REVİZYON TABLOSU

REVİZYON NO	REVİZYON GEREKÇESİ	TARİH
01	2022 versiyon değişikliği	01.10.2024

1. AMAÇ

Bu prosedür; Aksaray Üniversitesi'nde bilgi ve bilgi işleme tesislerine erişimi kısıtlamak, yetkili kullanıcı erişimini temin etmek ve sistem ve hizmetlere yetkisiz erişimi engellemek, kullanıcıları kendi kimlik doğrulama bilgilerinin korunması konusunda sorumlu tutmak ve sistem ve uygulamalara yetkisiz erişimi engellemek için uygulanan yöntemleri ve alınacak tedbirleri tanımlamak üzere düzenlenmiştir.

2. KAPSAM

Bu prosedür; Bilgi Güvenliği Yönetim Sistemi kapsamında alınacak tüm Erişim Kontrolü tedbirlerini ve bu tedbirlerin uygulanmasına ait yönetimini kapsar.

3. UYGULAMA

3.1 ERİŞİM KONTROLÜ

3.1.1 Erişim Kontrolü İş Gereklilikleri

3.1.1.1 Erişim Kontrol Politikası

İş ve bilgi güvenliği şartları temelinde oluşturulmuş, dokümante edilmiş, yönetim tarafından gözden geçirilmiş bir erişim kontrol politikası vardır.

Erişim Kontrol Politikası;

- ✓ ASÜ Bilgi güvenliği yönetim sistemi kapsamı dâhilindeki faaliyetlerinde kullandığı bilgilerin güvenliğinin sağlanmasında en üst seviyede önlem almayı kabul eder.
- ✓ Çalışanların tüm iş faaliyetlerinde bilgiye erişim yetkisi, **"bilmesi gereken"** prensibine göre verilir ve faaliyetler **"Açıkça izin verilmedikçe her şey yasaktır"** prensibine göre yürütülür.
- ✓ ASÜ çalışanları, bilgi varlıklarını BGYS/BP/02 Varlık Yönetimi Prosedüründe belirlenen bilgi sınıflandırma düzeylerine göre doğru bir biçimde sınıflayarak etiketlemekle yükümlüdür. Tüm etiketlenmiş bilgi varlıklarının sınıflarına göre korunması esastır.
- ✓ ASÜ'de bilgi varlıklarına ve bilgi işleme tesislerine erişim yetkileri belirlenmiştir. Tüm kullanıcılar kendilerine verilmiş olan yetki çerçevesinde bilgi varlıklarına erişir ve bilgi sistem teçhizatını kullanırlar.

- ✓ Bilgi ve bilgi işleme olanaklarına erişimi sınırlandırmak amacı ile kuruluş içerisinde ortak iş rollerine göre standart kullanıcı erişim profilleri kullanılır.

Bilgi sınıflandırması ve buna bağlı olarak bilginin değeri (üçüncü tarafların eline geçmesi durumunda kuruma olan etkisi) BGYS/BP/02 Varlık Yönetimi Prosedüründe tanımlanmış, tüm kurum ve gerekli olduğu durumlarda tedarikçi çalışanları farkındalık ve oryantasyon eğitimlerinde konu hakkında bilgilendirilir.

- ✓ Erişim haklarının verilmesi, düzenlenmesi ve/veya kaldırılması ile ilgili erişim hakları talep yönetimi BGYS/BF/006 Yetkilendirme ve Talep Formu üzerinde yönetilmekte ve geliştirilmektedir.
- ✓ Kullanıcı kimlik bilgileri ve gizli kimlik doğrulama bilgileri kullanımı ve yönetimi ile ilgili tüm önemli olaylar kayıt altına alınmaktadır.
- ✓ Ayrıcalıklı erişim hakkı talebe bağlı olarak kontrollü ve sınırlı olarak verilir ve takip edilir.
- ✓ Erişim Kontrol politikası her yıl yönetimin gözden geçirme toplantısında yeniden gözden geçirilir.
- ✓ Verilere veya hizmetlere erişimin sınırlandırılmasına dair ilgili yasalar ve sözleşme yükümlülüklerine uyum sağlanmıştır.

