İÇİNDEKİLER

1 Amaç

Bu politikanın amacı, ESOGÜ BİDB bünyesinde her türlü sisteme erişim için kullanılan/kullanılabilecek kullanıcı adı ve parola ile erişim sağlanan sistemlerin güveliği için gerekli parolaların minimum gereksinim politikasını tanımlanmasıdır.

2 Kapsam

ESOGÜ BİDB bünyesinde çalışan tüm personel ve koşan sistemler bu politika kapsamındadır.

3 Sorumlular

Bu prosedürün oluşturulmasından BGYS Yönetim Temsilcisi sorumludur. Politikanın uygulanmasından tüm ESOGÜ BİDB 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 ESOGÜ personeli ve öğrencileri aşağıdaki tanımlanmış genel kurallara uymakla sorumludur.

4.1 Genel Kurallar

4.1. Parola oluşturma kuralları (genel)

• Parolalar en az 10 karakter uzunluğunda olmalıdır ve bu karakterlerin en az bir tanesi sayılardan, bir tanesi büyük harf bir tanesi de küçük harften oluşmalıdır.

• Aşağıdaki karakterlerin en az üçünü içermelidir;

- o Büyük harf, (örn. ABCDEF...)
- o Küçük harf, (örn, abcdef ...)
- o Rakam, (örn: 1234567890)
- o Noktalama işareti, (örn: !?., vb.)

Hazırlayan	Kontrol Eden	Onaylayan
DİLEK ÇELİK	SEVİNÇ ÇOLAK	SERKAN UĞURLUOĞLU

o Özel karakterler (Örn: @#$%^&*()_+|~-=\`{}[]:";'<>/ vb.)

• Parolalar aşağıdaki şekilde oluşturulmamalıdır;

o İçeriğinde, kişisel bilgiler bulunmamalıdır (örneğin aile bireylerinin isimleri, doğum tarihleri, telefon numarası veya adres bilgileri gibi)

o Kelime veya rakam dizileri kullanılmamalıdır. (Örn; aaabbb, qwerty, zyxwvuts, 12345678, 123321, vb.)

4.2. Parola oluşturma kuralları (Sistem)

• Tüm kullanıcı hesaplarına ait bir parola vardır.

• Yeni kullanıcı hesaplarına ait parolaların ilk kez giriş yapılırken kullanıcı tarafından kurallara uygun olarak tanımlanması sağlanır.

• Başarısız parola denemeleri üst üste 3 kere ile sınırlandırılmıştır. Üçüncü denemeden sonra şifre ve bağlı olduğu kullanıcı, kullanım dışı bırakılır. Parolanın yenilenmesi için destek ogu.edu.tr den konu ile ilgili çağrı açılır, Eğer kullanıcı öğrenci ise kimlik ile birlikte BİDB Sistem Destek birimine şahsen gelmesi gerekmektedir.

• Yazılan parolanın ekranda görünmemesi veya maskelenerek görünmesi sağlanır.

• Kullanıcı parolaları, saklandıkları ortamlarda, geri dönüşü mümkün olmayan bir şekilde maskelenerek korunur (örneğin Hash), bu sayede en yetkili kişilerin bile kullanıcı parolasını görmesi engellenir.

• Bilgi kaynaklarına başarılı ve başarısız erişimlerin tarih, zaman ve erişilen kaynağın detayı ile ilgili bilgilerinin kaydı tutulur.

• Kullanıcıların kimlik doğrulaması yaparak oturum açtıkları sistemlerin başından ayrıldıklarında (sisteme parola ile giriş yapıldıktan sonra sistem açık bırakılması halinde) en geç 30 dakika sonra otomatik olarak kapanması (sistemin kilitlenmesi) sağlanır.

• Halka açık veya paylaşılan ağlardan iletilen kimlik bilgileri güçlü şifreleme metotları ile (SSL,TLS) korunur.

• Başkaları tarafından öğrenildiğinden şüphelenilen parolalar hemen değiştirilir.

Hazırlayan	Kontrol Eden	Onaylayan
DİLEK ÇELİK	SEVİNÇ ÇOLAK	SERKAN UĞURLUOĞLU

4.3. Parola kullanım kuralları
Sistem yönetim birimi:

- Bütün sistem seviyesinde kullanılan parolalar (örnek: root, administrator, enable vb.) en geç 6 ayda bir değiştirilmelidir.
- Bütün kullanıcı seviyeli parolalar (örnek: e-posta, web, masaüstü bilgisayar, uygulamalar vb.) en geç 6 ayda bir değiştirilmelidir.
- Sistem yöneticileri her sistem için farklı parolaları kullanmalıdır.
- Parolalar e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.
- Parolalar herhangi bir yerde not edilerek saklanmamalıdır.
- Parolalar güçlü (örnek: parola uzunluğu, karakter çeşitliliği, sözlük dışı ifadeler gibi) sayılabilecek nitelikle özellikleri barındırmalıdır.
- Kurum çalışanı olmayan harici kişiler için açılan kullanıcı hesaplarının parolaları da kolayca kırılamayacak güçlü bir yapıya sahip olmalıdır.

Tüm kullanıcılar:

• Her yeni parola için, son kullanılan 7 paroladan farklı yeni bir parola kullanılmalıdır.

• Parolalar hiç kimse ile paylaşılmamalıdır.

• Parolaların klavyeden girilmesi sırasında dikkatli olunmalı ve çevredeki kişilerin görmesine izin vermeyecek şekilde girilmelidir.

• E-posta yoluyla parolaların onaylanması veya güncellenmesi istenmez, bu yönde gelen e-postalar dikkate alınmamalıdır.

• Aynı parola birden fazla kaynakta kullanılmamalıdır.

• Parolalar ilave bir şifreleme metodu kullanılmadan hatırlamak amacıyla kayıt edilmemelidir (kâğıt, bilgisayardaki bir dosya, cep telefonu gibi ortamlarda saklanmamalıdır).

• İnternet tarayıcılarında (internet explorer, chrome, firefox vb.) "Parolayı hatırla" seçeneğinin kişisel bilgisayarlar dışında kullanılması yasaktır, kişisel bilgisayarlarda ise bir güvenlik açığı olduğu hatırlanmalıdır.

Hazırlayan	Kontrol Eden	Onaylayan
DİLEK ÇELİK	SEVİNÇ ÇOLAK	SERKAN UĞURLUOĞLU

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 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.

Hazırlayan	Kontrol Eden	Onaylayan
DİLEK ÇELİK	SEVİNÇ ÇOLAK	SERKAN UĞURLUOĞLU

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 Yaptırım

Bu politikanın ihlal edilmesi durumunda BGYS yöneticisi tarafından gerekli personel desteği de alınarak ihlal nedeni incelenir. İhlal kasıtsız olup personelin eğitim vb. bir eksikliğinden kaynaklanıyorsa problemin kaynağını oluşturan eksikliği kapatmak için çalışma yapılır. Personel BGYS Yöneticisi tarafından e-posta üzerinden yazılı olarak uyarılır.

Eğer ihlal işleminin kasıtlı olduğu anlaşılırsa veya kasıtsız olan ihlaller 3'ten fazla tekrar ederse 657 sayılı devlet memurları kanunu ve Üniversite resmi yazısıyla belirtilen ilave yaptırımlar gereğince personel hakkında işlem yapılır.

Tüm çalışanlar, güvenlik ihlali olaylarını ve bu politikanın ihlallerini, Olay İhlal Yönetimi Prosedüründe tanımlanan şekilde en kısa sürede bildirme sorumluluğundadır.

Hazırlayan	Kontrol Eden	Onaylayan
DİLEK ÇELİK	SEVİNÇ ÇOLAK	SERKAN UĞURLUOĞLU

6 İlgili Dokümanlar

PR.12 - OLAY İHLAL YÖNETİM PROSEDÜRÜ

Hazırlayan	Kontrol Eden	Onaylayan
DİLEK ÇELİK	SEVİNÇ ÇOLAK	SERKAN UĞURLUOĞLU