	PAROLA POLİTİKASI	Doküman No	PL.12
		Yayın Tarihi	16.07.2018
		Revizyon No	07
		Revizyon Tarihi	28.04.2026
		Sayfa No	1/9

Hazırlayan	Kontrol Eden	Onaylayan
BİLGİ GÜVENLİĞİ BİRİMİ	BİDB ŞUBE MÜDÜRÜ	BİDB DAİRE BAŞKANI

1 Amaç

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

2 Kapsam

ESOGÜ personeli ve öğrencileri, BİDB bünyesinde çalışan tüm personel ve kullanılan/koşan sistemler bu politika kapsamındadır.

3 Tanımlar ve Kısaltmalar

ESOGÜ: Eskişehir Osmangazi Üniversitesi

BİDB: Bilgi İşlem Daire Başkanlığı

BGYS: Bilgi Güvenliği Yönetim Sistemi

SSL: Secure Sockets Layer (Güvenli Soket Katmanı)

TLS: Transpot Layer Security (Taşıma Katmanı Güvenliği)

P.A.M: (Privileged Access Management) Ayrıcalıklı Erişim Yönetimi

4 Sorumlular

Bu politikanın oluşturulmasından Bilgi Güvenliği Birimi sorumludur. Politikanın uygulanmasından tüm ESOGÜ personeli, öğrencileri ve BİDB personeli sorumludur.

5 Genel 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 bu politikada tanımlanmış genel kurallara uymakla yükümlüdür. Netyetki için yeni parola belirlendiğinde aynı parola eposta hesabı için de geçerli olacaktır.

5.1 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 karakter türlerinin her birinden en az bir adet karakter içermelidir;

- Büyük harf, (örn. ABCDEF...)
- Küçük harf, (örn, abcdef ...)
- Rakam, (örn: 1234567890)

Parolalar aşağıdaki şekilde oluşturulmamalıdır

- İçeriğinde, kişisel bilgiler bulunmamalıdır (örneğin aile bireylerinin isimleri, doğum tarihleri, telefon numarası veya adres bilgileri gibi)
- Kelime, harf veya rakam dizileri kullanılmamalıdır. (Örn; kalem, aaabbb, qwerty, zyxwvuts, 12345678, 123321, vb.)

5.2 Parola Oluşturma Kuralları (Sunucu Yönetimi)

- Parolaları üretmek ve yönetmek için P.A.M. (Privileged Access Management) Ayrıcalıklı Erişim Yönetimi uygulaması kullanılır.
- Bütün sunucu ve sistem yönetimi seviyesinde kullanılan parolalar (örnek: root, administrator, enable vb.) en geç 3 ayda bir değiştirilir.
- Kullanılan uygulama üzerinde parola otomatik olarak üretilir.
- Kullanılan uygulamada, Parola 20 karakterden oluşmak üzere büyük harf, küçük harf ve rakam kombinasyonlarından oluşan rastgele karakterler üretir. Kullanılan uygulama, oluşan bu karakterler arasından seçme algoritması kullanarak parola oluşturur.
- Bilgi sistemlerine başarılı ve başarısız erişimlerin tarih, zaman ve erişilen kaynağın detayı ile ilgili bilgilerin kaydı tutulur.

5.3 Veri Tabanı Kullanıcısı Parola Oluşturma Kuralları

5.3.1 Parola Oluşturma

- Parolaları üretmek ve yönetmek için P.A.M. (Privileged Access Management) Ayrıcalıklı Erişim Yönetimi uygulaması kullanılır.
- Bütün veri tabanı, sunucu ve sistem yönetimi seviyesinde kullanılan parolalar (örnek: masterpass, root, administrator, enable vb.) en geç 3 ayda bir değiştirilir.
- Kullanılan uygulama üzerinde parola otomatik olarak üretilir.
- Kullanılan uygulamada, Parola 20 karakterden oluşmak üzere büyük harf, küçük harf ve rakam kombinasyonlarından oluşan rastgele karakterler üretir. Kullanılan uygulama, oluşan bu karakterler arasından seçme algoritması kullanarak parola oluşturur.

5.3.2 Parola Paylaşımı

- PAM üzerinde tanımlı kullanıcılar ile PAM üzerinden
- PAM üzerinde tanımlı kullanıcısı olmayan kişilere bidbdrive üzerinden yapılır.
- Kişisel kullanıcı hesabı oluşturulduysa parola paylaşıldıktan sonra, ilk login durumunda parola değişimine zorlanır.

6 Parola Kullanım Kuralları

6.1 Sunucu ve İnternet Sistemleri Birimi

- Bütün sunucu ve sistem yönetimi seviyesinde kullanılan parolalar (örnek: root, administrator, enable vb.) en geç 3 ayda bir değiştirilmelidir.
- Her yeni parola için, son kullanılan 7 paroladan farklı yeni bir parola kullanılmalıdır.
- Bütün kullanıcı seviyeli parolalar (örnek: e-posta, web, masaüstü bilgisayar, uygulamalar vb.) en geç 3 ayda bir değiştirilmelidir.

- Sistem yöneticileri her sistem için farklı parolalar kullanmalıdır.
- Parolalar e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.
- Parolalar ilave bir şifreleme metodu kullanılmadan hatırlamak amacıyla kayıt edilmemeli, herhangi bir yerde, görülebilecek, anlaşılabilecek şekilde kâğıt, bilgisayardaki bir dosya, cep telefonu gibi ortamlarda, not edilerek saklanmamalıdır.
- Parolalar güçlü (örnek: parola uzunluğu, karakter çeşitliliği, sözlük dışı ifadeler gibi) sayılabilecek nitelikte özellikleri barındırmalıdır.

6.2 Tüm Kullanıcılar

- Her yeni parola için, son kullanılan 7 paroladan farklı yeni bir parola kullanılmalıdır.
- Parolalar hiç kimse ile paylaşılmamalıdır.
- Başkaları tarafından öğrenildiğinden şüphelenilen parolalar, kullanıcı tarafından hemen değiştirilmelidir.
- Parolaların klavyeden girilmesi sırasında dikkatli olunmalı ve parolalar çevredeki kişilerin görmesine izin vermeyecek şekilde girilmelidir.
- Aynı parola birden fazla kaynakta kullanılmamalıdır.
- İnternet tarayıcılarında (internet explorer, chrome, firefox vb.) “Parolayı hatırla” seçeneğinin kişisel bilgisayarlar dışında kullanılmaması gerekir, kişisel bilgisayarlarda ise, “Parolayı hatırla” seçeneğinin kullanılması durumunda, bunun bir güvenlik açığı oluşturabileceği hatırlanmalıdır.
- Bütün kullanıcı seviyeli parolalar (örnek: Netyetki, web, masaüstü bilgisayar, uygulamalar vb.) en geç 3 ayda bir değiştirilmelidir.
- Parolalar e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.
- Parolalar ilave bir şifreleme metodu kullanılmadan hatırlamak amacıyla kayıt edilmemeli, herhangi bir yerde, görülebilecek, anlaşılabilecek şekilde kâğıt, bilgisayardaki bir dosya, cep telefonu gibi ortamlarda, not edilerek saklanmamalıdır.

- e-posta hesabı için, başarısız parola denemeleri, son 1 dakika içinde üst üste 20 kere ile sınırlandırılmıştır. Yirminci denemeden sonra şifre ve bağlı olduğu kullanıcı hesabı, 1 saat için kullanım dışı bırakılır.

- Netyetki hesabı için, başarısız parola denemeleri, son 5 dakika içinde üst üste 5 kere ile sınırlandırılmıştır. Beşinci denemeden sonra şifre ve bağlı olduğu kullanıcı hesabı, 5 dakika için kullanım dışı bırakılır.

