1. AMAÇ

Bu doküman, İzmir Yüksek Teknoloji Enstitüsü bünyesindeki Bilgi İşlem Daire Başkanlığı kapsamındaki bilgi ve bilgi işleme olanaklarına erişim için kullanılan parolalarının yönetimi için gereken kuralları tanımlamak amacıyla oluşturulmuştur.

2. KAPSAM

Şifreleme bilgisayar güvenliği için önemli bir özelliktir. Kullanıcı hesapları için ilk güvenlik katmanıdır. Zayıf seçilmiş bir şifre ağ güvenliğini tümüyle riske atabilir. İzmir Yüksek Teknoloji Enstitüsü çalışanları ve uzak noktalardan erişenler aşağıda belirtilen kurallar dâhilinde şifreleme yapmakla sorumludurlar.

3. KISALTMALAR VE TANIMLAR

Terim	Tanım/Açıklama
Aktif Dizin Etki Alanı	Bünyesinde kullanıcılar, gruplar ve yapılandırma bilgileri gibi pek çok öğeyi barındıran; kimlik doğrulama, yetkilendirme gibi özellikleri barındıran yapı.
BGYS	Bilgi Güvenliği Yönetim Sistemi
Kurum	İzmir Yüksek Teknoloji Enstitüsü

4. PAROLA POLİTİKASI

Parolalar, kurum bilgilerini korumak için uygulanan en önemli güvenlik önlemidir. Bu yüzden kolay tahmin edilemeyen ve güvenlik gerekliliklerini karşılayacak şekilde bir parola belirlenmelidir. Parola belirlerken dikkat edilmesi gereken hususlar aşağıda tanımlanmıştır:

(1) Kullanıcılar, kendilerine verilmiş olan kullanıcı adlarını ve parolalarını Daire Başkanı yada Üst Yönetim dahil başkaları ile paylaşmaz ve korurlar. Aksi durumlarda oluşabilecek olumsuz olaylardan kullanıcının kendisi sorumlu olacaktır.

(2) Kullanıcıların aktif dizin etki alanı parolalarının uzunluğu, süresi, karmaşıklığı gibi özellikler, Bilgi İşlem Daire Başkanlığı yetkili personeli tarafından düzenlenir.

(3) Parola kullanım süresi bittiğinde kullanıcının tekrar parola oluşturması sağlanır.

(4) Kullanıcılar, parolalarının ele geçirildiğinden kuşkulandıklarında Bilgi İşlem Daire Başkanlığına haber verir, gereken önlemleri alır ve bilgi güvenliği ihlal olayı kaydı açılır.

(5) Kullanıcılar, İzmir Yüksek Teknoloji Enstitüsü hizmetleri için kullandıkları parolaları, internet üzerinde İzmir Yüksek Teknoloji Enstitüsü tarafından sağlanmayan ortamlarda kullanmaz.

(6) Parolalar, dosya, otomatik komut dosyası, yazılım makrosu, erişim kontrolü olmayan bilgisayarlar ve başkalarının fark edebileceği şekilde bilgisayar donanımlarının fiziksel dış alanlarına, not kağıtlarına yazılmaz; başkalarının görebileceği şekilde herhangi bir panoya asılmaz.

(7) Sistemlere giriş ekranlarında herhangi bir ipucu olmaz. Eğer böyle bir işlem adımı var ise parola hatırlatması yapılmaz ve kullanıcıya geçici parola verilir. Hesabın bloke olması ya da parolanın unutulması durumlarında Bilgi İşlem Daire Başkanlığı personeline başvurulur.

(a) Parolalar, en az 9 karakterden oluşur ve büyük harf, küçük harf, alfa numerik ve rakam özelliklerinin hepsini içerecek şekilde karmaşık olarak belirlenir.
(8) Kurumsal bilgiye erişilebilen mobil cihazlar için ekran kilidi kullanımı zorunludur. Ekran kilidini açmak için kolay tahmin edilemeyen pin kodu, parola veya desen kullanılır.

5. İLGİLİ DOKÜMANLAR

5.1. İç Kaynaklı Dokümanlar

- E-posta Kullanım Kılavuzu
- İYTE E-Posta Kullanım Yönergesi

5.2. Dış Kaynaklı Dokümanlar

TS ISO/IEC 27001:2022 Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler