



AKSARAY ÜNİVERSİTESİ BGYS PROSEDÜRÜ

Doküman No	BGYS-PR-001
İlk Yayın Tarihi	17.01.2022
Revizyon Tarihi	01.10.2024
Revizyon No	01
Sayfa No	1/27

REVİZYON TABLOSU

REVİZYON NO	REVİZYON GEREKÇESİ	TARİH
01	2022 Versiyon Değişikliği	01.10.2024

1. AMAÇ

Bu prosedür, Aksaray Üniversitesi'nin Bilgi Güvenliği Yönetim Sistemi (BGYS)'nin kurulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi aşamalarında Standart şartlarının ve gereksinimlerinin nasıl karşılandığını açıklamak ve tariflemek amacıyla hazırlanmıştır.

2. KAPSAM

Bu prosedür, ISO 27001 standardının en son revizyonu olan ISO 27001:2022 versiyonuna uygun olarak hazırlanmıştır.

3. TANIMLAR

Kurum	: Aksaray Üniversitesi
Adres	: Aksaray Üniversitesi Bahçesaray Mahallesi 68100 Aksaray
Web Sitesi	: https://www.aksaray.edu.tr/
Telefon	: (0382) 288 30 60
Mail Adresi	: aksarayuniversitesi@aksaray.edu.tr
Kep Adresi	: aksarayuniversitesi@hs01.kep.tr

BGYS kapsamı "Aksaray Üniversitesi'nde sunulan yazılım geliştirme, bilişim hizmetleri ve danışmanlık hizmetleri, bu hizmetlere ilişkin yazılım geliştirme süreçleri, danışmanlık süreçleri ve bilişim hizmet süreçlerinde, finans, bilgi işlem, yazılım geliştirme, teknik destek, sistem, ağ yönetimi, Aksaray Üniversitesi'nde gerçekleşen tüm faaliyetleri gibi faaliyetlerin bilgi varlıkları ile bu varlıkları korumak amacıyla kullanılan tüm tedbirler ve varlıkların bulunduğu idari bina ve tesislerde bilgi güvenliğinin sağlanması." dır.

3.1. Bilgi Güvenliği Yönetim Sistemi

Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için, iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçasıdır.

BGYS: Bilgi Güvenliği Yönetim Sistemi

Hazırlayan	Yürürlük Onayı	Kalite Sistem Onayı
Birim Kalite Sorumlusu	Kalite Koordinatör Yardımcısı	Kalite Koordinatörü



AKSARAY ÜNİVERSİTESİ BGYS PROSEDÜRÜ

Doküman No	BGYS-PR-001
İlk Yayın Tarihi	17.01.2022
Revizyon Tarihi	01.10.2024
Revizyon No	01
Sayfa No	2/27

Bilgi: Herhangi bir konu ile ilgili verilerin bir araya gelmesi ile oluşan açıklayıcı ifadeler bütünüdür. Veri, olguların harf, sayı, renk gibi sembollerle ifade edilmesidir.

Bilgi Varlığı: Kuruluş için değer ifade eden herhangi değerli bilgi veya veri.

Bilgi Güvenliği: Bilginin gizliliğinin, bütünlüğünün ve erişilebilirliğinin korunması.

Varlık: Kuruluş için değeri olan herhangi bir şey. Varlıkların birçok çeşidi vardır: Bilgi varlığı, Yazılım varlığı (bir bilgisayar programı gibi), Fiziksel varlıklar (bilgisayar gibi), Tedarikçi hizmetleri, Kişiler, Maddi olmayan varlıklar (itibar ve imaj gibi)

Gizlilik: Bilginin yetkisiz kişiler, varlıklar veya prosesler için elverişli yapılmaması ya da açıklanmaması özelliği

Bütünlük: Varlıkların doğruluğunu ve tamlığını koruma özelliği.

Erişilebilirlik: Yetkili bir tüzel kişilik tarafından talep edildiğinde erişilebilir ve kullanılabilir olma özelliği.

Risk: Bir olay ve sonucunun olasılıklarının birleşimi.

Risk Sahibi: Bir riski yönetmek için sorumluluk ve yetki sahibi kişi veya birim.

Risk Analizi: Kaynakları belirlemek ve riski tahmin etmek amacıyla bilginin sistematik kullanımı.

Risk Değerlendirmesi: Risk analizi ve risk derecelendirmesini kapsayan genel proses

Risk İşleme: Risk değerlendirme sonuçlarını dikkate alarak; Riskin düşürülmesi, Riskin devredilmesi, Riskten kaçınma ve riski kabul etme faaliyetlerinin yapılması

Artık Risk: Risk işlemeden sonra geriye kalan risk.

Risk Kriterleri: Riskin kabul edilebilir ya da kabul edilemez olduğunun tespiti için kullanılan kurallar.

Tehdit: Bir sistem veya kuruluştaki zarara neden olabilecek istenmeyen bir olayın potansiyel nedeni.

Zafiyet: Bir tehdit tarafından istismar edilebilecek bir varlık ya da kontrol zafiyeti.

Uygulanabilirlik Bildirgesi: Bilgi Güvenliği Yönetim Sistemi ile ilgili ve uygulanabilir kontrol amaçlarını ve kontrolleri açıklayan belgelenmiş bildirme.

Uygunsuzluk: Bir şartın yerine getirilmemesi.

Düzeltilici Faaliyet: Mevcut bir uygunsuzluğun sebep ve/veya sebeplerini ortadan kaldırmak için yapılan faaliyettir.

Hazırlayan

Birim Kalite Sorumlusu

Yürürlük Onayı

Kalite Koordinatör Yardımcısı

Kalite Sistem Onayı

Kalite Koordinatörü



AKSARAY ÜNİVERSİTESİ BGYS PROSEDÜRÜ

Doküman No	BGYS-PR-001
İlk Yayın Tarihi	17.01.2022
Revizyon Tarihi	01.10.2024
Revizyon No	01
Sayfa No	3/27

Bilgi Güvenliği İhlal Olayı: İş operasyonlarını tehlikeye atma ve bilgi güvenliğini tehdit etme olasılığı yüksek olan tek ya da bir dizi istenmeyen ya da beklenmeyen bilgi güvenliği olayıdır.

4. UYGULAMA

4.1. KURULUŞUN BAĞLAMLI

4.1.1. Kuruluşun Bağlamının Anlaşılması

Aksaray Üniversitesi amaçları ile ilgili olan ve Bilgi Güvenliği Yönetim Sisteminin hedeflenen çıktılarını başarma kabiliyetini etkileyebilecek iç ve dış hususları BGYS/BF/001BGYS İlgili Taraf Beklentiler ve İletişim Formunda tanımlamıştır.

4.1.2. İlgili Tarafların İhtiyaç ve Beklentilerinin Anlaşılması

Aksaray Üniversitesi BGYS ilgili iç ve dış taraflara ait ihtiyaç ve beklentilerini (bilgi güvenliği gereksinimlerini) BGYS/BF/001BGYS İlgili Taraf Beklentiler ve İletişim Formunda tanımlamıştır.

4.1.3. Bilgi Güvenliği Yönetim Sisteminin Kapsamının Belirlenmesi

Aksaray Üniversitesi Bilgi Güvenliği Yönetim Sisteminin kapsamını sınırlarını ve uygulanabilirliğini aşağıdaki gibi belirlemiştir.

BGYS kapsamı

Sistem, sunucu, network alt yapı çalışmaları, yazılım geliştirme ve yazılım AR-GE faaliyetleri, Aksaray Üniversitesi faaliyetleri ve bu faaliyetleri gerçekleştirirken muhasebe, finans ve bilgi işlem, satın alma, insan kaynakları gibi faaliyetlerinin fiziksel ve elektronik bilgi varlıkları ile bu varlıkları korumak amacıyla kullandığı bilişim güvenliğinin sağlanması olarak belirlenmiştir.

BGYS kapsamına ait, sınırlarını ve uygulanabilirliğini lokasyon ve birim olarak aşağıdaki gibi tanımlanmıştır.

Birimler

- ✓ Ağ ve Sistemler Birimi
- ✓ Web Hizmetleri Birimi
- ✓ EBYS Birimi
- ✓ Taşınır/Satın Alma Birimi
- ✓ Teknik Servis Birimi

BGYS kapsamı ve sınırları içerisinde bulunan bilgi varlıkları kategorileri BGYS/BP/02 Varlık Yönetimi Prosedürü içerisinde tanımlanmıştır.

4.1.4. Bilgi Güvenliği Yönetim Sistemi

Aksaray Üniversitesi ISO IEC 27001:2022 Bilgi Güvenliği Yönetim Sisteminin şartları çerçevesinde PUKÖ (Planla-Uygula-Kontrol Et-Önlem Al) çalışma prensibine bağlı olarak bir Bilgi Güvenliği Yönetim Sistemi kurmuş, uygulamakta ve sürekli iyileştirmektedir.

Hazırlayan

Birim Kalite Sorumlusu

Yürürlük Onayı

Kalite Koordinatör Yardımcısı

Kalite Sistem Onayı

Kalite Koordinatörü



AKSARAY ÜNİVERSİTESİ BGYS PROSEDÜRÜ

Doküman No	BGYS-PR-001
İlk Yayın Tarihi	17.01.2022
Revizyon Tarihi	01.10.2024
Revizyon No	01
Sayfa No	4/27

4.2. LİDERLİK

4.2.1. Liderlik ve Bağlılık

Üst Yönetim, Bilgi Güvenliği Yönetim Sistemi ile ilgili olarak aşağıdaki hususlarda liderlik yapmaktadır.

- ✓ Üst Yönetim bilgi güvenliğine bakış açısını Bilgi Güvenliği Yönetim Sistemi Politikası altında tüm personele aktarmış ve bu politikanın getirdiği sorumluluklar ile BGYS ye uyum sağlamanın önemi tüm çalışanlara eğitimler ve duyurular yolu ile açıklanmıştır.
- ✓ Bilgi Güvenliği Yönetim Sistemi Politikasını ve bilgi güvenliği amaçlarını oluşturarak kuruluşun stratejik yönü ile uyumlu olmalarını sağlamıştır. Bilgi güvenliği amaç ve hedeflerinin gerçekleştirilmesi Üst Yönetim tarafından Yönetimin Gözden Geçirme toplantılarında incelenerek gelişme fırsatları belirlenmektedir.
- ✓ Bilgi Güvenliği Yönetim Sisteminin şartlarının kuruluşun süreçleri ile bütünleştirilmesini sağlamıştır.
- ✓ Bilgi Güvenliği Yönetim Sistemi için gerekli olan kaynakların erişilebilirliğini temin etmiştir. Bilgi Güvenliği Yönetim Sistemi için gerekli insan ve teknolojiye ait kaynak planlamaları birimler tarafından belirlenerek Üst Yönetime iletilir. Bu ihtiyaçlar belirlenirken risk analizi sonucunda alınması gereken önlemler, kaynak ihtiyacının en önemli girdilerindedir. Üst Yönetim, birimlerden alınan bu bilgi ışığında değerlendirme yaparak, uygun bulunanların teminini sağlar.
- ✓ Bilgi Güvenliği Yönetim Sisteminin etkinliğine katkı sağlamaları için kişilerin yönlendirilmesi ve desteklenmesini sağlamıştır. Personelin BGYS ile ilgili etkin katkı sağlamaları için gereken eğitim ihtiyaçları birim yöneticileri tarafından tespiti yapılır ve temini için Üst Yönetim onayına sunulur. Üst Yönetim, uygun bulunanların teminini sağlar.
- ✓ Sürekli iyileştirme için gerekli desteği sağlamıştır.

4.2.2. Politika

Üst Yönetim, aşağıdaki hususları karşılayan bir BGYS/POL/01 Bilgi Güvenliği Yönetim Sistemi Politikasını oluşturmuş tüm çalışanlara duyurmuş ve ilgili taraflarca erişilebilirliğini sağlamıştır.

- ✓ Kuruluşun amacına uygun,
- ✓ Bilgi güvenliği amaçlarını içeren veya bilgi güvenliği amaçlarını belirlemek için bir çerçeve sağlayan,
- ✓ Bilgi güvenliği ile ilgili uygulanabilir şartların karşılanmasına ve Bilgi Güvenliği Yönetim Sisteminin sürekli iyileştirilmesine dair bir taahhüt içeren politika.

4.2.3. Kurumsal Roller ve Sorumluluklar

Üst Yönetim, Bilgi Güvenliği Yönetim Sisteminin standardın şartlarına uyum sağlamasını temin etmek ve Bilgi Güvenliği Yönetim Sisteminin performansı hakkında kendisine raporlama yapmak için Bilgi güvenliği yöneticisi olarak Bilgi İşlem Dairesi Başkanlığı Öğretim Görevlisi Perihan Gülşah Gülhan atanmış ve tüm çalışanlara duyurulmuştur.

Hazırlayan	Yürürlük Onayı	Kalite Sistem Onayı
Birim Kalite Sorumlusu	Kalite Koordinatör Yardımcısı	Kalite Koordinatörü



AKSARAY ÜNİVERSİTESİ BGYS PROSEDÜRÜ

Doküman No	BGYS-PR-001
İlk Yayın Tarihi	17.01.2022
Revizyon Tarihi	01.10.2024
Revizyon No	01
Sayfa No	5/27

4.3. PLANLAMA

4.3.1. Risk ve Fırsatları Ele Alan Faaliyetler

4.3.1.1. Genel

Aksaray Üniversitesi Bilgi Güvenliği Yönetim Sistemi planlaması yaparken, aşağıdakilerin gerçekleştirilmesi için gerekli olan riskleri ve fırsatları ele almak için Risk değerlendirmesi, Risk işleme faaliyetlerini ve bu faaliyetlerin nasıl gerçekleştirileceğini Madde 4.3.1.2 ve 4.3.1.3 'te tanımlamıştır.

- ✓ Bilgi Güvenliği Yönetim Sisteminin amaçlanan çıktıları sağlayabilmesinin temin edilmesi,
- ✓ İstenmeyen etkilerin önlenmesi veya azaltılması,
- ✓ Sürekli iyileştirmenin başarılması,

4.3.1.2. Bilgi Güvenliği Risk Değerlendirme

Aksaray Üniversitesi, aşağıda belirtilen şartları yerine getiren bir Bilgi Güvenliği Risk Değerlendirmesi sürecini BGYS/BP/03 BGYS Risk Yönetimi Prosedüründe tanımlamış ve uygulamaktadır.

- ✓ Risk kabul kriterleri ve Bilgi Güvenliği Risk Değerlendirmesi yapılması için kriterler,
- ✓ Tekrarlanan Bilgi Güvenliği Risk Değerlendirmelerinin tutarlı, geçerli ve karşılaştırılabilir sonuçlar üretmesinin temin edilmesi,
- ✓ Bilgi Güvenliği Yönetim Sistemi kapsamı dâhilindeki bilginin Gizlilik, Bütünlük ve Erişilebilirlik kayıpları ile ilgili risklerin tespit edilmesi için Bilgi Güvenliği Risk Değerlendirme prosesinin uygulanması ve risk sahiplerinin belirlenmesi,
- ✓ Belirlenen riskler gerçekleştiği takdirde muhtemel sonuçların değerlendirilmesi,
- ✓ Belirlenen risklerin gerçekleşmesi ihtimalinin gerçekçi bir şekilde değerlendirilmesi ve Risk seviyelerinin belirlenmesi,
- ✓ Risk Analizi sonuçlarının risk kriterleri ile karşılaştırılması ve Analiz edilen risklerin risk işleme için önceliklendirilmesi.

4.3.1.3. Bilgi Güvenliği Risk İşleme

Aksaray Üniversitesi, aşağıda belirtilen şartları yerine getiren bir bilgi güvenliği risk işleme sürecini BGYS/BP/03 BGYS Risk Yönetimi Prosedüründe tanımlamış ve uygulamaktadır.

- ✓ Risk değerlendirme sonuçlarını dikkate alarak uygun bilgi güvenliği risk işleme seçeneklerinin seçilmesi,
- ✓ Seçilen bilgi güvenliği risk işleme seçeneklerinin uygulanmasında gerekli olan tüm kontrollerin belirlenmesi,
- ✓ EK-A'daki kontrollerin karşılaştırılması ve gerekli hiçbir kontrolün gözden kaçırılmadığının doğrulanması,
- ✓ EK-A da listelenen kontrol amaçları ve kontroller yeterli görülmediği durumlarda ilave kontrol amaçları ve kontrollerin tanımlanması,
- ✓ Gerekli kontrolleri, bunların dahil edilmesinin gerekçelendirilmesi, uygulanıp uygulanmadıklarını ve EK-A dan kontrollerin dışarıda bırakılmasının gerekçelendirilmesini içeren bir Uygulanabilirlik Bildirgesinin üretilmesi,
- ✓ Bir bilgi güvenliği risk işleme planının formüle edilmesi ve bilgi güvenliği risk işleme planına

Hazırlayan

Birim Kalite Sorumlusu

Yürürlük Onayı

Kalite Koordinatör Yardımcısı

Kalite Sistem Onayı

Kalite Koordinatörü



AKSARAY ÜNİVERSİTESİ BGYS PROSEDÜRÜ

Doküman No	BGYS-PR-001
İlk Yayın Tarihi	17.01.2022
Revizyon Tarihi	01.10.2024
Revizyon No	01
Sayfa No	6/27

dair risk sahiplerinin onayının alınması ve artık bilgi güvenliği risklerinin Üst Yönetim tarafından kabulü.

4.3.1.4. Bilgi Güvenliği Amaçları ve Bu Amaçları Başarmak İçin Planlama

Aksaray Üniversitesi Bilgi Güvenliği Yönetim Sistemi Politikasına uygun olarak Bilgi Güvenliği Yönetim Sisteminin esasını oluşturan varlıklarının gizlilik, bütünlük ve erişilebilirliğinin korunması amacıyla Bilgi Güvenliği Yönetim Sistemi Politikasında belirlediği ilkeleri aynı zamanda ana amaçları olarak kabul etmektedir.

Aksaray Üniversitesi Bilgi güvenliği amaçlarını başarmak için aşağıdaki hususları göz önüne alarak bir planlama yapmış ve BGYS /BF/002 BGYS Etkinlik Ölçümü ve Amaçlar Formu ile takip etmektedir.

- ✓ Bilgi Güvenliği Yönetim Sistemi Politikası ile tutarlı olmalı,
- ✓ Ölçülebilir olmalı (uygulanabilirse),
- ✓ Uygulanabilir bilgi güvenliği şartlarını ve risk değerlendirme ve risk işleminin sonuçlarını dikkate almalı,
- ✓ Duyurulmalı ve uygun şekilde güncellenmelidir.
- ✓ Ne yapılacağı,
- ✓ Hangi kaynakların gerekli olacağı,
- ✓ Kimin sorumlu olacağı,
- ✓ Ne zaman tamamlanacağı ve sonuçların nasıl değerlendirileceği

4.4. DESTEK

4.4.1. Kaynaklar

Aksaray Üniversitesi, Bilgi Güvenliği Yönetim Sisteminin kurulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi için gerekli olan kaynaklara ait bütçe planını belirlerken aşağıdaki hususları göz önüne almış ve uygulamaktadır.