7 Parola Oluşturmada Dikkat Edilecek Noktalar

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

7.1 Zayıf Parolalar

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

- Parolalar 6 veya daha az karaktere sahiptirler
- 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
- Herhangi bir kelimenin ya da dizinin geri yazılış şekli
- Herhangi bir kelimenin rakamla takip edilmesi (örnek, gizli1, gizli2)

7.2 Güçlü Parolalar

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

- Hem küçük hem de büyük karakterlere sahiptir (örnek, a-z, A-Z)
- Hem sayısal hem de noktalama karakterleri gibi özel karakterlere sahiptir. (0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Parolalar herhangi bir yere yazılmamalıdır veya elektronik ortamda tutulmamalıdır. Karmaşık parolaları seçerken, herhangi bir yere not etmeden kolayca hatırlanabilen parolalar oluşturulmalıdır. Örnek olarak; ”Birinci kalite hedefimiz, müşteri memnuniyetinin sağlanmasıdır!” cümlesindeki gibi ”1Kh,MmS!” veya türevleri şeklinde olabilir.
- Kurum içinde kullanılması zorunlu olan parolalar minimum 10 karakterden oluşan en az bir büyük harf, en az bir küçük harf ve en az bir sayı karakteri barındıran parolalardır.

7.3 Parolaların Korunması

Bütün kullanıcılar aşağıdaki kurallara titizlikle uymalıdır.

- Kurum bünyesinde kullanılan parolalar, kurum dışında herhangi bir şekilde kullanılmamalıdır. (örnek: internet erişim parolaları, bankacılık işlemlerinde veya diğer yerlerde).
- Değişik sistemler için farklı parolalar kullanılmalıdır. Örnek: Unix sistemler için farklı parolalar, Windows sistemler için farklı parolalar.
- Kurum bünyesinde kullanılan parolalar hiç kimseyle paylaşılmamalıdır. Bütün parolalar kurum ait özel bilgiler olarak düşünülmelidir.
- Hiç bir kişiye kendisine ait parolayı sözlü, yazılı veya telefonla paylaşmamalıdır.
- Üst yönetici dahil hiç kimseye parola söylenmemelidir.
- Başkaları önünde parolalar hakkında konuşulmamalıdır.
- Aile bireylerine ait isimler parola olarak kullanılmamalıdır.
- Herhangi form üzerinde parola belirtilmemelidir.
- Parolalar aile bireyleri ile paylaşılmamalıdır.

- Parolalar, işten uzakta olunan zamanlarda iş arkadaşlarına söylenmemelidir.
- Uygulamalardaki "parola hatırlatma" özellikleri parola olarak seçilmemelidir. (örnek: Outlook, Internet Explorer vs.)

8 İstisnai Durumlar

Üniversitede kullanılmakta olan cihaz, uygulama ve yazılımların kullanımı için tanımlanmış olan ve buradan kullanıcılara bildirim/otomatik eposta gönderen hesaplara ait parolaların 3 ayda bir yenilenmesinin olağanüstü bir zorluk oluşturduğu durumlarda; ilgili birim tarafından Bilgi İşlem Daire Başkanlığına gerekçesi belirtilerek parola yenileme zorunluluğunun kaldırılması talebi resmi yazı ile bildirildiğinde talebin uygunluğu değerlendirilerek işlem gerçekleştirilir.

9 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.

Kullanıcının e-posta parolası, netyetki parolası veya diğer kurumsal parolalarından birinin, başkası tarafından çalındığının tespiti durumunda, kullanıcının e-posta, netyetki vb. hesabı geçici olarak kullanıma kapatılır. Kullanıcı EBYS 'den yazılan resmi yazı ile bilgilendirilerek, parolasını değiştirmesi sağlanır.

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.

Hazırlayan	Kontrol Eden	Onaylayan
BİLGİ GÜVENLİĞİ BİRİMİ	BİDB ŞUBE MÜDÜRÜ	BİDB DAİRE BAŞKANI

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

10 İlgili Dokümanlar

PR.12 - OLAY İHLAL YÖNETİM PROSEDÜRÜ

Hazırlayan	Kontrol Eden	Onaylayan
BİLGİ GÜVENLİĞİ BİRİMİ	BİDB ŞUBE MÜDÜRÜ	BİDB DAİRE BAŞKANI