P06 ŞİFRE POLİTİKASI

1.1 Amaç

Bu politikanın amacı güçlü bir şifre oluşturulması, oluşturulan şifrenin korunması ve bu şifrenin değiştirilme sıklığı hakkında standart oluşturmaktır.

1.2 Kapsam

Bu politika kullanıcı hesabı olan (Bilgisayar ağına erişen ve şifre gerektiren kişiler) bütün kullanıcıları kapsamaktadır.

1.3 Politika

Şifre bilgisayar güvenliği için önemli bir özelliktir. Kullanıcı hesapları için ilk güvenlik katmanıdır. Zayıf seçilmiş bir şifre ağ güvenliğini tümüyle riske atabilir. Kurum çalışanları ve uzak noktalardan erişenler aşağıda belirtilen kurallar dahilinde şifre belirlemekle sorumludurlar.

1.3.1 Genel

a) Bütün sistem seviyeli şifreler (örnek, root, administrator) en 6 ayda bir değiştirilmelidir.
b) Bütün kullanıcı seviyeli şifreler Yönetim dahil (örnek, e-posta, web vs.) en az 6 ayda bir değiştirilmelidir.
c) Şifreler e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.
d) Kullanıcı, şifresini başkası ile paylaşmamalı, kâğıtlara ya da elektronik ortamlara yazmamalıdır.
e) Kurum çalışanı olmayan harici kişiler için açılan kullanıcı hesaplarının şifreleri de kolayca kırılamayacak güçlü bir şifreye sahip olmalıdır.
f) Şifrelerde Türkçe karakter kullanılmaması tavsiye edilir.

1.3.2 Ana Noktalar

1.3.2.1 Genel Şifre Oluşturma Kuralları

Şifreler değişik amaçlar için kullanılmaktadır. Bunlardan bazıları: kullanıcı şifreleri, web erişim şifreleri, e-posta erişim şifreleri, ekran koruma şifreleri,

yönlendirici erişim şifreleri vs. Bütün kullanıcılar güçlü bir şifre seçimi hakkında özen göstermelidir.

Zayıf şifreler aşağıdaki karakteristiklere sahiptir.

- Şifreler az karaktere sahiptir.
- Şifreler sözlükte bulunan bir kelimeye sahiptir.
- Şifreler aşağıdaki gibi ortak değere sahiptir.
    - Ailesinin, arkadaşının sahip olduğu bir hayvanın veya bir sanatçının ismine sahiptir.
    - Bilgisayar terminolojisi ve isimleri, komutlar, donanım veya yazılım gibi
    - "universite" , "giresun" gibi
    - AaaBb, qwerty ,qazwsx, 123321 gibi sıralı harf veya rakamlar

Güçlü Şifreler aşağıdaki karakteristiklere sahiptir.

- Küçük ve büyük karakterlere sahiptir. (A-Z , a-z)
- Hem dijit hem de noktalama karakterleri ve ayrıca harflere sahiptir.(0-9,!,@,&=(,}?,\)
- Alfanümerik karaktere sahiptir.

- Herhangi bir dildeki argo lehçe veya teknik bir kelime olmamalıdır.

1.3.2.2 Şifre Koruma Standartları

Kurum bünyesinde kullanılan şifreleri kurum dışında herhangi bir şekilde kullanılmamalıdır ve kimse ile paylaşılmamalıdır. İlgili şifreler Kuruma ait gizli bilgiler olarak düşünülmelidir. Değişik sistemler için farklı şifre kullanılmalıdır.

Aşağıdakiler şifreler ile ilgili yapılmayacaklar listesidir.

a) Herhangi bir kişiye telefonda şifre vermek,
b) E-posta mesajlarında şifre belirtmek,
c) Üst yöneticinize şifreleri söylemek,
d) Başkaları önünde şifreler hakkında konuşmak,
e) Aile isimlerini şifre olarak kullanmak,
f) Şifreleri işten uzakta olduğunuzda iş arkadaşlarınıza bildirmek,
g) Uygulamalardaki "şifre hatırlatma" özelliklerini seçmek,

1.3.2.3 Uygulama Geliştirme Standartları

Uygulama geliştiricileri programlarındaki aşağıdaki güvenlik özelliklerinin sağlandığından emin olmalıdırlar.

- Bireylerin (grupların değil) kimlik doğrulaması işlemini destekleyebilmelidir.
- Şifreleri text olarak veya kolay anlaşılabilir formda saklamamalıdır.

1.3.2.4 Uzaktan Erişen Kullanıcılar İçin Şifre Kullanımı

Kurumun bilgisayar ağına uzaktan erişim tek yönlü şifreleme algoritması veya güçlü bir passphrase ile yapılmalıdır.