- ✓ Bilgi Güvenliği Yönetim Sistemi için gerekli insan ve teknolojiye ait kaynak planlaması
- ✓ Risk analizi sonuçlarına göre alınması gereken önlem ve kontrollere ait kaynak planlaması
- ✓ Çalışanların BGYS ile ilgili etkin katkı sağlamaları için gereken eğitim ihtiyaçlarına ait kaynak planlaması
- ✓ Bilgi Güvenliği Yönetim Sisteminin kurulması için gerekli hizmete ait kaynak planlaması

4.4.2. Yeterlilik

Aksaray Üniversitesi çalışanların BGYS yeterliliğinin sağlanması hususunda aşağıdaki hususları dikkate alarak planlama yapmakta ve gerçekleştirmektedir. Yeterliliğin delili olan kayıtlar saklanmaktadır.

- ✓ Bilgi güvenliği performansını etkileyen (BGYS Kurulu Üyeleri ve Birimlerin BGYS Sorumluları) çalışanların gerekli BGYS yeterliliklerinin temin edilmesi,
- ✓ Yeterliliklerin teminine yönelik girişimlerin etkinliğinin değerlendirilmesi ve yeterliliğin delili olarak uygun yazılı bilgilerin (sertifika, eğitim notları vb.) muhafaza edilmesi.

4.4.3. Farkındalık

Aksaray Üniversitesi çalışanlarının BGYS farkındalıklarının sağlanması ile ilgili aşağıdaki hususları da içeren

Hazırlayan	Yürürlük Onayı	Kalite Sistem Onayı
Birim Kalite Sorumlusu	Kalite Koordinatör Yardımcısı	Kalite Koordinatörü



AKSARAY ÜNİVERSİTESİ BGYS PROSEDÜRÜ

Doküman No	BGYS-PR-001
İlk Yayın Tarihi	17.01.2022
Revizyon Tarihi	01.10.2024
Revizyon No	01
Sayfa No	7/27

farkındalık eğitim programlarını yılda en az bir kez düzenlenmektedir. Farkındalık programlarına ait kayıtlar saklanmaktadır.

- ✓ Bilgi Güvenliği Yönetim Sistemi Politikası,
- ✓ Bilgi Güvenliği Yönetim Sistemi
- ✓ Çalışanların iyileştirilmiş bilgi güvenliği performansının faydaları da dâhil Bilgi Güvenliği Yönetim Sisteminin etkinliğine yaptıkları katkı ve Bilgi Güvenliği Yönetim Sistemi şartlarına uyum sağlamamanın sonuçları

4.4.4. İletişim

Aksaray Üniversitesi Bilgi Güvenliği Yönetim Sistemi ile ilgili dâhili ve harici iletişim ihtiyaçlarını aşağıdaki hususları da içerecek şekilde BGYS/BF/001BGYS İlgili Taraf Beklentiler ve İletişim Formunda belirlemiştir.

- ✓ İletişimin konusu,
- ✓ Ne zaman iletişim kurulacağı,
- ✓ Kiminle iletişim kurulacağı,
- ✓ Kimin iletişim kuracağı ve
- ✓ İletişimin hangi süreçten etkileneceği

4.4.5. Yazılı Bilgiler

4.4.5.1. Genel

Aksaray Üniversitesi Bilgi Güvenliği Yönetim Sistemi aşağıdaki yazılı bilgileri içermektedir.

- ✓ ISO IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi standardının gerektirdiği yazılı bilgiler,
- ✓ Aksaray Üniversitesi tarafından Bilgi Güvenliği Yönetim Sisteminin etkinliği için gerekli olduğu belirlenen yazılı bilgiler.

4.4.5.2. Oluşturma ve Güncelleme

Aksaray Üniversitesi yazılı bilgileri oluşturma ve güncelleme ile ilgili hususları aşağıdakileri de içerecek şekilde BGYS/BP/04 Doküman ve Kayıtların Kontrolü Prosedüründe tanımlamış ve uygulamaktadır.

- ✓ Tanımlama ve tarif etme (örneğin, bir başlık, tarih, yazar veya referans numarası),
- ✓ Biçim (örneğin; dil, yazılım sürümü, grafikler) ve ortam (örneğin, kâğıt, elektronik),
- ✓ Uygunluğun ve doğruluğun gözden geçirilmesi ve onaylanması

4.4.5.3. Yazılı Bilgilerin Kontrolü

Aksaray Üniversitesi yazılı bilgilerin kontrolü ile ilgili hususları aşağıdakileri de içerecek şekilde BGYS/BP/04 Doküman ve Kayıtların Kontrolü Prosedüründe tanımlamış ve uygulamaktadır.

- ✓ Gereken yerde ve zamanda kullanım için erişilebilir ve uygun olması,
- ✓ Doğru bir şekilde korunması (örneğin, gizlilik kaybindan, uygun olmayan kullanımdan veya bütünlük kaybindan).
- ✓ Dağıtım, erişim, getirme ve kullanım,

Hazırlayan

Birim Kalite Sorumlusu

Yürürlük Onayı

Kalite Koordinatör Yardımcısı

Kalite Sistem Onayı

Kalite Koordinatörü



AKSARAY ÜNİVERSİTESİ BGYS PROSEDÜRÜ

Doküman No	BGYS-PR-001
İlk Yayın Tarihi	17.01.2022
Revizyon Tarihi	01.10.2024
Revizyon No	01
Sayfa No	8/27

- ✓ Okunaklılığın korunması da dâhil olmak üzere saklama ve koruma koşulları,
- ✓ Değişikliklerin kontrolü (örneğin sürüm kontrolü)
- ✓ Muhafaza etme ve yok etme.
- ✓ Bilgi Güvenliği Yönetim Sisteminin planlaması ve işletimi için gerekli olduğu belirlenen dış kaynaklı yazılı bilgilerin tespit edilmesi

4.5. İŞLETİM

4.5.1. İşletimsel Planlama ve Kontrol

Aksaray Üniversitesi Risk Değerlendirmesi, Risk İşleme ve Bilgi Güvenliği amaçları ve bu amaçları başarmak ile ilgili planlamalarını yapmış uygulamaktadır.

4.5.2. Bilgi Güvenliği Risk Değerlendirme

Aksaray Üniversitesi Bilgi Güvenliği Risk Değerlendirme kriterlerini de dikkate alarak, Bilgi Güvenliği Risk Değerlendirmelerini planlanan aralıklarda veya önemli değişiklikler önerildiğinde BGYS/BF/13 Risk Değerlendirme Formu ile gerçekleştirmekte ve kayıtlarını saklamaktadır.

4.5.3. Bilgi Güvenliği Risk İşleme

Aksaray Üniversitesi Risk değerlendirme sonuçlarını dikkate alarak bilgi güvenliği risk işleme faaliyetlerini BGYS/BF/13 Risk Değerlendirme Formu üzerinden gerçekleştirmekte ve kayıtlarını saklamaktadır.

