

**Bursa Teknik Üniversitesi**

Bilgi Güvenliği Yönetim Sistemi

Erişim Kontrol Prosedürü

**İÇİNDEKİLER**

[1. Amaç 2](#_Toc534493691)

[2. Kapsam 2](#_Toc534493692)

[3. Revizyon Kayıtları 2](#_Toc534493693)

[4. Tanımlamalar ve Kısaltmalar 2](#_Toc534493694)

[5. Uygulama 2](#_Toc534493695)

[5.1. Ağ ve Ağ Hizmetlerine Erişim 2](#_Toc534493696)

[5.2. Kullanıcı Erişim Yönetimi 3](#_Toc534493697)

[5.2.1. Kullanıcı Kaydetme ve Kayıt Silme 3](#_Toc534493698)

[5.2.2. Kullanıcı Erişimine İzin Verme 3](#_Toc534493699)

[5.2.3. Ayrıcalıklı Hakların Yönetimi 3](#_Toc534493700)

[5.2.4. Kullanıcılara Ait Gizli Kimlik Doğrulama Bilgilerinin Yönetimi 4](#_Toc534493701)

[5.2.5. Erişim Haklarının Gözden Geçirilmesi, Düzenlenmesi veya Kaldırılması 4](#_Toc534493702)

[5.3. Kullanıcı Sorumlulukları 4](#_Toc534493703)

[5.3.1. Gizli Kimlik Doğrulama Bilgisinin Kullanımı 4](#_Toc534493705)

[5.4. Bilgiye Erişimin Kısıtlanması 4](#_Toc534493706)

[5.5. Güvenli Oturum Açma 5](#_Toc534493707)

[5.6. Parola Yönetim Sistemi 5](#_Toc534493708)

[5.7. Ayrıcalıklı Destek Programlarının Kullanımı 6](#_Toc534493709)

[5.8. Program Kaynak Koduna Erişim 6](#_Toc534493710)

[6. İlgili Dokümanlar 6](#_Toc534493711)

[6.1. İç Kaynaklı Dokümanlar 6](#_Toc534493712)

[6.2. Dış Kaynaklı Dokümanlar 6](#_Toc534493713)

# Amaç

Bu dokümanın amacı, BGYS Kapsam Analizi Dokümanında belirtilen birimlerdeki varlıkların erişim kontrollerinde uyulması gereken kuralları belirlemektir.

# Kapsam

Bu doküman, Kapsam Analizi Dokümanında belirtilen birimlerde belirlenecek tüm erişim kontrollerini kapsar.

# Revizyon Kayıtları

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Revizyon No** | **Tarih** | **Revizyon Nedeni** | **Revizyon Sayfa No** | **Revize Edilen Bölüm** |
| 01 | 20.02.2019 | Erişim haklarının gözden geçirilmesi kısmı güncellendi | 4 | 5.2.5. |
| 02 | 21.11.2019 | Parola Yönetim Sistemi kısmı güncellendi | 5 | 5.6. |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Tanımlamalar ve Kısaltmalar

Bu dokümandaki kısaltma ve tanımlar, Kısaltmalar ve Tanımlar Kılavuzunda açıklanmaktadır.

# Uygulama

## Ağ ve Ağ Hizmetlerine Erişim

1. Ağlar hizmet verdikleri servislere göre ayrılır ve yetki gruplarına göre erişim tanımlanır,
2. Ağlar arası iletişimde ihtiyaç duyulan servislere göre erişim tanımlanır,
3. Ağlar ve bu ağlarda hizmet veren servislerde ihtiyaç dışı erişim servisleri kapatılır,
4. Ağlara ve ağ hizmeti veren sistemlere erişim için yetki kontrolü kimlik doğrulaması ile gerçekleştirilir,
5. Ağ ve ağ cihazlarına erişimdeki anomalileri belirlemek ve yasal gereksinimleri karşılamak için iz kayıtları saklanır,
6. Ağ güvenliğine ilişkin kontroller Ağ Güvenliği Prosedürü ve Uzaktan Erişim ve Çalışma Prosedürüne uygun olarak gerçekleştirilir.

## Kullanıcı Erişim Yönetimi

Kurum bünyesindeki tüm kurumsal uygulama ve bilgi sistemlerine yetkisiz erişimleri önlemek için belli erişim kontrolleri uygulanmaktadır. Bu uygulama ve bilgi sistemlerine erişim yetkileri her bir kullanıcı için ayrı belirlenir. Bu yetkiler;

1. Personelin sorumlulukları ile orantılı,
2. Başka kullanıcılar ile paylaşılmamış tek bir kullanıcı adına ait,
3. Bu kullanıcı adı farklı tek bir parolaya sahip olmalıdır.

Yetkisiz herhangi bir değişiklik yapılmadığından ve erişim süresi bitmiş dış kullanıcıların kaydının kaldırıldığından emin olabilmek için BGYS yöneticisi kullanıcı erişim yetkilerini personel listesi ile Erişim Listesi’ni karşılaştırarak altı ayda bir gözden geçirir.

### Kullanıcı Kaydetme ve Kayıt Silme

1. Kullanıcı erişim talepleri, Bilgi İşlem Dairesi Başkanlığı’na resmi yazı ile bildirilir.
2. Üçüncü Taraflar için oluşturulacak kullanıcı hesapları sözleşme sürelerine ve şartlarına göre oluşturulur. Üçüncü taraf kullanıcı erişimleri, talep resmi yazı ile Bilgi İşlem Dairesi Başkanlığı’na iletildiğinde tanımlanır.
3. Her kullanıcı için bir hesap oluşturulur.
4. Kullanıcıların kendilerine tahsis edilen kullanıcı hesap bilgileri ile bilişim sistemleri kullanımı esnasındaki sorumluluklarının farkında olunmasını sağlamak için kullanıcılara, Kurumsal Kullanıcı Taahhütnamesi imzalatılarak, Üçüncü Taraflar için ise Üçüncü Taraf Personeli Gizlilik Sözleşmesi İmzalatılarak Bilgi İşlem Dairesi Başkanlığı’na iletilir.
5. Kurumda göreve yeni başlayanlar, kurumdan ayrılanlar ve birim değişiklikleri, İnsan Kaynakları Güvenliği Prosedürüne göre Bilgi İşlem Dairesi Başkanlığı’na iletildikten sonra en kısa sürede erişim yetkileri düzenlenir.
6. Kurumdan ayrılan ya da ilişiği kesilen kullanıcılarının hesapları, yetkileri düşürülerek ve pasif hale getirilerek ayrı bir OU içerisinde saklanır.

### Kullanıcı Erişimine İzin Verme

1. Kullanıcılara standart kullanıcı haricinde verilen izinler “Yetki Talep Formu” ile bildirilir.
2. Kullanıcılara verilen yetkilerde görevlerin ayrılığı ilkesi göz önünde bulundurulur.
3. Kullanıcılara atanacak tüm yetkiler düzenlenmeden hesap aktif edilmez.

### Ayrıcalıklı Hakların Yönetimi

1. Kullanıcılara standart kullanıcı haricinde verilen izinler “Yetki Talep Formu” ile bildirilir.
2. Ayrıcalıklı erişim hakları için gerekli süreler tanımlanır.
3. Ayrıcalıklı erişim haklarının iz kayıtları öncelikli incelenir.
4. Ayrıcalıklı erişim hakları tanımlanırken ihtiyacı kadar ilkesi göz önünde bulundurulur.
5. Sistem ve ağ yönetimi için kullanılacak ayrıcalıklı erişim hakları için ayrı bir hesap tanımlanır.
6. Sistem yapılandırma yetenekleri olan kullanıcı parolaları çok gizli bilgi şartlarına uygun olarak saklanır.

### Kullanıcılara Ait Gizli Kimlik Doğrulama Bilgilerinin Yönetimi

1. Parolalar Parola Politikasına göre belirlenir.
2. Kullanıcılara parolaları yüz yüze bildirilir ve değiştirmeleri gerektiği söylenir.
3. Kullanıcıların ilk oturum açtıklarında parolalarını değiştirmesi zorunludur.
4. Her kullanıcı için farklı geçici parola oluşturulur.
5. Parola değiştirme, kullanıcı kendi isteğiyle parola ayarlarından belirleyebilir. Ayrıca herhangi bir sorun olduğunda Aktif Dizinde değiştirme yöntemi kullanılır.

### Erişim Haklarının Gözden Geçirilmesi, Düzenlenmesi veya Kaldırılması

1. Aktif dizinde kullanıcı yetkileri sistem yöneticisi tarafından en az altı ayda bir olmak üzere periyodik olarak gözden geçirilir.
2. Ayrıcalıklı kullanıcı yetkileri sistem yöneticisi tarafından en az ayda bir gözden geçirilir ve kullanılmayan hesapların veya ayrıcalık süresi dolmuş hesapların yetkileri düşürülür.

## Kullanıcı Sorumlulukları



### Gizli Kimlik Doğrulama Bilgisinin Kullanımı

1. Erişim bilgileri kurum içi ya da kurum dışı paylaşılmaz.
2. Erişim bilgileri başkalarının erişebileceği alanlarda saklanmaz.
3. Erişim bilgilerinin ifşa olması ya da olma ihtimalinin doğması durumunda değişiklik yapılır ve ihlal olayı bildirilir.
4. Gizli kimlik bilgilerinin uygulamalar tarafından hatırlanmaması sağlanır.
5. Kurumsal erişim bilgileri kurum dışı erişimler için kullanılmaz. (özel e-posta hesabı, sosyal medya hesapları)
6. Kullanıcı, erişim bilgilerinin kullanımını devretmez.

