلق بحمايتها
حول المبادئ
أنظمة

IKVKK_Y7الإصدار 1.00

1.المقدمة والأهداف والتعريفات

1.1.يحدد هذا النظام الإجراءات المعمول بها ويقدم توصيات للمستخدمين فيما يتعلق باستخدام و/أو حماية كلمات مرور المستخدم المحددة/التي سيتم تحديدها فيما يتعلق بجميع أنواع أنظمة المعلومات والاتصالات المستخدمة داخل الشركة.

2.مبادئ تحديد كلمة مرور قوية

2.1.تتوقع الشركة أن يضمن المستخدمون حماية فعّالة لكلمات المرور من خلال تحديد كلمات مرور قوية، مع الالتزام بالمعايير التالية: 2.1.1.يجب ألا يقل طول كلمة المرور عن 8أحرف. 2.1.2.يجب أن تحتوي كلمة المرور على ثلاثة عناصر على الأقل من العناصر التالية:

(I)الأرقام (0-9)

(II)الأحرف الكبيرة (AZ)

(III)الأحرف الصغيرة (قليلة)

(رابعاً) الأحرف الخاصة (!، @، #، %، ؟)إلخ.)

2.1.3.يجب ألا تحتوي كلمة المرور على أي مما يلي:

(I)كلمة مأخوذة من قاموس (أي لغة)، أو من لغة عامية، أو اختصار عام.

(II)اسم شخص أو مكان.

(III)تاريخ يسهل تخمينه، مثل تاريخ ميلاد زوج/شريك المستخدم.

(IV)المعلومات المعروفة بأنها مرتبطة بالمستخدم، مثل رقم لوحة ترخيص مركبة المستخدم، ورقم الهوية في الجمهورية التركية، ورقم بطاقة الوصول.

(V)يجب أن يكون اسم المستخدم للحساب هو نفسه أو مشابهًا لـ (بما في ذلك أسماء المستخدمين المعكوسة أو المكتوبة بشكل خاطئ)

(VI)أي كلمات مرور أو معلومات أو ما شابه ذلك واردة كأمثلة على الموقع الإلكتروني للشركة أو في هذه اللائحة.

2.1.4.لا يمكن أن تكون كلمة المرور الجديدة هي نفسها أي من كلمات المرور الست الأخيرة المستخدمة.

3.المبادئ التي يجب اتباعها لحماية كلمة المرور

3.1.يجب على المستخدمين اختيار كلمة مرور يسهل تذكرها، وتجنب كتابة كلمات المرور، وعدم ترك كلمات المرور تحت أي ظرف من الظروف في مكان يمكن للآخرين الوصول إليه بسهولة.

3.2.يجب على المستخدمين عدم إفشاء كلمات مرورهم للآخرين. لن تطلب الشركة كلمة مرور أي مستخدم على الإطلاق. الشخص الوحيد الذي يحتاج إلى معرفة كلمة مرورك هو المستخدم نفسه.
إذا تلقى المستخدم أي بريد إلكتروني أو رسالة أو ما شابه ذلك تحتوي على مثل هذا الطلب، فيجب اعتبار هذا الاتصال محاولة احتيال إلكتروني، ويجب إبلاغ مدير تكنولوجيا المعلومات على الفور دون الرد.

3.3.إذا اكتشف المستخدم أن كلمة المرور الخاصة به قد تم الكشف عنها عن طريق الخطأ أو بأي طريقة أخرى، فعليه تغيير كلمة المرور الخاصة به على الفور وإبلاغ مدير تكنولوجيا المعلومات على الفور.

3.4.يجب على المستخدمين التأكد من عدم تمكن الآخرين من رؤية شاشاتهم أثناء كتابة كلمة مرور تسجيل الدخول، كما يجب عليهم عدم وضع شاشاتهم بطريقة تسمح لأي شخص، بما في ذلك الزملاء، برؤيتهم أثناء إدخال كلمة المرور. وينبغي أيضًا وضع الشاشات داخل المكتب بطريقة تمنع رؤيتها من خارج المبنى.

3.5.يجب على المستخدمين عدم إدخال كلمات مرورهم على أي موقع إلكتروني إلا إذا كانوا متأكدين من أنه الموقع الرسمي لأنظمة المعلومات والاتصالات الخاصة بالشركة. وأفضل طريقة للتأكد من ذلك هي إضافة المواقع إلى المفضلة.

يتضمن ذلك تقديم عناوين URL الخاصة بك أو الوصول إليها باستخدام عناوين URL التي أدخلتها. تجنب استخدام الروابط، وخاصة تلك الموجودة في رسائل البريد الإلكتروني التي تدّعي أنها شرعية.

4.تغيير كلمات المرور

4.1.من الضروري أن يقوم المستخدمون بتغيير كلمات مرورهم بشكل دوري. ويجوز لنائب المدير العام تحديد فترة تغيير كلمة المرور بما يتراوح بين 30 يومًا وسنة واحدة، وذلك بناءً على أدوار ومسؤوليات أصحاب الحسابات المصرح لهم من قبل الشركة.

4.2.يمكنك تغيير كلمة المرور الخاصة بك عن طريق تسجيل الدخول إلى أجهزة الكمبيوتر المسجلة في قائمة جرد الشركة واستخدام الرابط التالي:
http://www.kardelenboya.com.tr/

4.3.لا يُسمح بإعادة استخدام كلمات المرور القديمة. هذه ممارسة جيدة، ويمكنك تطبيقها على الأنظمة خارج الشركة أيضًا.

4.4.سيُطلب من المستخدمين الذين تبين أن كلمات مرورهم لا تتوافق مع أحكام هذه اللائحة تغيير كلمات مرورهم على الفور.

4.5.سيتم التواصل مع المستخدمين الذين يحتاجون إلى تغيير كلمات مرورهم من قبل موظف في الشركة عبر البريد الإلكتروني أو الهاتف أو شخصيًا. وسيتمكن المستخدمون بعد ذلك من تغيير كلمات مرورهم لدى الشركة.
لا ينبغي له أن يفصح عن هذا لأي شخص، بما في ذلك موظفيه.

5.كلمات المرور المستخدمة للأنظمة الخارجية

5.1.يوصى بتطبيق أفضل ممارسات الاستخدام الموضحة في هذه اللائحة عند استخدام أنظمة أخرى خارج الشركة.

5.2.تجنب استخدام اسم المستخدم وكلمة المرور الحاليين داخل الشركة لإنشاء حسابات على مواقع الويب أو موارد الإنترنت الأخرى.