4.6. PERFORMANS DEĞERLENDİRME

4.6.1. İzleme, Ölçme, Değerlendirme ve Analiz

Aksaray Üniversitesi bilgi güvenliği performansını ve Bilgi Güvenliği Yönetim Sisteminin etkinliğini aşağıdaki unsurları da içerecek şekilde BGYS/BF/002 BGYS Etkinlik Ölçümü ve Amaçları Formu ile takip etmekte ve kayıtlarını saklamaktadır.

- ✓ Bilgi güvenliği süreçleri ve kontrolleri dâhil olmak üzere neyin izlenmesi ve ölçülmesinin gerekli olduğu,
- ✓ Geçerli sonuçları temin etmek için, uygun İzleme, ölçme, analiz ve değerlendirme yöntemleri,
- ✓ İzleme ve ölçmenin ne zaman yapılacağı,
- ✓ İzlemeyi ve ölçmeyi kimin yapacağı,
- ✓ İzleme ve ölçme sonuçlarının ne zaman analiz edileceği ve değerlendirileceği ve
- ✓ Bu sonuçları kimin analiz edeceği ve değerlendireceği.

4.6.2. İç Tetkik

Aksaray Üniversitesi, Bilgi Güvenliği Yönetim Sisteminin, aşağıdaki hususları yerine getirip getirmediği konusunda bilgi elde etmek için planlanan aralıklarda BGYS/BP/05 İç Denetim Prosedürüne göre İç Tetkik gerçekleştirmekte ve yazılı bilgileri muhafaza etmektedir.

- ✓ Bilgi Güvenliği Yönetim Sisteminin ilgili standart şartlara, yasalara ve sözleşmelere uygun olup olmadığını,

Hazırlayan

Birim Kalite Sorumlusu

Yürürlük Onayı

Kalite Koordinatör Yardımcısı

Kalite Sistem Onayı

Kalite Koordinatörü



AKSARAY ÜNİVERSİTESİ BGYS PROSEDÜRÜ

Doküman No	BGYS-PR-001
İlk Yayın Tarihi	17.01.2022
Revizyon Tarihi	01.10.2024
Revizyon No	01
Sayfa No	9/27

- ✓ Etkin bir şekilde uygulanması ve sürdürülmesi

4.6.3. Yönetimin Gözden Geçirmesi

Aksaray Üniversitesi Üst Yönetimi, yılda en az bir kez Yönetim Gözden Geçirme Toplantısını Bilgi Güvenliği Yönetim Sisteminin sürekli uygunluğunu, doğruluğunu ve etkinliğini takip etmek amacıyla gerçekleştirir. Toplantıya ait kayıtlar saklanmaktadır.

Girdiler

- ✓ Önceki Yönetimin Gözden Geçirmelerinden gelen görevlerin durumu,
- ✓ Bilgi Güvenliği Yönetim Sistemini ilgilendiren dış ve iç konulardaki değişiklikler,
- ✓ Uygunsuzluklar ve Düzeltici Faaliyetler,
- ✓ İzleme ve ölçme sonuçları,
- ✓ Tetkik sonuçları ve Bilgi güvenliği amaçlarının yerine getirilmesi,
- ✓ İlgili taraflardan geri bildirimler,
- ✓ Risk değerlendirme sonuçları ve risk işleme planının durumu ve Sürekli iyileştirme için fırsatlar.

Çıktılar

- ✓ BGYS'nin etkinliğini iyileştirme,
- ✓ Risk değerlendirme ve risk işleme planını güncelleştirme,
- ✓ Gerekliğinde, BGYS üzerinde etkisi olabilecek iç ya da dış olaylara karşılık vermek için bilgi güvenliğini etkileyen prosedür ve kontrol değişiklikleri ve aşağıdaki konularla ilgili değişiklikler:
 - ✓ İş gereksinimleri,
 - ✓ Güvenlik gereksinimleri,
 - ✓ Mevcut iş gereksinimlerini etkileyen iş prosesleri,
 - ✓ Düzenleyici ya da yasal gereksinimler, anlaşma yükümlülükleri
 - ✓ Risk seviyeleri ve/veya risk Kabul kriterleri.
 - ✓ Kaynak ihtiyaçları,
 - ✓ Kontrollerin etkinliğinin nasıl ölçüldüğünü iyileştirme

4.7. İYİLEŞTİRME

4.7.1. Uygunsuzluk ve Düzeltici Faaliyet

Aksaray Üniversitesi bir uygunsuzluk oluştuğunda yapılacak faaliyetleri BGYS/BP/06 Düzeltici Faaliyetler Prosedüründe tanımlamış ve uygulamaktadır. Uygunsuzluk ve Düzeltici Faaliyetlere ilişkin kayıtlar saklanmaktadır.

4.7.2. Sürekli İyileştirme

Aksaray Üniversitesi Bilgi Güvenliği Yönetim Sisteminin uygunluğunu, doğruluğunu ve etkinliğini sürekli olarak iyileştirmektedir.

Hazırlayan

Birim Kalite Sorumlusu

Yürürlük Onayı

Kalite Koordinatör Yardımcısı

Kalite Sistem Onayı

Kalite Koordinatörü



AKSARAY ÜNİVERSİTESİ BGYS PROSEDÜRÜ

Doküman No	BGYS-PR-001
İlk Yayın Tarihi	17.01.2022
Revizyon Tarihi	01.10.2024
Revizyon No	01
Sayfa No	10/27

A. 5. BİLGİ GÜVENLİĞİ POLİTİKALARI

A.5.1. Bilgi Güvenliği İçin Yönetimin Yönlendirilmesi

A.5.1.1. Bilgi Güvenliği İçin Politikalar

Bilgi Güvenliği şartları, Bilgi Güvenliği Kurulu tarafından oluşturulmuş ve Aksaray Üniversitesi Üst Yönetim tarafından onaylanmış ve BGYS/POL/01 Bilgi Güvenliği Yönetim Sistemi Politikası adıyla kurum içi duyuru kanalları ile tüm çalışanlara ve firmamız web sayfası üzerinden tüm dış taraflara duyurulmuştur.

BGYS politikasını desteklemek için, bilgi güvenliği ile sınırlı kalmayacak şekilde aşağıda tanımlanan konular ile ilgili Bilgi Güvenliği Yönetim Sistemi Prosedürü ve talimatlar oluşturulmuştur. Politika, prosedür, talimat ve kılavuzlar elektronik ortamda bilmesi gereken prensibi çerçevesinde erişilebilir olacaktır.