3.1.1.2 Ağlara ve Ağ Hizmetlerine Erişim

- ✓ ASÜ içerisinde kullanılan network mantıksal olarak birbirinden ayrılmış ve ayrılmış networkler üzerinden veri akışı erişim kuralları ile kontrol edilir.
- ✓ ASÜ içinden ve dışından geçen Network kablolarının güvenliği uygun koruma yöntemleri ile sağlanır.
- ✓ Bilgisayarların ve diğer ağ öğelerinin birbirlerine bağlanmasına olanak veren ağ donanımlarına (Switch, Router, Modem vb.) erişim ve yönetimi sadece yetki verilmiş sistem yöneticileri tarafından yapılır.
- ✓ Bilgisayarların ve diğer ağ öğelerinin birbirlerine bağlanmasına olanak veren ağ donanımları (Switch, Router, Modem vb.) fiziksel olarak güvenli bölgede ve kilit altında tutulurlar.
- ✓ Bilgisayarların ve diğer ağ öğelerinin birbirlerine bağlanmasına olanak veren ağ donanımlarının (Switch, Router, Modem vb.) uzaktan yönetimi maksadıyla sadece sistem yöneticisinin erişebileceği şekilde yetkilendirilir.
- ✓ Internet üzerinden gelebilecek saldırıların ağ altyapısına erişimini önleme amacı ile güvenlik duvarı, atak tespit ve önleme (IPS, IDS) sistemleri kurum bünyesinde kullanılmaktadır.
- ✓ Çalışanlara uzaktan bağlantı izni talebi BGYS/BF/006 Yetkilendirme ve Talep Formunun doldurulması ve ilgili bölüm yöneticisinin onayı sonrasında Bilgi Teknolojileri Yöneticisi tarafından güvenlik gereksinimleri değerlendirildikten sonra verilmektedir.
- ✓ Kablosuz ağ altyapısı ASÜ genelinde kullanılmaktadır. Üretim alanındaki erişimler sadece işletme envanterindeki taşınabilir bilgisayar kullanıcıları ve el terminalleri tarafından kullanılabilmektedir. Kablosuz ağlara erişim için güvenli kimlik doğrulama yöntemleri devreye alınmıştır.
- ✓ Misafirlerin kullanımı için firewall üzerinde Hotspot özelliği devreye alınarak yerel ağdan

yalıtılmış ayrı bir internet erişim ağı oluşturulmuştur. Misafir ağına erişim için güvenli kimlik doğrulama yöntemleri devreye alınmıştır.

3.2.1 Kullanıcı Erişim Yönetimi

3.2.1.1 Kullanıcı Kaydetme ve Kayıt Silme

- ✓ Sisteme yeni bir kullanıcı kaydı ve iptal işlemleri BGYS/BF/006 Yetkilendirme ve Talep Formu üzerinden yapılmaktadır.
- ✓ Kullanıcı adları mutlaka tekildir.
- ✓ Tüm kullanıcılar şahsi kullanımları için kendine ait tek bir kullanıcı tanımına sahiptir.
- ✓ İş akdi feshedilen personelin bilgi sistemlerine erişim yetkileri, aksi belirtilmedikçe, ayrılışın kendisine bildirilmesinden 2 iş günü önce bilgi teknolojilerine İnsan Kaynakları tarafından yazılı olarak ve/veya e-mail ile bildirilmesinin ardından iş akdinin sona ermesinden 1 gün önce mesai bitiminde kaldırılır.
- ✓ Belediyemizden ayrılan / iş akdi feshedilen personele ait kullanıcı hesapları kaldırılır ve/veya bloke edilir.
- ✓ Kullanıcı erişim haklarının sağlanması, düzenlenmesi ya da iptali BGYS/BF/006 Yetkilendirme ve Talep Formu üzerinden yönetilmektedir.
- ✓ Gereksiz kullanıcı kimliklerini belirlemek ve kaldırmak ya da engellemek için kullanıcı hesapları en az 6 ayda bir gözden geçirilir.

3.2.1.2 Kullanıcı Erişimine İzin Verme

- ✓ Yetkilendirme talep aşamaları tamamlanmadan önce hiçbir bilgi sistemlerine ve hizmetlerine sistemlerde erişim hakları verilmez.
- ✓ Tedarikçi ASÜ çalışanı ve/veya yetkilisi admin kullanıcısını kullanamaz. Hizmet alınan dış kaynak ASÜ için AD (Active Directory)'ye ticari unvanlarını içeren kullanıcılar eklenir ve hizmet alınan firmalar sistem üzerinden gerekli işlemlerini bu kullanıcılar üzerinden tanımlanan yetkiler çerçevesinde gerçekleştirirler.
- ✓ Bilgi sistemlerine ve hizmetlerine erişim hakları (erişim hakkı verilmesi, değiştirilmesi, kaldırılması gibi hususlar) BGYS/BF/006 Yetkilendirme ve Talep Formu üzerinde gerçekleştirilir. (E-posta talepleri, Akıllı telefon, Tablet vb. cihazlar üzerinden sistemlere erişim talepleri, İnternet erişim talepleri, Dosya ve/veya klasör erişim talepleri, v.b)
- ✓ Kuvvetli yetkilendirme ve kimlik doğrulamasının gerektiği durumlarda sadece parola ile yetinilmeyip veriye erişimin 2. metotla şifrelenmesi kontroller de kullanılmaktadır.
- ✓ Çalışan ya da yüklenici tarafından yetkisiz erişim teşebbüsü olması halinde Bilgi Güvenliği İhlal olayı formu düzenlenir ve yasa ve sözleşme şartlarına göre ilgili disiplin yönetmeliği uygulanır.

3.2.1.3 Ayrıcalıklı Erişim Haklarının Yönetimi

- ✓ Ayrıcalıklı yetkilerin tanımlanması kontrollü ve sınırlı olarak yapılmaktadır.
- ✓ Ayrıcalıklı erişim hakları düzenli iş faaliyetleri için kullanılan kullanıcı kimliğinden farklı bir kullanıcı kimliği ile yapılmakta ve düzenli olarak takip edilmektedir.

- ✓ Ayrıcalıklı erişim hakkı yetkilendirme talebi onaylanmadan verilmemektedir.
- ✓ Ayrıcalıklı erişim hakları; görev değişikliği, sözleşmenin sona ermesi, işten ayrılma gibi durumlarda yeniden düzenlenir.
- ✓ Ayrıcalıklı erişim hakları en az 6 ayda bir Bilgi Teknolojileri tarafından gözden geçirilir. Tedarikçilere ve/veya müşterilere tanımlanan ayrıcalıklı erişim haklarının geri alınması ile ilgili bölüm yöneticileri Bilgi Teknolojileri departmanına mail ile bildirimde bulunur.
- ✓ İşletim sistemleri üzerinde, veri tabanı yönetim sistemleri üzerinde sadece Bilgi Teknolojileri Müdürlüğü çalışanları ayrıcalıklı yetkiye sahiptir.
- ✓ Ayrıcalıklı bir kullanıcı işten ayrıldığında ya da işi değiştiğinde parolalar değiştirilir, uygun mekanizmalarla ayrıcalıklı kullanıcılar arasında iletişim sağlanır.
- ✓ Fonksiyonel roller için asgari gereklilikler temelinde ayrıcalıklı erişim hakkı verilir.

3.2.1.4 Kullanıcılara Ait Gizli Kimlik Doğrulama Bilgilerinin Yönetimi

- ✓ Bilgi sistemlerinde kullanılan bilgisayarların ve diğer cihazların üretici firmaları tarafından verilen varsayılan sistem parolaları mutlak surette değiştirilir.
- ✓ Kullanıcılar kişisel gizli kimlik doğrulama bilgilerini başka biriyle paylaşılmaması konusunda uyarılmıştır.

3.2.1.5 Kullanıcı Erişim Haklarının Gözden Geçirilmesi

- ✓ Kullanıcı erişim hakları görev değişikliği, işten ayrılma, yetki talepleri dışında yılda en az bir kez sistem yöneticisi tarafından gözden geçirilmektedir.
- ✓ Ayrıcalıklı hesapların değişimi yılda en az bir kez gözden geçirilmektedir.

3.2.1.6 Erişim Haklarının Kaldırılması veya Düzenlenmesi

- ✓ Kuruluş içerisinde bir birimden başka bir birime görevlendirilen personelin erişim hakları Bilgi İşlem Daire Başkanlığı'na yazılı ve/veya mail yoluyla bildiriminden sonra Bilgi teknolojileri bölümü tarafından yeniden düzenlenir.
- ✓ İşten ayrılan, iş akdi feshedilen, sözleşmesi sona eren tedarikçi ve çalışanına ait erişim hakları İnsan Kaynakları Müdürlüğünün ya da ilgili bölüm müdürlüğünün yazılı ve/veya mail yoluyla bildiriminden sonra Bilgi İşlem Müdürlüğü tarafından kaldırılır.
- ✓ Erişim haklarındaki değişiklikler BGYS/BF/006 Yetkilendirme ve Talep Formu üzerinden yapılır.
- ✓ Kaldırılacak ya da yeniden ayarlanacak erişim hakları, fiziksel ve/veya mantıksal erişim haklarını içermektedir.
- ✓ İşten ayrılan bir çalışanın veya dış taraf kullanıcısının aktif kalan kullanıcı kimliklerinin parolalarını biliyorlarsa, istihdam, anlaşma veya sözleşme feshi durumunda veya değişiminde değiştirilmektedir.

3.3.1 Kullanıcı Sorumlulukları

3.3.1.1 Gizli Kimlik Doğrulama Bilgisinin Kullanımı

- ✓ Kullanıcıların parolaları gizli, benzersiz ve şifre politikalarına uygun olarak oluşturulmaktadır.
- ✓ Parola, başkaları tarafından kolay tahmin edilemeyecek şekilde oluşturulmaktadır. (Doğum tarihi, çocukların isimleri, telefon numarası vb. olmamalıdır).
- ✓ Kullanıcılar parolalarını başkaları ile paylaşmayacaktır. Paylaşanlar hakkında disiplin işlemi uygulanır.
- ✓ Çalışanlar şifrelerini kâğıtlara veya elektronik ortamlara yazmayacaktır.

3.4.1 Sistem ve Uygulama Erişim Kontrolü

3.4.1.1 Bilgiye Erişimin Kısıtlanması

- ✓ Bilgiye erişim sağlayan uygulamalar yetki verilen kullanıcılar tarafından yetkileri çerçevesinde kullanılır.
- ✓ Hassas uygulamaların, uygulama verilerinin veya sistemlerin yalıtımı için fiziksel ya da mantıksal erişim kontrolleri uygulanmaktadır.
- ✓ Kullanıcıların erişim hakları okuma, yazma, silme ve çalıştırma yetkileri ile sınırlandırılmıştır.
- ✓ Dosya sunucuları, veri tabanları üzerindeki dosya ve veri erişim yapısı;
- ✓ Kullanıcıların yedeklenmesi gereken elektronik dosyaları dosya sunucusu üzerinde saklanmaktadır. Dosya sunucusuna erişimler yetkilendirilmiştir. (Okuma, Yazma, Silme) Sadece erişim yetkisi bulunan kullanıcılar ilgili dosya ve klasörlere erişim sağlayabilmektedir.
- ✓ Veri tabanlarına erişim yetkisi sınırlandırılmıştır. Veri tabanlarına erişim yetkisi sadece Bilgi Sistemleri bölümü çalışanlarında bulunmaktadır. Erişimler takip edilmektedir.

