

PAROLA POLİTİKASI

Bu politikanın amacı, kurum bilgi varlıklarının korunması için kullanılan tüm kimlik doğrulama mekanizmalarında güçlü, benzersiz ve güvenli parola kullanımını sağlamaktır. Politika; ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi ve Siber Hijyen gereklilikleri doğrultusunda hazırlanmıştır.

Güçlü Parola Kuralları

Parolalar minimum aşağıdaki gereklilikleri sağlamalıdır:

- En az 8 karakter uzunlukta olup keepass gibi korunaklı uygulamalarda saklanmalıdır.
- Büyük harf, küçük harf, rakam ve özel karakter kombinasyonundan oluşmalıdır,
- Kolay tahmin edilebilir bilgiler (ad, doğum tarihi, kullanıcı adı) kullanılmamalıdır,
- Kolay tahmin edilebilir yaygın kelimeler kullanılmamalıdır,
- Parola; daha önce kullanılmış son 7 paroladan biri olmamalıdır.

Parola Yenileme Süresi

- Parola zorunlu periyodik yenileme süresi 90 gündür.

Parola Paylaşımı Yasaktır

- Hiçbir parola, yönetici dahil olmak üzere, kimseyle paylaşılamaz.
- Geçici parola paylaşımları yasaktır; bunun yerine yetkilendirme mekanizmaları kullanılmaktadır.

Çok Faktörlü Kimlik Doğrulama (MFA)

Aşağıdaki sistemlerde MFA zorunludur:

- VPN erişimleri,
- Bulut hizmetleri,
- Yönetici hesapları,
- Kritik uygulamalar,
- Dış erişimi olan tüm sistemler,

Genel Müdür

PAROLA POLİTİKASI

Parola Saklama ve Yönetim Kuralları

- “Temiz Masa Temiz Ekran Politikası” kuralları geçerlidir.
- Parolalar asla düz metin olarak saklanamaz.
- Kullanıcılar parola yöneticisi (password manager) kullanmaya teşvik edilmelidir.
- Parolalar, E-posta içinde veya paylaşımlı alanlarda tutulamaz.

Yönetici Hesapları İçin Ek Kurallar

- Admin hesapları kişiye özel olmalı; ortak “admin” hesabı kullanılmamalıdır.
- Yönetici hesapları günlük işler için kullanılmamalı, yalnızca ihtiyaç halinde yetkilendirilmelidir.
- Yüksek kritik sistemlerde farklı seviyelerde admin hesabı uygulanmalıdır (tiering).

Hizmet Hesapları İçin Ek Kurallar

- Parolalar karmaşık ve otomatik kullanım için tasarlanmış olmalıdır.
- “Hiç süresi dolmayan parola” kullanımı yasaktır.
- Hizmet hesaplarının yetkileri minimum seviyede tutulmaktadır.

Kullanıcı Sorumlulukları

Kullanıcılar:

- Parolalarını paylaşmaları yasaktır,
- Aynı parolayı iş ve kişisel hesaplarında kullanmaları yasaktır,
- Şüpheli bir aktivite fark ederse derhal bildirmekle mükelleftir,
- Parolasını kimsenin göremeyeceği şekilde girmelidir.

Parola İhlalleri ve Bildirim

- Parola güvenliğinin ihlal edildiği şüphesi oluştuğunda kullanıcı derhal yardım masasına veya bilgi güvenliği ekibine haber vermelidir.
- Riskli görülen tüm kullanıcı parolaları sistem tarafından sıfırlanabilir.
- İhlal sonrası kullanıcı eğitimi ve farkındalık süreci uygulanmaktadır.

İstisnalar

- Teknik olarak uygulamanın mümkün olmadığı durumlarda istisna talebi yazılı olarak yapılır.
- Risk azaltıcı önlemler devreye alınır.

Genel Müdür