- ✓ Bilgi Güvenliği Organizasyonu
- ✓ İnsan Kaynakları Güvenliği
- ✓ Erişim Kontrolü
- ✓ Varlık Yönetimi
- ✓ Kriptografi
- ✓ Fiziksel ve Çevresel Güvenlik
- ✓ İşletim Güvenliği
- ✓ Haberleşme Güvenliği
- ✓ Sistem Edinimi, Geliştirme ve Bakımı
- ✓ Tedarikçi İlişkileri
- ✓ Risk Yönetimi
- ✓ Bilgi Güvenliği İhlal Olayı Yönetimi
- ✓ İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları
- ✓ Uyum

A.5.1.2. Bilgi Güvenliği İçin Politikaların Gözden Geçirilmesi

Aksaray Üniversitesi Bilgi Güvenliği Yönetim Sistemi Politikası ve diğer yönetim sistemine ait politikaları organizasyonel değişiklikler iş şartları, yasal ve teknik düzenlemeler vb. nedenlerle günün koşullarına uyumluluk açısından elverişliliğinin ve etkinliğinin devam etme durumunu belirlemek için değerlendirir.

Bilgi Güvenliği Yönetim Sistemi Politikası ve yönetim sistemine ait diğer politikalar düzenli olarak en az yılda bir kez olmak koşulu ile belirgin değişiklikler olduğunda uygunluğunun elverişliliğinin ve etkinliğinin devam etme durumunu belirlemek için yönetim tarafından Yönetimin Gözden Geçirme Toplantısında gözden geçirilir. Gözden geçirme verileri, Bilgi Güvenliği Yöneticisi tarafından oluşturulur. Gözden geçirilen ve güncellenen BGYS şartları, firmamız yönetimi tarafından onaylandıktan sonra daha önce belirlenmiş kanallar yolu ile yayınlanır.

A.6 BİLGİ GÜVENLİĞİ ORGANİZASYONU

A.6.1 İç Organizasyon

A.6.1.1 Bilgi Güvenliği Roller ve Sorumlulukları

Aksaray Üniversitesi bilgi güvenliği rollerini ve sorumluluklarını BGYS/BP/09 Bilgi Güvenliği Organizasyonu Prosedüründe tanımlamış ve uygulamaktadır.

Hazırlayan	Yürürlük Onayı	Kalite Sistem Onayı
Birim Kalite Sorumlusu	Kalite Koordinatör Yardımcısı	Kalite Koordinatörü



AKSARAY ÜNİVERSİTESİ BGYS PROSEDÜRÜ

Doküman No	BGYS-PR-001
İlk Yayın Tarihi	17.01.2022
Revizyon Tarihi	01.10.2024
Revizyon No	01
Sayfa No	11/27

A.6.1.2 Görevlerin Ayrılığı

Çelişen görevler ve sorumluluklar, yetkilendirilmemiş veya kasıtsız değişiklik fırsatlarını veya kuruluş varlıklarının yanlış kullanımını azaltmak amacıyla ayrılması ile ilgili yöntemler BGYS/BP/09 Bilgi Güvenliği Organizasyonu Prosedüründe tanımlanmış ve uygulamaktadır.

A.6.1.3 Otoritelerle İletişim

Aksaray Üniversitesi ne zaman ve hangi otoritelerle (örneğin; yasa düzenleyici kurumlar, denetim otoriteleri) temas kurulacağını BGYS/BF/001 İlgili Taraf Beklentiler ve İletişim Formunda tanımlamıştır.

A.6.1.4 Özel İlgili Grupları ile İletişim

Özel ilgi grupları veya diğer uzman güvenlik forumları ve profesyonel dernekler ile sahip olunan bilgiyi geliştirmek ve en iyi uygulamalar ve ilgili güvenlik bilgileri hakkında güncel bilgi sahibi olmak için temas kurulacak kurumlar BGYS/BF/001 İlgili Taraf Beklentiler ve İletişim Formunda tanımlamıştır.

A.6.1.5 Proje Yönetiminde Bilgi Güvenliği

Yürütülen tüm projelerde Bilgi Güvenliği hususlarını göz önünde bulundurmaktadır. Projelerde gerekli kontrolleri belirlemek için projenin ilk safhalarında bilgi güvenliği risk belirlemesi ve değerlendirilmesi BGYS/BF/005 Proje Risk Yönetim Değerlendirme Test ve Kabul Formu ile yapılmakta ve bilgi güvenliği, uygulanan proje metodolojisinin tüm safhalarında dikkate alınmaktadır.

Proje'nin başlangıç, planlama, uygulama, izleme ve kapanış aşamalarında bilgi güvenliği ile ilgili riskler değerlendirilir.

Bilgi teknolojileri sistem, ağ altyapı ve yazılım geliştirme projelerinde bilgi güvenliği ile ilgili aşağıdaki hususlar dikkate alınmaktadır;

- ✓ Mevcut ya da yeni alınacak yazılımların kurulum ve geliştirme aşamaları, son kullanıcılara açılacak yeni ara yüzler, protokol değişiklikleri,
- ✓ Kimlik doğrulama mekanizmasındaki değişiklikler,
- ✓ Yeni sistem/sunucu kurulumu,
- ✓ Sunucu lokasyon/segment değişiklikleri,
- ✓ Network alt yapısı değişiklikleri,
- ✓ Kurumun aldığı kritik hizmetlerdeki değişiklikler, yenilemeler, vb. (müşteri, lokasyon, uygulama)
- ✓ Fiziksel ve çevresel güvenlik sistemlerindeki değişiklikler, (kamera, bariyer, turnike sistemleri, duvar, tel örgü vb.)
- ✓ Bilgi sistemleri güvenlik ürünleri (firewall, anti-virüs, anti-spam, IPSec, vb..) kurulumu ve değişiklikleri,

A.6.2 Mobil Cihazlar ve Uzaktan Çalışma

A.6.2.1 Mobil Cihaz Politikası

Aksaray Üniversitesi Mobil cihazların kullanımı ile ortaya çıkan risklerin (iş bilgilerinin ele geçirilmesi)

Hazırlayan	Yürürlük Onayı	Kalite Sistem Onayı
Birim Kalite Sorumlusu	Kalite Koordinatör Yardımcısı	Kalite Koordinatörü



AKSARAY ÜNİVERSİTESİ BGYS PROSEDÜRÜ

Doküman No	BGYS-PR-001
İlk Yayın Tarihi	17.01.2022
Revizyon Tarihi	01.10.2024
Revizyon No	01
Sayfa No	12/27

yönetilmesi amacı ile aşağıdaki hususları göz önünde bulundurarak alınması gereken güvenlik önlemlerini BGYS/BP/10 Mobil Cihazlar ve Uzaktan Çalışma Prosedüründe belirlemiş ve uygulamaktadır.