3.4.1.2 Güvenli Oturum Açma Prosedürleri

- ✓ Uygulanabilir tüm sistemlerde girdi alanları tamamlandıktan sonra sisteme giriş bilgisi doğrulanmaktadır. Bir hata ortaya çıktığında sistem hangi bilgilerin doğru olduğunu, hangilerinin yanlış olduğunu göstermemektedir.
- ✓ Parola girişi sırasında karakterler görünmemekte veya sembollerle gizlenmektedir.
- ✓ 300 sn sonra oturum ekranını kilitleyen bir zaman aşımı kolaylığı kullanılmaktadır.
- ✓ Başarısız oturum açma denemesi üç deneme ile sınırlandırılmıştır. Fazla denemelerde sistem kendisini belirli bir sure kilitleyecek ve kullanıcıya uyarı verecek şekilde ayarlanmıştır.
- ✓ Ağ üzerinden parolalar açık metin olarak iletilmemektedir.
- ✓ Başarılı ve başarısız girişimlerin kayıtları tutulmaktadır.
- ✓ Yüksek riskli uygulamalar için ek güvenliği sağlamak ve yetkisiz erişim fırsatlarını azaltmak amacıyla bağlantı sürelerinin kısaltılması.

3.4.1.3 Parola Yönetim Sistemi

- ✓ Uygulanabilir tüm sistemlerde hesap verilebilirliği sağlamak için kullanıcılar nitelikli parola seçimine ve kullanımına zorlanmaktadır.
- ✓ Uygun olan sistemlerde kullanıcıların kendi parolalarını seçmelerine ve değiştirmelerine izin verilmekte, giriş hataları için bir doğrulama prosedürü uygulanmaktadır.
- ✓ Uygun olan sistemlerde kullanıcılar şifrelerini 5 kez hatalı girmeleri durumunda sistem tarafından kullanıcı hesabı geçici olarak bloke edilir.
- ✓ Uygulanabilir tüm sistemlerde kullanıcılar kendi parolalarını ilk oturum açmada değiştirmeye zorlanmaktadır,
- ✓ Kullanıcılar uygulanabilir tüm sistemlerde düzenli olarak parola değiştirmeye zorlanmaktadır.
- ✓ Uygulanabilir tüm sistemlerde kullanıcıların bir önceki parolalarını tekrar kullanmaları engellenmektedir,
- ✓ Giriş yapılırken parolaların ekranda görüntülenmemesi sağlanmaktadır,
- ✓ Kullanıcıların kendi parolalarını seçme imkânı olmayan sistemlerde kullanıcılara atanan parolaların saklandığı dosyaların güvenliği sistem üzerinden parola atama yetkisi olan yöneticilere aittir. Parola dosyaları Uygulama sistem verilerinden ayrı bir yerde uygulanabilir durumlarda şifreli olarak saklanmak zorundadır.
- ✓ Kullanıcıların kendi parolalarını seçme imkânı olmayan sistemlerde kullanıcılara atanan parolaların kullanıcılara e-mail üzerinden ya da sistem üzerinden açık bir metin olarak iletilmesi yasaklanmıştır. Şifreler korumalı formlarda iletilmektedir.
- ✓ Şifre politikalarımız aşağıdaki gibi tanımlanmış ve uygulanmaktadır;

Active Directory (Etki Alanı) Şifre Politikası

- ✓ Şifreler tüm bölüm çalışanları için en az 8 karakter olması gerekmektedir ve kullanıcı adı içermemelidir.
- ✓ Parola belirlenirken Büyük harf, küçük harf, rakam ve semboller kullanılacaktır. Ardışık harf ve rakamlar, bilinen isimler, tarihler parola belirlerken kullanılmayacaktır.
- ✓ Şifreler karmaşık içeriğe sahip olmaktadır. (En az 1 büyük harf, en az 1 sayı ve en az 1 sembol (*, ? , /, % vb.) kullanılmalıdır.)
- ✓ Şifreler en son belirlenen 3 şifre ile benzerlik göstermemektedir.
- ✓ Şifrelerin her 6 ayda bir tekrar yenilenmesi isteniyor, sistem tarafından kullanıcılar son 7 gün kala uyarılmaktadır.
- ✓ Oturum açma ve şifre değişim işlemleri ADManager programı tarafından kayıt altına alınmaktadır.

VPN (Virtual Private Network) Şifre Politikası

- ✓ VPN Şifreleri en az 8 karakter ve karmaşık içeriktedir.
- ✓ VPN hizmeti kullanımlarına ait loglar kayıt altına alınmaktadır.
- ✓ VPN Erişim yetki talepleri programı üzerinden gerçekleştirilmekte ve kayıt altına alınmaktadır.

