# AMAÇ

Bu politikanın amacı üniversitemizde;

* Bilgi ve bilgi işleme olanaklarına erişim kontrolü,
* Yetkili kullanıcı erişimini temin etmek ve sistem ve hizmetlere yetkisiz erişimi engelleme,
* Kullanıcıları kendi kimlik doğrulama bilgilerinin korunması konusunda sorumlu tutma,
* Sistem ve uygulamalara yetkisiz erişimi engelleme hususlarında gerekli faaliyetleri belirlemektir.

# KAPSAM

Bu politika, Yıldız Teknik Üniversitesi’nde Bilgi Güvenliği Yönetim Sistemi içinde yer alan tüm dokümanları ve çalışmaları kapsar.

# TANIMLAR

**Bilgi güvenliği:** Bilginin gizliliği, bütünlüğü ve kullanılabilirliğinin korunması. Ek olarak, doğruluk, açıklanabilirlik, inkâr edememe ve güvenilirlik gibi diğer özellikleri de kapsar.

**Bilgi güvenliği yönetim sistemi:** Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için, iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçası.

# SORUMLULUKLAR

Bu prosedürün hazırlanması ve yönetiminden BGYS Ekibi sorumludur.

# UYGULAMA

# Ağ ve Ağ Hizmetlerine Erişim

Kullanıcılara sadece özellikle kullanımı için yetkilendirildikleri ağ ve ağ hizmetlerine erişim verilmelidir. Bu kapsamda:

* Bilgi İşlem Daire Başkanlığı’nda bulunan ağlar birbirinden bağımsız olarak çalışmaktadır. Misafirler için Daire Başkanlığı bünyesinde güvenlik amacıyla ağ erişim izni verilmemektedir.
* Kullanıcıların erişim cihazları üzerinden ağa bağlanabilmeleri için, Kurum kullanıcı adı ve parolası bilgilerini etki alanı adı ile beraber girmeleri sağlanmalı ve Kurum kullanıcısı olmayan kişilerin, kablosuz ağa yetkisiz erişimi engellenmelidir.
* Erişim cihazları üzerinden gelen kullanıcıların ağ kaynaklarına erişim yetkileri, internet üzerinden gelen kullanıcıların yetkileri ile sınırlı olmalıdır.
* Kablosuz ağa dahil olan kurum çalışanları için bile erişimler sınırlandırılmalıdır.
* Sadece internete çıkacak olan kullanıcıların kablosuz ağ üzerinden diğer uygulamaların (ses, güvenlik, mobilite vb) çalıştığı networklere erişimi engellenmeli gerekirse networkler farklı IP aralıkları üzerinde ayarlanmalı, cihaz üzerinde Access Control Listler (Yetki kuralları) oluşturulmalıdır.

# Kullanıcı Erişim Yönetimi

# Kullanıcı Kaydetme ve Kayıt Silme

* Kurumsal sistem kaynakları kullanımı (kütüphane, yazılım servisi, kablosuz erişim vs) AD üzerinden sağlanmaktadır.
* AD servisi üzerine kayıt yapılması
	+ Personel -İşe ilk başlayan personel kurum sicil kaydını tamamladıktan sonra teknikdestek.yildiz.edu.tr üzerinden erişim yetkisi talep etmektedir.
	+ Öğrenci – öğrenci kaydı tamamlandıktan sonra OBS ( öğrenci bilgi sistemi) üzerinden alınan kayıtlarla toplu olarak kayıt edilmektedir.
* Kullanıcı İsmi belirlenmesi
	+ Personel - Tüm personelin kullanıcı adları ad.soyad birleşik ve ismin ilk harfi ve soyadı olacak şekilde oluşturulmaktadır. Mail adresleri ise ad.soyad@yildiz.edu.tr olarak verilmektedir. Teknikdestek.yildiz.edu.tr destek talebine cevaben iletilmektedir.
	+ Öğrenci- kullanıcı adları öğrencilik numaralarına göre verilmektedir. OBS kayıtlarındaki kişisel eposta adreslerine iletilmektedir.
* Tüm kullanıcılar AD OU(organisyon gruplarına göre) kayıt edilmektedir. Kullanıcı açma işlemleri manuel server üzerinden bat dosyası ile oluşturulmaktadır.
* Kullanıcı kullanıcı şifresini adservise kanalı üzerinden değiştirebilmektedir. Şifre ile ilgili sorun yaşaması durumunda teknikdestek.yildiz.edu.tr üzerinden talep ederek gerekli işlemlerini yapabilmektedir.
* İşten ayrılan personel, adli sicil gibi durumlardaki personel daire başkanlığı tarafından EBYS üzerinden resmi bilgiler doğrultusunda AD servisinde pasif hale getirilerek bağlantı sonlandırılır. Öğrenciler mezuniyet tarihinden sonra OBS sistemi üzerinden alınan bilgiler doğrultusunda toplu olarak kullanıcı işlemleri pasif hale getirilmektedir.
* Bilgi İşlem Daire Başkanlığı, işten ayrılan kişinin kullanıcı hesabını 1 hafta içinde kullanıma kapatır. Şifreler geçersiz hale gelmiş olur ve söz konusu çalışanın bilgi sistemlerine erişimi engellenir.
* Bilgi güvenliği açısından İşten ayrılan personelin şirkete ait gizliliği olan önem derecesi yüksek verileri herhangi biçimde farklı veya dış bir alana transfer etmemesine yönelik kontrollerin yapılması esastır.
* İşten ayrılan personelin üzerinde bulunan bilgi varlıkları zimmetinden düşülür.

# Kullanıcı Erişimine İzin Verme

Tüm kullanıcıların AD servisi üzerinde OU guruplarına göre erişim tanımlamarı (rolleri) mevcuttur. Örnek Kütüphane . tüm kullanıcılara açıktır.

Kurum içi sistemler(programlar) AD servisine bağlıdır. İlgili programa bağlanacak personel ilgili programın moderatörü tarafından yetki tanımlaması yapılması gerekmektedir. Örnel EBYS üzerinde yazışma yapacak personel EBYS yetki tanımlamasına göre programın içerisine moderatör tarafından tanımlanır ve AD servisi kullanıcı adı ve parolasıyla erişimi sağlanmış olur. \*\*\*Yetki tanımlamaları kurum tarafından verilmektedir. Ve kulalanıcı loğları ilgşli program tarafından tutulmaktadır.

# Ayrıcalıklı Erişim Hakları

* Standart erişim haricindeki erişimler ayrıcalıklı erişim haklarıdır.
* Kullanıcılara standart kullanıcı haricinde verilen izinler , ilgili sistemlerin moderatörü tarafından yetkilendirimektedir. Örnek EBYS sistemi kullanacak personel EBYS moderatörü ve personeln birimi tarafından yetkilendirilir.
* Erişim hakları tanımlanırken ihtiyacı kadar ilkesi göz önünde bulundurulur. İlkeler ve yetki tanımları program içerisinde tanımlanmıştır. Örnek EBYS standart yazışma ilkesine sahip kullanıcı gizli evraklar üzerinde görme ve yazışma yapamaz.
* Düzenli olarak kullanılacak ayrıcalıklı erişim hakları için ortak hesap kullanılmaz. Tüm kullanıcılar AD servisi üzerinden kendi hesaplarıyla erişim sağlayabilirler.

# Gizli Kimlik Doğrulama Bilgilerinin Yönetimi

* Kullanıcıların gizli kimlik doğrulama bilgisi kullanıcı adı ve paroladır.
* Kullanıcıların hesap bilgileri yönetimi “Parola Politikası” dokümanında tanımlandığı şekilde yapılır.
* Oluşturulan kullanıcı hesap bilgileri, kullanıcılara gereken gizlilik kurallarına dikkat edilerek bildirilir.
* Kaybedilen veya unutulan kullanıcı hesap bilgilerinin bildiriminde, kullanıcıya yeni geçici parola verilir. Güvenlik şüphesi uyandıran durum varsa bilgi güvenliği ihlal olay kaydı oluşturulur.

# Erişim Haklarının Kaldırılması veya Düzenlenmesi

* Tüm çalışanların ve dış taraf kullanıcılarının bilgi ve bilgi işleme olanaklarına erişim yetkileri, istihdamları, sözleşmeleri veya anlaşmaları sona erdirildiğinde kaldırılır. Değişiklikler olması durumunda erişim yetkileri incelenerek düzenlenir.

# Kullanıcı Sorumlulukları

* Kullanıcı sorumluluğu
	+ Sözleşmeli personel - “Personel Gizlilik Taahhütnamesi”nde belirtilmiştir.
	+ Akademik, idari ve öğrenci ilgili mevzuatlara tabidir.
* Tüm kimlik bilgilerinin yönetimi “Parola Politikası”na uygun olarak yapılır.
* Kullanıcı hesap bilgilerinin uygulamalar tarafından hatırlanmaması sağlanır.

# Sistem ve Uygulama Erişim Kontrolü

# Bilgiye Erişimin Kısıtlanması

* Erişim izinlerinde kullanıcıya, standart yetkilerin dışında daha fazla erişim yetkisi tanımlanmaz.
* Kullanıcılara standart kullanıcı haricinde verilen izinler ilgili programlar tarafından takip edilir.
* Kullanıcılara verilen yetkilerde görevlerin ayrılığı ve ihtiyacı kadar ilkesi göz önünde bulundurulur.
* Kullanıcılara atanacak yetkiler düzenlenmeden hesap aktif edilmez.
* Kullanıcı adı ve parola kullanımı olmadan uygulamalara erişim sağlanmaz.
* Kullanıcıların uygulamalara erişiminde sadece kullanacağı menülere erişim verilir.
* Hangi verinin hangi kullanıcı ya da kullanıcı grubu erişimi için olduğu belirlenir.
* Kullanıcılara verilecek erişim hakları okuma, değiştirme ve yönetme gibi yetkiler olarak belirlenir.

# Güvenli Oturum Açma Ve Parola Yönetimi

* Oturum açma işlemleri sırasında, yetkisiz kullanıcılara yol göstermemesi amacıyla yardım mesajları yayınlanmaz. Hatalı bir giriş yapıldıysa hangi verinin hatalı olduğu belirtilmez.
* Oturum açma işlemleri “Parola Politikası”nda belirtildiği şekilde yapılır.
* Tanımlanan bir hareketsizlik süresi sonunda aktif olmayan oturumlar sonlandırılır. Hareketsizlik süresi, bilginin kritikliği, uygulama özellikleri ve istemcinin taşıdığı risklerin derecesine göre belirlenir.
* Tüm bilişim sistemlerine ya da uygulamalara parola girilirken ekranda karakterlerin görüntülenmemesi sağlanır.
* Kullanıcılar tarafından kullanılan parolalar “Parola Politikası”na uygun olarak tanımlanır.

# Ayrıcalıklı Destek Programlarının Kullanımı

* Kullanıcıların yürütmekte olduğu iş ve işlemlerin gereği olarak yardımcı programların kullanımı için aşağıdaki kurallar dikkate alınır:
* Ayrıcalıklı destek programlarının erişim talebi ihtiyaç olduğu durumlarda ilgili birim sorumlusunun bilgisi dâhilinde paylaşılan bir bağlantı linki üzerinden gerçekleştirilir.
* Ayrıcalıklı destek programları erişim yetkisi süreli olarak açılır.
* Ayrıcalıklı destek programlarının erişimi için kimlik doğrulama ve yetkilendirme kriterlerine dikkat edilmesi sağlanır.
* Gerekli olmayan ayrıcalıklı destek programları sistemlerden kaldırılır.

# Program Kaynak Koduna Erişim Kontrolü

* Geliştirilen bütün yazılımların kaynak kodları GİT üzerinden saklanır.
* Yazılım Geliştirme Birimleri yaptıkları geliştirmeyi GİT deposuna aktarmak ile sorumludur.
* GİT üzerinde Yazılım Geliştirme Birimi personellerinin yetkisi vardır. GİT hesapları yazılım birimleri üzerinden kontrol edilerek kullanıcı kimliğinin kontrol edilmesi sağlanır.
* GİT sisteminde yeni bir kullanıcı açılması ygun şekilde onay mekanizmalarından geçerek gerçekleştirilir.
* Sadece bu GİT deposunda bulunan kodlar canlı ortama taşınabilir. Devreye alma sırasında GİT kaynak olarak kullanılır, diğer dışarıdaki kodlar devreye alınamaz.
* Program kaynak kodunun ve kütüphanelerinin alınması ve saklanması şartnamelerde belirtilir. Alınan kaynak koduna erişimlerin kısıtlanması için en az aşağıdaki adımlar göz önünde bulundurulmalıdır:
	+ Kaynak kod ve kütüphaneler canlı uygulama ortamında tutulmaz.
	+ Personelin, kaynak kod ve kütüphanelerine erişimi ihtiyaçlara göre sınırlandırılır.
	+ Program kaynak kod ve kütüphanelerine erişim, Yazılım Geliştirme Birimi yöneticisinden onay alınmadan yapılamaz.
	+ Program kaynak kod ve kütüphanesi ile ilgili değişiklikler için olay kayıtları tutulur ve saklanır.
	+ Değişiklikler öncesi kaynak kod ve kütüphanelerin tüm sürümleri GİT üzerinde saklanır.

# Uzaktan Erişimler

* Kurum içerisindeki sunucuların erişimi sadece BİDB ‘ye aittir. Sunucular üzerinde bağlantı için IP izni gereklidir. VPN erişim izinleri [www.teknikdestek.yildiz.edu.tr](http://www.teknikdestek.yildiz.edu.tr) üzerinden destek talebi ile yapılmaktadır. Gizlilik taahhütnamesi imzalayan firmaların uzaktan erişimi firewall üzerinden verilmektedir.
* Kuruluş çalışanları hiçbir şekilde kendilerinin login ve e-posta şifrelerini aile bireyleri dahil olmak üzere hiç kimseye vermemelidir.
* Çalışanlar kuruluş ile ilgili çalışmalarında kuruluşun dışındaki e-posta hesaplarını kullanmamalıdır.
* Kuruluş ağına standart dışı erişim isteğinde bulunan organizasyon veya kişiler birimin özel izni ile belirlenen IPler üzerinden geçici olarak izin verilebilirler.
* İşten ayrılan kullanıcı hesapları ilişiği kesildikten hemen sonra kaldırılmalıdır. Kurumdan ilişiği kesilmiş veya görevi değişmiş kullanıcıların gerekli bilgileri yürütülen projeler üzerinden otomatik olarak alınmalı, yetkiler ve hesap özellikleri buna göre güncellenmelidir.
* Kurumun bilgilerine ulaşabilen tüm kuruluşlar ile Tedarikçi Gizlilik Taahhütnamesi imzalanmaktadır.
* Uzaktan erişim güvenliği sıkı şekilde denetlenmelidir. Kontrol tek yönlü şifreleme (one-time password authentication, örnek; Token Device) veya güçlü bir passphrase (uzun şifre) destekli public/private key sistemi kullanılması tavsiye edilmelidir.
* Kurum çalışanları bağlantı bilgilerini hiç kimse ile paylaşmamalıdır. İhlal durumunda “PR-033-Bilgi Güvenliği İhlal Olayları ve Disiplin Soruşturması Prosedürü” uygulanır.
* Kurumun ağına uzaktan bağlantı yetkisi Proxy yetkilendirmeleri üzerinden ve sabit IP üzerinden verilmektedir. Güvenlik tedbirleri gereğince güvenli olmayan ağlardan bağlantı durumunda kullanıcılar sorumludurlar.
* Kurum ağına uzaktan erişecek bilgisayarların işletim sistemi ve anti virüs yazılımı güncellemeleri yapılmış olmalıdır.
* Uzak erişim için kullanılacak olan servisler kuruma ait IP adresleri ile yapılmalıdır.
* Uzak erişim bağlantısında boşta kalma süresi (Herhangi bir işlem yapılmadığı takdirde connection time out süresi) kısa tutulmalıdır. Gereksiz bağlantı sürelerinden kaçınılmalıdır.

# Fiziksel Erişimler

* Fiziksel erişimler için kullanılan giriş kontrol önlemleri Bilgi Güvenliği Yönetim Sistemi Fiziksel ve Çevresel Güvenlik Uygulamaları Talimatı içerisinde tanımlanmıştır. .

# Üçüncü Taraf Erişim Kontrolü

* Kuruma dışarıdan erişim sağlayan üçüncü taraf bağlantıları için kurum içerisindeki bir bilgisayar üzerinden ilgili personel eşliğinde bağlantı sağlanmaktadır.
* Üçüncü taraflar için oluşturulan kullanıcı hesaplarına sözleşme gereği dışında yetki verilmez. Yetki verilmesi ihtiyacında ilgili birim yöneticisi onayı ile yetki tanımlanır.
* Üçüncü taraf kurumlar ve personeller için verilecek VPN gibi yetki talepleri teknikdestek.yildiz.edu.tr veya EBYS üzerinden kayıt altına alınır
* Sözleşmesi sona eren üçüncü tarafların hesaplarının kapatılması için erişimi talep eden birim tarafından Bilgi İşlem Daire Başkanlığına teknikdestek.yildiz.edu.tr üzerinden bildirilir ve akabinde hesapları kapatılır ve karşı kullanıcıya destek cevabı gönderilir.

# YAPTIRIM

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 Temsilcisi tarafından e-posta üzerinden yazılı olarak uyarılır. Eğer ihlal işleminin kasıtlı olduğu anlaşılırsa veya kasıtsız olan ihlaller 3’ten fazla tekrar ederse “PR-033-Bilgi Güvenliği İhlal Olayları ve Disiplin Soruşturması Prosedürü” gereğince kişiler hakkında işlem yapılır. Tüm çalışanlar, güvenlik ihlali olaylarını ve bu politikanın ihlallerini, birim amirinin bilgisi dahilinde BGYS Ekibi’ne en kısa sürede bildirme sorumluluğundadır.