- ✓ Mobil cihazların kaydı,
- ✓ Fiziksel koruma için gereksinimler,
- ✓ Yazılım kurulum kısıtlaması,
- ✓ Mobil cihaz yazılım sürümleri ve yamaların uygulanması için gereksinimler
- ✓ Bilgi hizmetlerine bağlantı kısıtlaması,
- ✓ Erişim kontrolleri,
- ✓ Kriptografik teknikler,
- ✓ Kötücül yazılım koruması,
- ✓ Uzaktan devre dışı bırakma, silme ya da kilitleme,
- ✓ Yedekleme

A.6.2.2 Uzaktan Çalışma

Aksaray Üniversitesi, Uzaktan çalışma alanlarında erişilen, işlenen veya depolanan bilgiyi korumak amacı ile aşağıdaki hususları göz önünde bulundurarak alınması gereken güvenlik önlemlerini BGYS/BP/10 Mobil Cihazlar ve Uzaktan Çalışma Prosedüründe belirlemiş ve uygulamaktadır.

- ✓ Kuruluşun iç sistemlerine uzaktan erişim ihtiyacı, erişilecek ve haberleşme hattından geçirilecek bilginin hassasiyeti ve dâhili sistemin hassaslığı dikkate alınarak haberleşme güvenlik gereksinimleri,
- ✓ Kişiye ait teçhizat üzerindeki bilgilerin işlenmesini ve saklanmasını önleyen sanal masaüstü erişim izni
- ✓ Aynı ikametgâhı kullanan aile ve arkadaşlar gibi kişiler tarafından bilgi ve kaynaklara yetkisiz erişim tehdidi,
- ✓ Ev ağlarının kullanımı ve kablosuz ağ hizmetleri yapılandırmasında gereksinimler ya da kısıtlamalar,
- ✓ Kötücül yazılımdan koruma ve güvenlik duvarı gereksinimleri.

A.7 İNSAN KAYNAKLARI GÜVENLİĞİ

A.7.1 İstihdam Öncesi

A.7.1.1 Tarama

Tüm işe alınacak adaylar için ilgili yasa, düzenleme ve etiğe göre ve iş gereksinimleri, erişilecek bilginin sınıflandırması ve alınan risklerle orantılı olarak geçmiş doğrulama kontrolleri ile ilgili hususlar BGYS/BP/11 İnsan Kaynakları Güvenliği Prosedüründe tanımlanmıştır.

A.7.1.2 İstihdam Hüküm Koşulları

Çalışanlar ve yükleniciler ile kendilerinin ve Aksaray Üniversitesi bilgi güvenliği sorumluluklarını açıklamak için uygulanan yöntemler BGYS/BP/11 İnsan Kaynakları Güvenliği Prosedüründe açıklanmıştır.

Hazırlayan	Yürürlük Onayı	Kalite Sistem Onayı
Birim Kalite Sorumlusu	Kalite Koordinatör Yardımcısı	Kalite Koordinatörü



AKSARAY ÜNİVERSİTESİ BGYS PROSEDÜRÜ

Doküman No	BGYS-PR-001
İlk Yayın Tarihi	17.01.2022
Revizyon Tarihi	01.10.2024
Revizyon No	01
Sayfa No	13/27

A.7.2 Çalışma Esnasında

A.7.2.1 Yönetim Sorumlulukları

Aksaray Üniversitesi Üst Yönetimi, çalışanların ve yüklenicilerin bilgi güvenliği sorumlulukları hakkında bilgilendirilmesi ile ilgili hususlar BGYS/BP/11 İnsan Kaynakları Güvenliği Prosedüründe tanımlanmış ve uygulanmaktadır.

A.7.2.2 Bilgi Güvenliği Farkındalığı, Eğitim ve Öğretimi

Aksaray Üniversitesi Bilgi güvenliği farkındalığı, eğitim ve öğretimi ile ilgili hususları BGYS/BP/11 İnsan Kaynakları Güvenliği Prosedüründe tanımlanmış ve uygulanmaktadır.

A.7.2.3 Disiplin Prosesi

Bilgi güvenliği ihlal olayını gerçekleştiren çalışanlara yönelik uygulanacak yaptırım ve cezalara yönelik yöntem ve metotlar BGYS/BP/11 İnsan Kaynakları Güvenliği Prosedüründe tanımlanmış ve uygulanmaktadır.

A.7.3 İstihdamın Sonlandırılması veya Değiştirilmesi

A.7.3.1 İstihdam Sorumluluklarının Sonlandırılması veya Değiştirilmesi

İstihdamın sonlandırılması veya değiştirilmesi aşamalarında Aksaray Üniversitesi çıkarlarını korumak için gerekli BGYS/BP/11 İnsan Kaynakları Güvenliği Prosedüründe tanımlanmış ve uygulanmaktadır.

A.8 VARLIK YÖNETİMİ

A.8.1 Varlıkların Sorumluluğu

A.8.1.1 Varlık Envanteri

Aksaray Üniversitesi Bilgi ve Bilgi İşleme Tesisleri ile ilgili varlıklarını belirlemiş bu varlıklara ait envanterini Varlık Envanteri ve Değerleri Raporu oluşturmuştur. Varlıkların yaşam döngüsü (oluşturma, işleme, depolama, iletme, silme ve imha) kuralları BGYS/BP/02 Varlık Yönetimi Prosedüründe tanımlanmış ve uygulanmaktadır.

A.8.1.2 Varlıkların Sahipliği

Aksaray Üniversitesi Bilgi ve Bilgi İşleme Tesisleri ile ilgili tüm varlıklarının sahiplerini BGYS/BF/012 Varlık Envanteri ve Değerleri Formunda belirlemiştir. Varlık sahiplerinin sorumlulukları BGYS/BP/02 Varlık Yönetimi Prosedüründe tanımlanmıştır.

A.8.1.3 Varlıkların Kabul Edilebilir Kullanımı

Aksaray Üniversitesi Bilgi ve Bilgi İşleme Tesisleri ile ilgili bilgi ve varlıkların Kabul edilebilir kullanımına dair kuralları BGYS/BP/02 Varlık Yönetimi Prosedüründe tanımlanmış ve uygulanmaktadır.

A.8.1.4 Varlıkların İadesi

Tüm çalışanlar ve dış tarafların kullanıcıları, istihdamlarının, sözleşme veya anlaşmalarının sonlandırılmasının ardından ellerinde olan tüm kurumsal varlıkları iade etmesi ile ilgili yöntemler BGYS/BP/02 Varlık Yönetimi Prosedüründe tanımlanmış ve uygulanmaktadır.