Sistem Altyapısı Şifre Politikası

- ✓ BT Sistem altyapısında bulunan cihazlar ve özel yazılımlara (Switch, Güvenlik Duvarları, Storage, vb.) erişim şifreleri karmaşık olarak tanımlanmakta ve minimum 7 karakterden oluşmaktadır.
- ✓ İlgili şifreler cihaz veya yazılımların sistemi etkilememesi koşulu göz önüne alınarak değiştirilmektedir.
- ✓ Parola belirlenirken büyük harf, küçük harf, rakam ve semboller kullanılacaktır. Ardışık harf ve rakamlar, bilinen isimler, tarihler parola belirlerken kullanılmayacaktır.
- ✓ Şifreler karmaşık içeriğe sahip olmaktadır. (En az 1 büyük harf, en az 1 sayı ve en az 1 sembol (*, ? , /, % vb.) kullanılmalıdır.)
- ✓ Yerel Yönetici Hesapları Şifre Politikası
- ✓ Yerel Yönetici şifreleri sistemi etkilememesi koşulu göz önüne alınarak değiştirilmektedir.

3.4.1.4 Ayrıcalıklı Destek Programlarının Kullanımı

- ✓ Sunucu ve sistemler üzerinde ayrıcalıklı destek programlarının kullanımı kısıtlanmış ve hesap verilebilirlik için yetkilendirilmiştir. Kullanımı kayıt altına alınmaktadır.
- ✓ Ayrıcalıklı destek programlarının kullanımı ile ilgili yetkilendirme talepleri BGYS/BF/006 Yetkilendirme ve Talep Formu üzerinden yapılmaktadır.
- ✓ Uygulama yazılımları ve destek programları birbirinden ayrılmıştır, (Destek programları; genel sistem destek işlemlerini yapmak için kullanılan programlardır. Diskleri biçimlendirmek, dosyaları kopyalamak, disklerdeki programları yedeklemek, dosya sıkıştırma, virüs temizleme v.b işlemleri yaparlar.)
- ✓ Sistem ve uygulamaların kontrollerini geçersiz kılma kabiliyetine sahip yöntemleri (ARP Poisoning, DHCP Snooping, Proxy, Portable uygulama kullanımı, uzaktan erişim ve benzeri) kullanan uygulama ve donanımların engellenmesi için gerekli kontroller devreye alınmıştır.
- ✓ Uygulanabilir durumlarda Uygulama ve işletim sistemlerindeki tüm gereksiz yardımcı programlar kaldırılmakta ya da devre dışı bırakılmaktadır.
- ✓ Kullanıcı bilgisayarlarında local admin hakları işletim sistemi üzerinde bulunan ayrıcalıklı destek programlarının kullanımının önlenmesi amacıyla alınmıştır.

3.4.1.5 Program Kaynak Koduna Erişim Kontrolü

- ✓ Kurum içi yazılımların kaynak kodları veri tabanı sunucusu ve GIT üzerinde saklanmaktadır. Geliştirmeler ve kodda yapılan değişiklikler GIT üzerinde versiyonlanmaktadır. İlgili kaynak kodlara erişim uygulama veya veri tabanı sunucusu üzerinde erişim hakları ile sınırlandırılmıştır.
- ✓ Kurum içi yazılımların program kaynak kütüphanelerinin, ilgili öğelerin ve program kaynaklarının programcılara yayımı verilen grup (BT yazılım ve BT otomasyon yazılım birimleri) yetkileri ile sağlanmaktadır.
- ✓ Destek personeli, program kaynak kütüphanesine kontrollü erişim yetkisine sahip olabilir.
- ✓ Program kaynak kütüphanelerine yapılan tüm erişimler ile ilgili denetim kayıtları tutulmaktadır.

5. SORUMLULUK

Kapsam dâhilindeki tüm personel Erişim Kontrolü Prosedürü uygulama esaslarına uygun hareket etmekle yükümlüdür**.**

6. EK

BGYS/BP/02 Varlık Yönetimi Prosedürü

BGYS/BF/006 Yetkilendirme ve Talep Formu