معايير وتعليمات كلمات المرور

مفهوم كلمة المرور (Password):

طريقة تحقق تستخدم للتحكم بالدخول الى الموارد المختلفة، وهي تتكون من سلسلة سرية من الرموز معروفة في النظام يدخلها المستخدم من اجل اثبات هويته للنظام .

اولا: الهدف

حماية الموارد المعلوماتية من الدخول غير المشروع إليها عن طريق وضع معايير واضحة لانشاء كلمات مرور فعالة، وحمايتها وتغييرها بشكل دوري.

ثانيا: المجال

تغطي هذه التعليمات جميع المستخدمين الذين لهم سجلات دخول الكترونية داخل الدائرة، وآلية تصميم ومراقبة واستخدام كلمات المرور التي تستعمل لإثبات هوية المستخدم للنظام أو الملف أو الخدمة التي يريد الدخول اليها، مثل أجهزة الحاسوب الشخصية والمحمولة والخادمة، وسجلات البريد الالكتروني، وسجلات الدخول الالكترونية الى الأجهزة والشبكات، والبرامج والنظم الإدارية والمالية.

ثالثا: المعايير والتعليمات :

1- تعامل كلمات المرور على أنها معلومات مصنفة، وتستمد حساسيتها من حساسية المعلومات للنظام المرتبط بها، وذلك لأغراض شمولها بسياسات امن وحماية المعلومات.
2- تعطى للموظف كلمة مرور لاستعمال نظام محوسب خاص بالمديرية او القسم الذي يعمل فيه ولديه موافقة خطية من مديره على استعمال النظام المحوسب.
3- يعطى للموظف كلمة مرور للبريد الالكتروني الرسمي الخاص به.
4- يعطى للموظف كلمة مرور لجهاز الحاسوب الشخصي/المحمول الذي يعمل عليه.
5- تعطى كلمة مرور للخوادم للموظف الذي لديه تصريح بالعمل على الخوادم.
6- تعطى كلمة مرور للشبكات للموظف الذي لديه تصريح بالعمل على الشبكات.
7- على الموظف حماية كلمة المرور التي يزود بها من الضياع وعدم الافصاح عنها بشكل غير مرخص ولأي سبب كان وبأي طريقة كانت مثل كتابتها وتعليقها في مكان ظاهر، أو اعطائها للغير مشافهة أو بشكل مكتوب بطريقة إلكترونية أو غير إلكترونية، وتحت طائلة المساءلة القانونية وفقا لأحكام الخدمة المدنية.
8- عدم كتابة كلمات المرور أمام أي شخص يشاهد عملية الادخال على لوحة المفاتيح.

9- عدم استعمال كلمات المرور الخاصة بالدائرة في مواقع الانترنت التي لا علاقة لها بالعمل الرسمي إلا عندما يكون الاتصال بهذه المواقع آمنا بقدر الاستطاعة .

10- تغيير كلمة المرور عند الافصاح عنها بشكل غير مرخص سواء بشكل متعمد أو غير متعمد.

11- عند اختيارأو تغييركلمة مرور (Password) يجب الأخذ بعين الاعتبارالأمور التالية :

أ- ألا تكون قد استخدمت مسبقا من فترة قريبة.

ب- ألا تكون سهلة التخمين، مثل اسم الشخص، أو تاريخ ولادته، أو رقم هاتفه، أو اسم سجل الدخول الالكتروني للمستخدم.

ت- ألا تكون من الكلمات المتداولة في القواميس أو الملفات المعروفة.

ث- ألا تكون مبنية بحيث تشكل في مجملها جملة واحدة كاملة من حروف وأرقام متتابعة ومتسلسلة بشكل منطقي ومعروف للعامة.

ج- أن تكون مركبة من الحروف والأرقام والرموزالخاصة، وبدون تكرار.

ح- أن تكون طويلة بشكل كاف.

خ- ألا تحتوي اختصارات معروفة مثل gov , moJ , sep

د- أن يتم تغييرها بشكل دوري .

ذ- عدم استخدامها في اكثر من نظام .

12- يعبأ نموذج تعهد والتزام بالمحافظة على كلمة المرور التي تعطى للموظف من قبل الموظف نفسه.

13- يتوجب على مدير النظام حماية الموارد المعلوماتية من الدخول غير المشروع أو غير المخول عن طريق إعداد النظام لاستخدام وقبول كلمات المرور التي تحقق الشروط التي تم ذكرها أعلاه في هذه المعايير، ورفض كلمات المرور الضعيفة.

14- المستخدم مسؤول عن أي عمليات أو مراسلات تحدث عن طريق سجل الدخول الالكتروني الخاص به سواء عن طريقه أو عن طريق أي شخص استخدم كلمة المرور الخاصة بهذا المستخدم، وتحت طائلة المساءلة القانونية وفقا لأحكام الخدمة المدنية.

15- عدم انتحال هويات الموظفين الآخرين عن طريق استعمال كلمات مرورهم من اجل المنفعة الشخصية أو التسبب بايذاء جهة ما أو منفعة جهة أخرى بشكل غير قانوني، وتحت طائلة المساءلة القانونية وفقا لأحكام الخدمة المدنية.

16- على المستخدم ومدير النظام (الموظف) تسليم كل ما بحوزته من كلمات مرور للجهة المسؤولة عن ذلك في الوزارة عند انتهاء وظيفته أو سفره أو مغادرته في اجازة طويلة (اجازة بدون راتب او حسب ما تستدعيه طبيعة العمل بالتنسيق مع المسؤول المباشر).