	TNKÜ PAROLA POLİTİKASI	Doküman No:	EYS-PO-012
		Hazırlama Tarihi:	07.09.2018
		Revizyon Tarihi:	14.08.2025
		Revizyon No:	2
		Toplam Sayfa Sayısı:	3

1 AMAÇ

Bu politikanın amacı, Tekirdağ Namık Kemal Üniversitesi Bilgi İşlem Daire Başkanlığı bünyesinde her türlü sisteme erişim için kullanılan/kullanılabilecek kullanıcı adı ve parola ile erişim sağlanan sistemlerin güvenliği için gerekli parolaların minimum gereksinim politikasını tanımlanmasıdır.

2 KAPSAM

Tekirdağ Namık Kemal Üniversitesi Bilgi İşlem Daire Başkanlığı bünyesinde çalışan tüm personel ve koşan sistemler bu politika kapsamındadır.

3 SORUMLULAR

Bu prosedürün oluşturulmasından BGYS Yönetim Temsilcisi sorumludur. Politikanın uygulanmasından tüm Tekirdağ Namık Kemal Üniversitesi Bilgi İşlem Daire Başkanlığı personeli sorumludur.

4 KURALLAR

Güçlü parola politikası, bilgi güvenliğinin sağlanması açısından kritik bir öneme sahip olup, varlıkların yetkisiz erişimlerinden korunması açısından kullanıcı hesaplarında en önemli güvenlik katmanını teşkil etmektedir. Zayıf seçilmiş bir parola ağ ve sistem güvenliği başta olmak üzere tüm altyapıyı, uygulamaları ve verileri riske atabilir. Uzaktan erişenler dahil tüm kurum personeli aşağıdaki tanımlanmış genel kurallara uymakla sorumludur.

4.1 Genel Kurallar

a) Bütün sistem seviyesinde kullanılan parolalar (örnek: root, administrator, enable vb.) en geç 1 yılda bir değiştirilmelidir.

b) Bütün kullanıcı seviyeli parolalar (örnek: e-posta, web, masaüstü bilgisayar, uygulamalar vb.) en geç 6 ayda bir değiştirilmelidir.

c) Sistem yöneticileri her sistem için farklı parolaları kullanmalıdır.

d) Parolalar e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.

e) Parolalar herhangi bir yerde not edilerek saklanmamalıdır.

f) Parolalar güçlü (örnek: parola uzunluğu, karakter çeşitliliği, sözlük dışı ifadeler gibi) sayılabilecek nitelikle özellikleri barındırmalıdır.

g) Kurum çalışanı olmayan harici kişiler için açılan kullanıcı hesaplarının parolaları da kolayca kırılamayacak güçlü bir yapıya sahip olmalıdır.

4.2 Parola Oluşturmada Dikkat Edilecek Noktalar

Parolalar aşağıda detayları verilen “zayıf parola” yapısından uzak olmalı ve “güçlü parola” yapısına uygun olmalıdır.

4.2.1 Zayıf Parolalar

Zayıf parolalar aşağıdaki karakteristiklere sahip olup kullanıcılar bu tip özelliklerden parola seçiminden kaçınmalıdır.

a) Parolalar 6 veya daha az karaktere sahiptirler.

b) Parolalar aşağıdaki gibi ortak değere sahiptir.

- Harf ve rakamlardan karmaşık oluşmayan
- Sözcükte geçen kelimelerden oluşturulan
- Bilgisayar terminolojisi vb. isimleri: komutlar, siteler, şirketler, donanım, yazılım vb.
- ”Merve”, ”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).

4.2.2 Güçlü Parolalar

Güçlü parolalar aşağıdaki karakteristiklere sahip olup kullanıcılar bu tip parola kurallarını uygulamalıdır:

a) Hem küçük hem de büyük karakterlere sahiptir (örnek, a-z, A-Z)

b) Hem sayısal hem de noktalama karakterleri gizi özel karakterlere sahiptir. (0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)

c) Sözlük isimleri gibi kelime bilgilerine ait olmamalıdır.

d) Parolalar herhangi bir yere yazılmamalıdır veya elektronik ortamda şifresiz olarak tutulmamalıdır. Karmaşık parolaları seçerken, herhangi bir yere yazmadan kolayca hatırlanabilen parolalar oluşturulmalıdır. Örnek olarak; ”Birinci kalite hedefimiz, müşteri memnuniyetinin sağlanmasıdır!” cümlesindeki gibi ”1Kh,MmS!” veya türevleri şeklinde olabilir.

e) Kurum içinde kullanılması zorunlu olan şifre politikası minimum 8 karakterden oluşan en az bir büyük harf, en az bir küçük harf ve en az bir sayı karakteri barındıran parolalardır.

Not: Yukarıdaki herhangi bir örneği şifre olarak kullanmayınız.

4.3 Parolaların Korunması

Bütün kullanıcılar aşağıdaki kurallara titizlikle uymalıdır.

a) Kurum bünyesinde kullanılan parolalar, kurum dışında herhangi bir şekilde kullanılmamalıdır. (örnek: internet erişim parolaları, bankacılık işlemlerinde veya diğer yerlerde).

b) Değişik sistemler için farklı parolalar kullanılmalıdır. Örnek: Unix sistemler için farklı parolalar, Windows sistemler için farklı parolalar.
c) Kurum bünyesinde kullanılan parolalar hiç kimseyle paylaşılmamalıdır. Bütün parolalar kurum ait özel bilgiler olarak düşünülmelidir.
d) Hiç bir kişiye kendisine ait parolayı sözlü veya yazılı telefonla paylaşmamalıdır.
e) Üst yönetici dahil hiç kimseye parola söylenmemelidir.
f) Başkaları önünde parolalar hakkında konuşulmamalıdır.
g) Aile bireylerine ait isimler parola olarak kullanılmamalıdır.
h) Herhangi form üzerinde parola belirtilmemelidir.
i) Parolalar aile bireyleri ile paylaşılmamalıdır.
j) Parolalar, işten uzakta olunan zamanlarda iş arkadaşlarına söylenmemelidir.
k) Uygulamalardaki "parola hatırlatma" özellikleri parola olarak seçilmemelidir. (örnek: Outlook, Internet Explorer vs.)

5 YAPTIRIM

Bu politikanın ihlal edilmesi durumunda Disiplin Prosedürü uygulanacaktır.

6 İLGİLİ DOKÜMANLAR

EYS-PR.021 - DİSİPLİN PROSEDÜRÜ