

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	KULLANICI HESABI YÖNETİMİ PROSEDÜRÜ	Doküman No	BGYS-PR20
		Yayın Tarihi	05.01.2022
		Revizyon Tarihi	
		Revizyon No	00
		Sayfa No	1 / 3

1. AMAÇ

Bu prosedürün amacı, Gençlik ve Spor Bakanlığı Bilgi İşlem Dairesi Başkanlığı'ndaki yürütülen faaliyetler sırasında kullanıcı tanımlama, şifre işlemleri, otomatik oturum kapatma, firewall, uzaktan erişim ve kablosuz erişim ile ilgili yöntemleri belirlemektir.

2. KAPSAM

Bu prosedürün uygulanmasından Gençlik ve Spor Bakanlığı Bilgi İşlem Dairesi Başkanlığı'ndaki tüm çalışanlar sorumludur.

3. KISALTMALAR VE TANIMLAR

Terim	Tanım/Açıklama
BGYS	Bilgi Güvenliği Yönetim Sistemi
Kurum	Gençlik ve Spor Bakanlığı Bilgi İşlem Dairesi Başkanlığı

4. UYGULAMA

4.1. Kullanıcı Tanımlama ve Şifre

- Kullanıcı tanımlanması ve takibinin yapılması kurum bünyesinde yer alan ağ cihazlarına, sistemlere ve uygulamalara erişimin izlenmesi amacını içermektedir.
- Kullanıcı ve şifre tanımlamaları resmi yazı ile ilgili birimlerden talep edilerek oluşturulmaktadır.
- Kullanıcılar için ilave erişim yetkilendirmeleri e-posta ile talep edilmektedir.
- Şifreler ilk verildiğinde benzersiz şifreler verilir ve ilk açıldığında kullanıcı şifre değiştirmeye zorlanır.
- Parolalar, en az 8 karakterden oluşur ve büyük harf, küçük harf, alfa numerik ve rakam özelliklerinin hepsini içerecek şekilde karmaşık olarak belirlenir.
- Parolalar maksimum 90 gün sonra değiştirmeye zorlanır.
- Kullanıcıların parolalarını maksimum 3 kez yanlış girme hakkı vardır. Bu sayıyı aşan kullanıcıların hesapları bir süreliğine donar.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	KULLANICI HESABI YÖNETİMİ PROSEDÜRÜ	Doküman No	BGYS-PR20
		Yayın Tarihi	05.01.2022
		Revizyon Tarihi	
		Revizyon No	00
		Sayfa No	2 / 3

- Tüm kullanıcılar ağ, sistem veya uygulamalara erişimde bilginin transfer edilmesi, alınması ve saklanması işlemlerinde kendilerine özel kullanıcı bilgilerini kullanacaklardır.
- Ağ cihazlarına, sisteme veya uygulamalara erişim taleplerinde daha önce tanımlanan kullanıcı adı ve güvenli bir şifre ile bağlantı sağlanacaktır.
- Şifre oluşturma, Parola Politikası bölümündeki kriterleri karşılayacaktır.
- Başkasına ait kullanıcı ve şifrelerin kullanılmasına izin vermemelidir.
- Kullanıcı bilgileri dokümantasyon edilmemeli, yazılı olmamalı veya benzeri bir güvensiz tutum içinde bulundurulmamalıdır.

4.2. Otomatik Oturum Kapatma

- Yüksek riskli sınıfındaki sunucular, istemci bilgisayarlar ve diğer bilgisayar sistemleri otomatik oturum kapatma veya hareketsiz bekleme modunda çalışmalıdırlar. Söz konusu sistemler hareketsiz halde maksimum 15 dakika kaldığında otomatik olarak oturuma son vermelidir.
- Düşük riskli sınıfındaki sunucular, istemci bilgisayarlar ve diğer bilgisayar sistemleri otomatik oturum kapatma ve hareketsiz bekleme modunda çalışmalıdırlar (Örneğin, şifre korumalı ekran koruyucu). Söz konusu sistemler hareketsiz halde 15 dakika kaldığında otomatik olarak oturumu engellenmelidir.
- Otomatik oturum kapatma veya hareketsiz bekleme süresi belirtilmemiş ancak bu tür bir modda çalışması gereken bir sistem olması durumunda aşağıda belirtilen prosedürlerden herhangi biri uygulanmalıdır:
 - a) Sistem otomatik oturum kapatma veya hareketsiz bekleme moduna yükseltmeli veya taşınmalıdır.
 - b) Sistem güvenli bir ortama taşınmalıdır.
 - c) Mevcut sistemdeki tüm veriler silinmeli ve otomatik oturum kapatma veya hareketsiz bekleme modu olan yeni bir sisteme taşınmalıdır.
 - d) Sunucu, istemci bilgisayarı veya diğer sistemlerden ayrılırken kilitlenmeli veya otomatik kapatma modu aktif hale getirilmelidir (CTRL + ALT + DELETE 'e basılmalı ve kilitlenmeli).

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	KULLANICI HESABI YÖNETİMİ PROSEDÜRÜ	Doküman No	BGYS-PR20
		Yayın Tarihi	05.01.2022
		Revizyon Tarihi	
		Revizyon No	00
		Sayfa No	3 / 3

4.3. Güvenlik Duvarı Kullanımı

Güvenlik duvarı yapılandırmalarının aşağıda belirtilen minimum gereksinimleri karşılaması gerekir:

- Ağa erişimi sadece yetkili kurum çalışanları ve onların birimleri ile sınırlandırılmalıdır.
- Konsol veya diğer yönetim portları uygun şekilde güvenli hale getirilmiş ve kapalı olmalıdır.
- Hatalı erişim denemelerini kayıt altına alacak mekanizma kurulmalıdır. Fiziksel olarak güvenli bir mekânda korunmalıdır.

5. İLGİLİ DOKÜMANLAR

- BGYS-PL01 BİLGİ GÜVENLİĞİ POLİTİKASI
- TS ISO/IEC 27001:2022 Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi