

KVKK_Y7

**KULLANICI ŐFRELERİNİN
BELİRLENMESİ, KULLANIMI
VE KORUNMASINA İLİŐKİN
USUL VE ESASLAR HAKKINDA
YÖNETMELİK**



ARES
ECZA DEPOSU

1. GİRİŞ, AMAÇ VE TANIMLAR

1.1.İşbu Yönetmelik, Şirket bünyesinde kullanılan her türlü bilişim ve iletişim sistemleri ile ilgili olarak tanımlanacak/tanımlanan kullanıcı şifrelerinin kullanımı ve/veya korunması hususunda geçerli prosedürleri belirler ve kullanıcılara tavsiyeler sunar.

2. GÜÇLÜ BİR ŞİFRE TANIMLANMASI İÇİN GEÇERLİ PRENSİPLER

2.1. Şirket, kullanıcılarının güçlü bir parola-şifre tanımlayarak etkin bir şifre koruması sağlanması açısından aşağıda açıklanan kriterler göre hareket edilmesini ön görmektedir:

2.1.1. Şifre uzunluk bakımından en az 8 karakter içermelidir.

2.1.2. Şifrede aşağıda sıralanan unsurlardan en az üç tanesi bulunmalıdır:

(I) Numerik karakterler (0-9)

(II) Büyük harfler (A-Z)

(III) Küçük harfler (a-z)

(IV) Özel karakterler(?, !, @, #, %, vb.)

2.1.3. Şifre aşağıdakilerden herhangi birini içermemelidir:

(I) Sözlük (herhangi bir dil), argo veya genel kısaltmadan alınan bir kelime.

(II) Bir kişinin veya yerin adı.

(III) Kullanıcının eşi/partnerinin doğum günü gibi kolayca tahmin edilebilen bir tarih.

(IV) Kullanıcının araç plakası, TC Kimlik numarası, giriş kartı numarası gibi kullanıcı ile ilgili olduğu bilinen bilgiler.

(V) Hesap kullanıcı adı ile aynı veya ona yakın (kullanıcı adının ters çevrilmesi veya yanlış yazılması dâhil olmak üzere)

(VI) Şirketin kurumsal web sitesinde veya işbu Yönetmelikte örnek olarak verilen herhangi bir şifre, bilgi vb.

2.1.4. Yeni belirlenecek şifre, kullanılan son 4 şifreden biriyle aynı olamaz.

3. ŞİFRELERİN KORUNMASI İÇİN TAKİP EDİLMESİ GEREKEN İLKELER

3.1. Kullanıcılar akılda kalıcı bir şifre seçmeli ve şifreleri yazmaktan kaçınmalı ve hiçbir koşulda başkalarının kolayca erişebileceği bir yerde şifre bırakmamalıdır.

3.2. Kullanıcılar şifrelerini başkalarına açıklamamalıdır. Şirket hiçbir zaman bir kullanıcının şifresini istemez. Parolanızı bilmesi gereken tek kişi kullanıcıdır. Bu yönde bir talep içeren herhangi bir e-mail, mesaj vb. kullanıcıya ulaştığı takdirde söz konusu ileti e-dolandırıcılık teşebbüsü olarak değerlendirilmeli, cevap vermekten kaçınılarak derhal IT sorumlusuna bilgi verilmelidir.

3.3. Bir kullanıcı şifresinin yanlışlıkla veya başka bir şekilde ifşa edildiğini fark ederse, şifresini derhal değiştirmeli ve derhal IT sorumlusuna bilgi verilmelidir.

3.4. Kullanıcı giriş şifresini ekrana yazarken başkalarının ekranını görmediğinden emin olmalı ve kullanıcı şifresini girerken çalışma arkadaşları dâhil kimsenin

görebileceği şekilde ekranını konumlandırmamalı ve bina dışından görülmeyecek şekilde ekranlar ofis içerisinde yerleştirilmelidir.

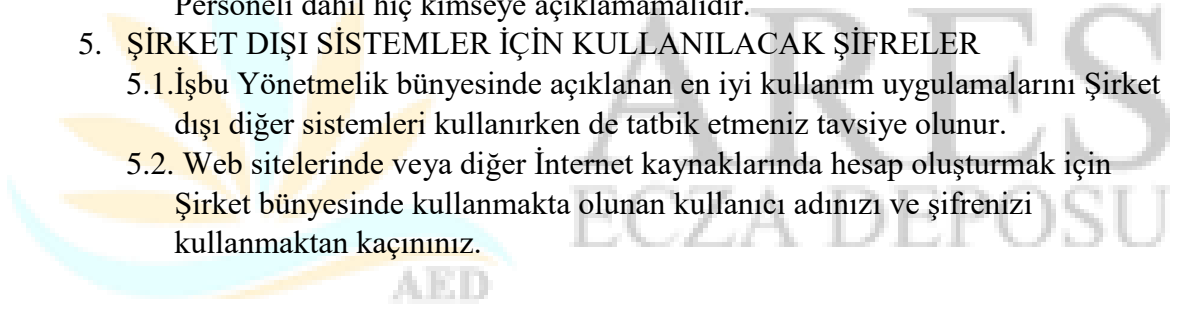
- 3.5. Kullanıcılar, Şirketin kurumsal resmi bilişim ve haberleşme sistemleri / web sitesi olduğundan emin olmadıkları sürece şifrelerini bir web sitesine girmemelidir. Bunu sağlamanın en iyi yöntemi, sitelere kendi yer imlerinizi vermeniz veya girilmiş URL'lerinizi kullanarak erişmektir. Özellikle meşru olduğunu iddia eden e-postaların içindeki bağlantıları kullanmaktan kaçınınız.

4. ŞİFRELERİN DEĞİŞTİRİLMESİ

- 4.1. Kullanıcıların düzenli aralıklarla şifrelerini değiştirmeleri elzemdir. Departman şefleri ile IT Departmanı Şefi, Şirketin yetkilendirdiği hesap sahiplerinin rollerine ve sorumluluklarına bağlı olarak 30 gün ile bir yıl arasında şifre değiştirme periyodunu belirleyebilirler.
- 4.2. Şirket envanterine kayıtlı bilgisayarlarda oturum açarak şirketin kurumsal e-mail sunucusunun göstereceği bağlantıyı kullanarak şifrenizi değiştirebilirsiniz:
- 4.3. Eski şifrelerin dönüşümlü olarak kullanımına izin verilmez. Bu, Şirket dışı sistemler için de kullanabileceğiniz iyi bir uygulamadır.
- 4.4. Kullandıkları şifrelerin İşbu Yönetmelik hükümlerine uygun olmadığı tespit edilen kullanıcıların derhal şifrelerini değiştirmeleri istenecektir.
- 4.5. Şifrelerini değiştirmesi gereken kullanıcılarla e-posta, telefon veya şahsen bir Şirket personeli tarafından iletişime geçilecektir. Kullanıcılar, şifrelerini Şirket Personeli dâhil hiç kimseye açıklamamalıdır.

5. ŞİRKET DIŞI SİSTEMLER İÇİN KULLANILACAK ŞİFRELER

- 5.1. İşbu Yönetmelik bünyesinde açıklanan en iyi kullanım uygulamalarını Şirket dışı diğer sistemleri kullanırken de tatbik etmeniz tavsiye olunur.
- 5.2. Web sitelerinde veya diğer İnternet kaynaklarında hesap oluşturmak için Şirket bünyesinde kullanmakta olunan kullanıcı adınızı ve şifrenizi kullanmaktan kaçınınız.





ARES
ECZA DEPOSU