## Bilgiye Erişimin Kısıtlanması

1. Erişim izinlerinde kullanıcıya tanımlanması gerekenden daha fazla erişim izni tanımlanmaz.
2. Uygulama erişiminde sadece ilgili menüler erişime açılır.
3. Hangi verinin hangi kullanıcı için olduğu belirlenir.
4. Kullanıcıların erişim haklarını okuma, yazma, silme ve yönetme gibi yetkiler olarak düzenlenir.
5. Diğer uygulamaların veriye erişim yetkileri göz önünde bulundurularak erişim yetkisi tanımlanır.
6. Çıktı olamayacak ya da kurum dışına çıkmayacak veriler belirlenir ve engellenir.

## Güvenli Oturum Açma

1. Oturum açma işlemleri sırasında yetkisiz kullanıcılara yol göstermemesi amacıyla yardım mesajları yayınlanmaz.
2. Hatalı bir giriş yapıldıysa hangi verinin hatalı olduğu belirtilmez.
3. Başarısız oturum açma girişimleri günlük kayıtlarında yer alması sağlanır. Özel bir yetkilendirme yapılmadıkça, daha sonraki oturum açma girişimlerinin engellenmesi veya belli bir süre ile kullanıcı hesabının bloke edilmesi sağlanır.
4. Oturum açma işlemi için izin verilen minimum ve maksimum süreler tanımlanır ve bu süre aşıldığında oturum açma istemi sonlandırılır.
5. Uygulamaların çalışmalarına uygun bağlantı zaman aşımı süreleri belirlenir.
6. Parola girilirken ekranda karakterler görüntülenmez.
7. Zaman aşımı süresi, bilginin kritikliği, uygulama özellikleri ve kullanıcı terminalinin taşıdığı risklerin derecesine uygun olarak belirlenir.
8. Kimlik bilgileri iletimi şifreli olarak gerçekleştirilir.
9. Kritik uygulamalar için bağlantı süreleri ve sayıları kısıtlanır.
10. Oturum açma için istemci zorunluluğu uygulayabiliriz.

## Parola Yönetim Sistemi

Kurumda kimlik doğrulama gerçekleştirilen her ortamda aşağıdaki parola politikası gereksinimleri göz önünde bulundurulur;

1. Parolalar aşağıdaki özelliklere uygun olmalıdır.
   1. Kullanıcı parolaları en az 8 karakterlidir, büyük harf, küçük harf, noktalama işareti ve rakam özelliklerinden en az üçünü içeren karmaşık parolalar belirlenir.
   2. Son kullanılan 3 parola yeni parola olarak belirlenmez.
   3. Parolalar 180 gün süreyle geçerlidir.
   4. 3 kez üst üste hatalı girişten sonra hesap 15 dakika kilitlenir.
2. Parolalar çalışanların, herkes tarafından bilinen ya da kolay tahmin edilebilecek kişisel veya ailevi bilgilerinden oluşmaz.
3. Oturum kapatma süresi 15 dakikadır.
4. Varsayılan parolalar kullanılmaz.

## Ayrıcalıklı Destek Programlarının Kullanımı

Sistem ve uygulama kontrollerini geçersiz kılma yeteneğine sahip olabilecek yardımcı programların kullanımı için aşağıdaki kurallar dikkate alınır;

1. Ayrıcalıklı destek programları kullanım yetkisi, Bilişim Teknolojileri Müdürlüğü onayı ile tahsis edilir.
2. Ayrıcalıklı destek programların erişimi için kimlik doğrulama ve yetkilendirme gereksinimlerinin karşılanması sağlanır.
3. Erişim yetkileri kayıt altına alınır.
4. Ayrıcalıklı destek programların işlem kayıtları tutulur ve saklanır.
5. Ayrıcalıklı destek programlarının sistemde kalma süreleri sınırlandırılır.
6. Kullanım ihtiyacı sonlanan programlar sistemden kaldırılır.

## Program Kaynak Koduna Erişim

Program kaynak kodlarının alınması ve saklanması şartnamelerde belirtilir. Alınan kaynak koduna erişimlerin kısıtlanması için en az aşağıdaki adımlar göz önünde bulundurulur;

1. Kaynak kütüphanesi işletim sistemi üzerinde tutulmaz.
2. Personelinin kaynak kütüphanelerine erişimi ihtiyaçlara göre sınırlandırılır.
3. Program kaynak kütüphanesine erişimler, Bilgi İşlem Dairesi Başkanlığı’ndan onay alınmadan yapılmaz.
4. Program kaynak kütüphanesi ile ilgili değişiklikler için günlük kayıtlar tutulur ve saklanır.
5. Değişiklikler öncesi kaynak kütüphanelerinin tüm sürümleri saklanır.

# İlgili Dokümanlar

## İç Kaynaklı Dokümanlar

1. Kapsam Analizi Dokümanı
2. Kısaltmalar ve Tanımlar Kılavuzu
3. Erişim Listesi
4. Fiziksel Güvenlik Prosedürü
5. Ağ Güvenliği Prosedürü
6. Uzaktan Erişim ve Çalışma Prosedürü
7. Kurumsal Kullanıcı Taahhütnamesi
8. Üçüncü Taraf Personeli Gizlilik Sözleşmesi

## Dış Kaynaklı Dokümanlar

1. TS EN ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı