MAKÜ

BURDUR MEHMET AKİF ERSOY ÜNİVERSİTESİ

ERİŞİM KONTROL POLİTİKASI

İçindekiler

1. Amaç

Bu doküman, "BGYS Kapsam Analizi Dokümanı"nda belirtilen, kuruluşumuz birimlerindeki bilgi ve bilgi işleme olanaklarına erişim için dikkat edilmesi gereken hususları belirlemek amacıyla oluşturulmuştur.

2. Kapsam

Bu doküman, "BGYS Kapsam Analizi Dokümanı"nda belirtilen, kuruluşumuz birimlerindeki tüm erişim yetkilerini kapsar.

3. Sorumluluk

Rol/Unvan / Görev	Üst Yönetim	Üst Yönetim Temsilcisi	BGYS Yöneticisi	BGYS Ekip Üyeleri	Diğer Çalışanlar
Dokümanın Hazırlanması			X	X	
Dokümanın Kontrolü			X	X	
Dokümanın Onaylanması	X	X			
Dokümanın Yayınlanması			X		
Dokümanın Güncellenmesi			X		
Dokümanın Uygulanması	X	X	X	X	X
Dokümanın Uygulamadan Kaldırılması	X	X			

4. Tanımlamalar ve Kısaltmalar

Terim	Tanım/Açıklama
Ayrıcalıklı Destek Programları	Sistem ve uygulamaların kontrollerini geçersiz kılma kabiliyetine sahip olabilen destek programları (Uzaktan destek programları vb.)
BGYS	Bilgi Güvenliği Yönetim Sistemi
Fiziksel Erişim	Bir mülke, binaya veya odaya fiziksel olarak yapılan erişimleri ifade eder
Kurum	Kuruluşumuzun Kapsam Analizi Dokümanı'nda belirtilen birimleri

Terim	Tanım/Açıklama
Politika	Bir şirket, kurum veya kişinin görüş, felsefe, amaç ve tutumunun belirli şekilde ifadesini, bu görüş, felsefe veya amaç doğrultusunda bir hareket planını içeren doküman tipidir.
Mantıksal Erişim	Donanım üzerindeki bir bilgi varlığına bilgisayar veya benzeri araçlarla uzaktan yapılan erişimleri ifade eder.
OrganizationalUnit (OU)	Bir aktif dizin alanı içerisindeki objeleri organize etmek amacıyla oluşturulmuş yapıdır. OU içerisinde kullanıcılar, gruplar, bilgisayarlar veya başka OU'lar olmak üzere başka objeler barındırılabilir.

5. Erişim Kontrol Politikası

Bilgi güvenliğini sağlamanın en temel yolu, bilgi varlığına yetkisiz kişilerin erişimlerini engellemek ve yetkisi olan kişilerin erişimlerini de ihtiyaca göre kısıtlamaktır. Bu erişimler, fiziksel ve mantıksal erişim olarak iki şekilde gerçekleşebilir. Erişim kontrollerinde yasal gereksinimler göz önünde bulundurulur, veri sızıntısı ve yetkisiz erişimlerin önüne geçmek için "Varlık Yönetimi Prosedürü"nde belirtilen varlık sınıflandırmasına uygun yetkilendirmeler yapılır. Her bir erişim için mutlaka Kurum tarafından belirlenmiş erişim yetkilendirme yöntemleri kullanılır. BGYS Ekip Üyeleri erişimlerin takibi ve kontrolünü yapar, değişikliklerle ilgili BGYS Yöneticisini bilgilendirir. Erişim kontrolleri yapılırken "BGYS Roller ve Sorumluluklar Kılavuzu"nda yer alan Görevler Ayrılığı ilkesi başlığı dikkate alınır. Kullanıcı kimlik bilgileri ve gizli kimlik doğrulama bilgileri kullanımı, kullanıcı erişim haklarının verilmesi ve kaldırılması, ayrıcalıklı erişim rollerinin kullanımı bu doküman ile açıklanmıştır.

5.1. Fiziksel Erişim Kontrolü

Fiziksel erişim için uygulanacak yöntemler "Fiziksel Güvenlik Prosedürü" dokümanında tanımlanmıştır. Erişim yetkileri "Erişim Yetki Matrisi" dokümanında takip ve kontrol edilir.

5.2. Mantıksal Erişim Kontrolü

Sistemlere erişim yetkileri "Erişim Yetki Matrisi" dokümanı ile takip ve kontrol edilir. Mantıksal erişim kontrolleri uygulanırken uyulacak kurallar, "Ağ Güvenliği Yönetimi Prosedürü" ve "Uzaktan Erişim ve Çalışma Politikası" göz önünde bulundurularak tanımlanır.

5.3. Sunucu ve Sistemlere Erişim Kontrolü

(1) Sunuculara ve sistemlere erişim talepleri "Erişim Talep Formu" ile yapılır.
(2) 'Erişim Talep Formu' üçüncü taraf erişimleri için ıslak imzalı olarak, kurum personeli için ise Erişim Talep Formu doldurularak birim amiri tarafından onaylanmak suretiyle Bilgi İşlem Birimi'ne iletilir.
(3) Sunucu ve sistemlere parola ile erişim esastır. Kullanıcı adı ve parola gönderme yeteneği olmayan sistemler için IP bazında erişim yetkisi verilir.
(4) Sistemlere erişimlerde ortak hesap kullanılmaz.
(5) Kritik sistemlere yapılan tüm erişimlerin olay kayıtları tutulur.
(6) Sistem yöneticileri teknik zorunluluklar haricinde 'Administrator' ve 'root' gibi ön tanımlı yönetici sistem hesaplarını kullanmaz.
(7) Erişim yetkileri verilirken bilmesi gerektiği kadar prensibine göre hareket edilir.
(8) Sistem yöneticisi rolündeki personel, sunucu ve sistemler üzerinde her türlü işlem için tam yetkilidir.
(9) Sunucu ve sistemlere uzaktan erişim gerektiren durumlarda "Uzaktan Erişim ve Çalışma Politikası"ndaki kurallara uyulur.
(10) Sunucu ve sistemlere erişim için kullanılan parolalar "Parola Politikası"na göre belirlenir.

5.4. Kullanıcı Erişim Yönetimi

Yetkili kullanıcı erişimini temin etmek, sistem ve hizmetlere yetkisiz erişimi engellemek için dikkat edilmesi gereken hususlar aşağıda belirtilmiştir.

5.4.1. Kullanıcı Hesaplarının Yönetilmesi

(1) Kullanıcı ve e-posta hesabı açma talepleri ve bilişim sistemleri kullanımı esnasındaki sorumlulukların bildirimi "İnsan Kaynakları Güvenliği Prosedürü"nde belirtildiği şekilde uygulanır.
(2) Kurumla ilişkisi kesilen (ücretsiz izin, geçici yurtiçi veya yurt dışı görevlendirme, askerlik, açığa alınma, işten çıkarılma, emeklilik, istifa vb.) personelin Bilgi İşlem Birimi'ne bildirim tarihi itibariyle hesapları pasif duruma getirilir.

5.4.2. Kullanıcı Erişimine İzin Verme

(1) Kullanıcılara standart kullanıcı haricinde verilen izinler "Erişim Talep Formu" ile talep ve takip edilir.
(2) Kullanıcılara verilen yetkilerde görevlerin ayrılığı ve ihtiyacı kadar ilkesi göz önünde bulundurulur.
(3) Kullanıcılara atanacak yetkiler düzenlenmeden hesap aktif edilmez.

5.4.3. Ayrıcalıklı Erişim Haklarının Yönetimi

(1) Standart erişim haricindeki erişimler ayrıcalıklı erişim haklarıdır.

(2) Kullanıcılara standart kullanıcı haricinde verilen izinler "Erişim Talep Formu" ile talep edilir.
(3) Ayrıcalıklı web sitesi erişimleri "Erişim Talep Formu" ile talep edilir.
(4) Erişim hakları tanımlanırken ihtiyacı kadar ilkesi göz önünde bulundurulur.
(5) Düzenli olarak kullanılacak ayrıcalıklı erişim hakları için ortak hesap kullanılmaz.
(6) Kurum çalışanları için süresiz erişim açılabilirken üçüncü taraflar için sözleşme bitim tarihini aşmamak kaydıyla süreli erişim açılır.
(7) Standart erişim dışındaki internet erişim talepleri "Erişim Talep Formu" ile talep edilir. Ancak bu talepler "İnternet Kullanım Politikası" doğrultusunda değerlendirilir.

5.4.4. Kullanıcılara Ait Gizli Kimlik Doğrulama Bilgilerinin Yönetimi

(1) Kullanıcıların gizli kimlik doğrulama bilgisi kullanıcı adı ve paroladır.
(2) Kullanıcıların hesap bilgileri yönetimi "Parola Politikası" dokümanında tanımlandığı şekilde yapılır.
(3) Oluşturulan kullanıcı hesap bilgileri, kullanıcılara gereken gizlilik kurallarına dikkat edilerek bildirilir.
(4) Kaybedilen veya unutulan kullanıcı hesap bilgilerinin bildiriminde, kullanıcıya yeni geçici parola verilir. Güvenlik şüphesi uyandıran durum varsa bilgi güvenliği ihlal olay kaydı oluşturulur.
(5) Parola değiştirme işlemleri e-mail tarafında kullanıcıların kendisi tarafından yapılır.

5.4.5. Erişim Haklarının Gözden Geçirilmesi, Düzenlenmesi veya Kaldırılması

(1) Hesaplar üzerindeki erişim haklarının gözden geçirilmesi, düzenlenmesi veya kaldırılması "İnsan Kaynakları Güvenliği Prosedürü"ne göre yapılır.
(2) Kullanımı sona eren uygulamaların, yazıcıların e-posta hesapları ve ayarlarının devre dışı bırakılması için erişimi talep eden birim tarafından Bilgi İşlem Birimi'ye bilgi verilir.
(3) Erişim hakları "Erişim Kontrol Listesi"nde belirtilen sürelere göre altı ayda en az bir kez BGYS Yöneticisi tarafından kontrol edilir. Erişim süresi sona eren hesaplar ve/veya erişimleri kapatılır.

5.5. Üçüncü Taraf Erişim Kontrolü

(1) Üçüncü tarafların erişim yetkileri "Erişim Kontrol Listesi"nde takip edilir.
(2) Kuruma dışarıdan erişim sağlayan üçüncü taraf bağlantıları için sorumluluklar "Tedarikçi İlişkilerinde Bilgi Güvenliği Politikası"na göre iletilir.
(3) Üçüncü taraflar için oluşturulan kullanıcı hesaplarına sözleşme gereği dışında yetki verilmez. Yetki verilmesi ihtiyacında ilgili birim yöneticisi onayı ile yetki tanımlanır.
(4) Sözleşmesi sona eren üçüncü tarafların hesaplarının kapatılması için erişimi talep eden birim tarafından Bilgi İşlem Birimi'ne bildirilir ve akabinde hesapları kapatılır.

5.6. Kullanıcı Sorumlulukları

(1) Kullanıcı sorumluluğu "Bilişim Sistemleri Kullanıcı Taahhütnamesi"nde belirtilmiştir.
(2) Tüm kimlik bilgilerinin yönetimi "Parola Politikası"na uygun olarak yapılır.
(3) Kullanıcı hesap bilgilerinin uygulamalar tarafından hatırlanmaması sağlanır.

5.7. Bilgiye Erişimin Kısıtlanması

Erişim izinlerinde kullanıcıya, standart yetkilerin dışında daha fazla erişim yetkisi tanımlanmaz.

(1) Uygulamalara erişim yetkileri **Hata! Başvuru kaynağı bulunamadı.**0 Kullanıcı Erişimine İzin Verme maddesinde belirtildiği şekilde yapılır.
(2) Kullanıcı adı ve parola kullanımı olmadan uygulamalara erişim sağlanmaz.
(3) Kullanıcıların uygulamalara erişiminde sadece kullanacağı menülere erişim verilir.
(4) Hangi verinin hangi kullanıcı ya da kullanıcı grubu erişimi için olduğu belirlenir.
(5) Kullanıcılara verilecek erişim hakları okuma, değiştirme ve yönetme gibi yetkiler olarak belirlenir.

5.8. 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) Oturum açma işlemleri "Parola Politikası"nda belirtildiği şekilde yapılır.
(4) Tanımlanan bir hareketsizlik süresi sonunda aktif olmayan oturumlar sonlandırılır. Hareketsizlik süresi, bilginin kritikliği, uygulama özellikleri ve istemcinin taşıdığı risklerin derecesine göre belirlenir.
(5) Tüm bilişim sistemlerine ya da uygulamalara parola girilirken ekranda karakterlerin görüntülenmemesi sağlanır.

5.9. Parola Yönetim Sistemi

Kullanıcılar tarafından kullanılan parolalar "Parola Politikası"na uygun olarak tanımlanır.

5.10. Ayrıcalıklı Destek Programlarının Kullanımı

Kullanıcıların yürütmekte olduğu iş ve işlemlerin gereği olarak yardımcı programların kullanımı için aşağıdaki kurallar dikkate alınır:

(1) Ayrıcalıklı destek programlarının erişim talebi ihtiyaç olduğu durumlarda ilgili birim sorumlusunun bilgisi dahilinde paylaşılan bir bağlantı linki üzerinden gerçekleştirilir.
(2) Ayrıcalıklı destek programları erişim yetkisi süreli olarak açılır.

(3) Ayrıcalıklı destek programlarının erişimi için kimlik doğrulama ve yetkilendirme kriterlerine dikkat edilmesi sağlanır.
(4) Gerekli olmayan ayrıcalıklı destek programları sistemlerden kaldırılır.

5.11. Program Kaynak Koduna Erişim Kontrolü

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

(1) Kaynak kod ve kütüphaneler, canlı uygulama ortamında tutulmaz.
(2) Personelin, kaynak kod ve kütüphanelerine erişimi ihtiyaçlara göre sınırlandırılır.
(3) Program kaynak kod ve kütüphanesine erişimler, Bilgi İşlem Birimi yöneticisinden onay alınmadan yapılmaz.
(4) Program kaynak kod ve kütüphanesi ile ilgili değişiklikler için olay kayıtları tutulur ve saklanır.
(5) Değişiklikler öncesi kaynak kod ve kütüphanelerinin tüm sürümleri saklanır.

6. İlgili Dokümanlar

6.1. İç Kaynaklı Dokümanlar

(1) KA.01 BGYS Kapsam Analizi
(2) PL.05 Uzaktan Erişim ve Çalışma Politikası
(3) PL.08 Parola Politikası
(4) PR.02 Varlık Yönetimi Prosedürü
(5) PR.11 Fiziksel Güvenlik Prosedürü
(6) PR.21 Ağ Güvenliği Yönetimi Prosedürü
(7) KL.01 BGYS Roller ve Sorumluluklar Kılavuzu
(8) TH.01 Bilişim Sistemleri Kullanıcı Taahhütnamesi
(9) FR.08 Erişim Talep Formu
(10) FR.20 Erişim Yetki Matrisi

6.2. Dış Kaynaklı Dokümanlar

(1) TS ISO/IEC 27001:2013 Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler

Revizyon Kayıtları

Rev. No	Tarih	Hazırlayan	Revizyon Nedeni /Sayfa No	Onaylayan	İmza
1					
2					
3					
4					
5					