1. Amaç – Kapsam

Personelin, bilgi sistemlerinin kullanımında güçlü şifreleme mekanizmalarını kullanması, oluşturulan şifrelerin korunması ve bu şifrelerin değiştirilme sıklığı hakkında standart oluşturmaktır.
Kurum ve hizmet verdiğimiz birimler kapsam dâhilindedir.

2. Sorumlular

Bu prosedürün oluşturulmasından yazılım geliştirme ve otomasyon birimi ile sistem birimi sorumlu olup kullanıcı hesabı olan (şifre gerektiren kişiler uygulamalara erişen) bütün çalışanlar da uygulamadan sorumludur.

3. Uygulama

Şifreleme, bilgi güvenliğinin sağlanması açısından kritik bir öneme sahip olup ilk güvenlik katmanını teşkil etmektedir. Zayıf seçilmiş bir şifre ağ güvenliğini tümüyle riske atabilir. Kurum personeli ve uzak noktalardan erişenler aşağıda belirtilen kurallar dahilinde şifreleme yapmakla sorumludurlar.

Genel Kurallar

a) Bütün sistem seviyeli şifreler (örnek, root, administrator, enable, vs) en az üç ayda bir değiştirilmeli veya private key kullanılarak erişim sağlanmalıdır.
b) Farklı yetkiye sahip kullanıcı şifreleri (örnek, e-posta, web, masaüstü bilgisayar vs.) en az altı ayda bir değiştirilmelidir.
c) Sistem yöneticisi her sistem için farklı şifreler kullanmalı veya private key kullanılarak erişim sağlamalıdır.
d) Şifreler e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.
e) Kullanıcı, şifresini başkası ile paylaşmaması, kağıtlara yada elektronik ortamlara yazmaması konusunda eğitilmelidir.
f) Kurum çalışanı olmayan harici kişiler için açılan kullanıcı hesaplarının şifreleri de kolayca kırılamayacak güçlü bir şifreye sahip olmalıdır.

Şifre Oluşturma Kuralları

Şifreler kullanıcı hesaplarında, domain erişimlerinde, web uygulamalarında, e-posta hesaplarında, ekran koruma işlemlerinde, network erişim uygulamalarında vb. kullanılmakta aşağıda belirtilen kurallar çerçevesinde oluşturulmaları sistem açısından büyüm önem arzetmektedir.

Zayıf Şifreler

Zayıf şifreler aşağıdaki karakteristiklere sahip olup kullanıcılar bu tip şifrelemeden kaçınmalıdır.

a) Şifreler sekizden daha az karaktere sahiptirler.
b) Şifreler sözlükte bulunan bir kelimeye sahip değildir.
c) Şifreler aşağıdaki gibi ortak değere sahiptir.
   - Harf ve rakamlardan karmaşık oluşur.
   - Bilgisayar terminolojisi ve isimleri; komutlar, siteler, şirketler, donanım, yazılım vb.
   - ”Verita”, ”trabzon”, ”ankara” gibi özel isimler.
   - Doğum tarihi, adres ve telefon numaraları gibi kişisel bilgiler.
   - Aaabbb, qwerty, zyxwuts, 123321 vs. Gibi sıralı harf veya rakamlar.
   - Yukardaki herhangi bir kelimenin geri yazılış şekli.
   - Yukarıdaki herhangi bir kelimenin rakamla takip edilmesi (örnek, gizli1, gizli2).

Güçlü Şifreler

Güçlü şifreler aşağıdaki karakteristiklere sahip olup kullanıcılar bu tip şifreleme kurallarını uygulamalıdır:

a) Küçük ve büyük karakterlere sahiptir (örnek, a-z, A-Z)
b) Hem dijit hemde noktalama karakterleri ve ayrıca harflere sahiptir. (0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
c) En az altı adet alfa nümerik karaktere sahiptir.
d) Herhangi bir dildeki argo, lehçe veya teknik bir kelime olmamalıdır.
e) Aile isimleri gibi kişisel bilgilere ait olmamalıdır.
f) Şifreler herhangi bir yere yazılmamalıdır veya elektronik ortamda tutulmamalıdır. Kolayca hatırlanabilen şifreler oluşturulmalıdır. Örnek olarak; ”Birinci hedefimiz müşteri memnuniyetinin sağlanmasıdır” ”1KhMmS!” veya türevleri şeklinde olabilir.

Not: Yukarıdaki herhangi bir örneği şifre olarak kullanmayınız.

Şifre Koruma Standartları

Bütün kullanıcılar aşağıdaki kurallara titizlikle uymalıdır.

a) Kurum bünyesinde kullanılan şifreler kurum dışında herhangi bir şekilde kullanmamalıdır. (örnek, internet erişim şifreleri, bankacılık işlemlerinde veya diğer yerlerde).
b) Değişik sistemler için farklı şifreleme kullanılmalıdır. Örnek, Unix sistemler için farklı şifre, Windows sistemler için farklı şifre.
c) Kurum bünyesinde kullanılan şifreleri herhangi bir kimseyle paylaşmayınız. Bütün şifreler kuruma ait gizli bilgiler olarak düşünülmelidir.
d) Herhangi bir kişiye telefonda şifre verilmemelidir.
e) e-posta mesajlarında şifre belirtmemelidir.
f) Üst yönetici dahil hiç kimseye şifre söylenmemelidir.
g) Başkaları önünde şifreler hakkında konuşulmamalıdır.
h) Aile isimlerini şifre olarak kullanılmamalıdır.
i) Herhangi form üzerinde şifre belirtilmemelidir.
j) Şifreler aile bireyleri ile paylaşılmamalıdır.
k) Şifreler, işten uzakta olduğunuz zamanlarda iş arkadaşlarınıza söylenmemelidir.
l) Herhangi bir kimse şifre isteğinde bulunursa bu dokümanı referans göstermesini ve ilgili amirini aramasını söyleyiniz.
m) Uygulamalardaki “şifre hatırlama” özelliklerini seçmeyiniz. (örnek, Outlook, Internet Explorer vs.)
n) Şifreleri herhangi bir yere yazmayınız ve herhangi bir ortamda elektronik olarak saklamayınız.
o) Şifreler an az altı ayda bir değiştirilmelidir (sistemlerin şifreleri ise en az üç ayda bir değiştirilmelidir). Tavsiye edilen aralık ise 3 ayda birdir.
p) Şifre kırma ve tahmin etme operasyonları belli aralıklar ile yapılabilir. Güvenlik taraması sonucunda şifreler tahmin edilirse veya kırılırsa kullanıcıya şifresini değiştirmesi talep edilecektir.

4. BGYS Kayıtlar

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN
BİLGİ İŞLEM DAİRE BAŞKANLIĞI	KURUMSAL KALİTE GELİŞTİRME VE AKREDİTASYON KOORDİNATÖRLÜĞÜ	KURUMSAL YETKİLİ