A.8.2 Bilgi Sınıflandırma

A.8.2.1 Bilgilerin Sınıflandırılması

Bilgi yasal gereksinimler, değeri, kritikliği ve yetkisiz ifşa veya değiştirilmeye karşı hassasiyetine göre

Hazırlayan

Birim Kalite Sorumlusu

Yürürlük Onayı

Kalite Koordinatör Yardımcısı

Kalite Sistem Onayı

Kalite Koordinatörü



AKSARAY ÜNİVERSİTESİ BGYS PROSEDÜRÜ

Doküman No	BGYS-PR-001
İlk Yayın Tarihi	17.01.2022
Revizyon Tarihi	01.10.2024
Revizyon No	01
Sayfa No	14/27

BGYS/BP/02 Varlık Yönetimi Prosedüründe sınıflandırılmıştır. Bilgi gizliliği sınıflandırması aşağıdaki dört seviyeyi temel almaktadır:

- ✓ İfşa edilmesi durumunda hiçbir zarar olmaz,
- ✓ İfşa edilmesi durumunda küçük bir mahcubiyete ya da küçük bir sıkıntıya neden olur,
- ✓ İfşa edilmesi durumunda işlemler ya da taktik amaçlar üzerinde kısa vadeli etkiye neden olur,
- ✓ İfşa edilmesi stratejik hedefler üzerinde uzun vadeli etkiye neden olur ya da kuruluşun hayatiyetini risk altına sokar vb.

A.8.2.2 Bilgi Etiketleme

Bilgi etiketleme için kurallar benimsenen bilgi sınıflandırma düzenine göre BGYS/BP/02 Varlık Yönetimi Prosedüründe tanımlanmış ve uygulanmaktadır.

A.8.2.3 Varlıkların Kullanımı

Varlıkların kullanımı ile ilgili kurallar benimsenen bilgi sınıflandırma düzenine BGYS/BP/02 Varlık Yönetimi Prosedüründe tanımlanmış ve uygulanmaktadır.

A.8.3 Ortam İşleme

A.8.3.1 Taşınabilir Ortam Yönetimi

Taşınabilir ortam yönetimi için kurallar benimsenen bilgi sınıflandırma düzenine BGYS/BP/02 Varlık Yönetimi Prosedüründe tanımlanmış ve uygulanmaktadır.

A.8.3.2 Ortamın Yok Edilmesi

Ortamın artık ihtiyaç kalmadığında güvenli bir şekilde yok edilmesi ile ilgili kurallar BGYS/BP/02 Varlık Yönetimi Prosedüründe tanımlanmış ve uygulanmaktadır.

A.8.3.3 Fiziksel Ortam Aktarımı

Bilgi içeren ortamın, aktarım sırasında yetkisiz erişim, kötüye kullanım ve bozulmaya karşı korunması ile ilgili kurallar BGYS/BP/02 Varlık Yönetimi Prosedüründe tanımlanmış ve uygulanmaktadır.

A.9 ERİŞİM KONTROLÜ

A.9.1 Erişim Kontrolünün İş Gereklilikleri

A.9.1.1 Erişim Kontrol Politikası

Aksaray Üniversitesi Bilgi varlıklarına yönelik özel kullanıcı rolleri için ve ilişkili bilgi güvenliği risklerini yansıtan kontrolleri, erişim kontrol kurallarını, erişim haklarını ve kısıtlamalarını BGYS/BP/12 Erişim Kontrol Prosedüründe tanımlanmış ve uygulamaktadır. Erişim kontrolleri hem mantıksal hem de fiziksel olarak uygulanmaktadır.

A.9.1.2 Ağlara ve Ağ Hizmetlerine Erişim

Ağ ve ağ hizmetlerinin kullanımı, kullanıcılara sadece özellikle kullanımı için yetkilendirildikleri ağ ve ağ hizmetlerine erişim verilmesi ile ilgili kontroller BGYS/BP/12 Erişim Kontrol Prosedüründe tanımlanmış ve

Hazırlayan

Birim Kalite Sorumlusu

Yürürlük Onayı

Kalite Koordinatör Yardımcısı

Kalite Sistem Onayı

Kalite Koordinatörü



AKSARAY ÜNİVERSİTESİ BGYS PROSEDÜRÜ

Doküman No	BGYS-PR-001
İlk Yayın Tarihi	17.01.2022
Revizyon Tarihi	01.10.2024
Revizyon No	01
Sayfa No	15/27

uygulamaktadır.

A.9.2 Kullanıcı Erişim Yönetimi

A.9.2.1 Kullanıcıyı Kaydetme ve Kayıt Silme

Erişim haklarının atanmasını sağlamak için kullanıcı kaydetme ve kayıt silme prosesleri ile kullanıcı kimlik bilgisi yönetimine ait kontroller ve politikalar BGYS/BP/12 Erişim Kontrol Prosedüründe tanımlanmış ve uygulamaktadır.

A.9.2.2 Kullanıcı Erişimine İzin Verme

Kullanıcı kimliklerine verilen erişim haklarının atanması ya da iptali için gerekli politikalar BGYS/BP/12 Erişim Kontrol Prosedüründe tanımlanmış ve uygulamaktadır.

A.9.2.3 Ayrıcalıklı Erişim Haklarının Yönetimi

Ayrıcalıklı erişim haklarının kullanımı kısıtlanmış ve kontrol edilmektedir. Ayrıcalıklı erişim haklarının tahsisi ile ilgili yöntem ve hususlar BGYS/BP/12 Erişim Kontrol Prosedüründe tanımlanmış ve uygulamaktadır.

A.9.2.4 Kullanıcılara Ait Gizli Kimlik Doğrulama Bilgilerinin Yönetimi

Aksaray Üniversitesi, kullanıcılara ait gizli kimlik doğrulama bilgisinin tahsis edilmesi ile ilgili yöntem ve uygulamaları BGYS/BP/12 Erişim Kontrol Prosedüründe tanımlanmış ve uygulamaktadır.

A.9.2.5 Kullanıcı Erişim Haklarının Gözden Geçirilmesi

Aksaray Üniversitesi kullanıcı erişim haklarının gözden geçirilmesi ile ilgili yöntem ve uygulamaları BGYS/BP/12 Erişim Kontrol Prosedüründe tanımlanmış ve uygulamaktadır.

A.9.2.6 Erişim Haklarının Kaldırılması veya Düzenlenmesi

Tüm çalışanların ve dış taraf kullanıcılarının bilgi ve Bilgi İşleme Tesislerine erişim yetkilerinin, istihdamları, sözleşmeleri veya anlaşmaları sona erdirildiğinde kaldırılması veya yeniden düzenlenmesi ile ilgili yöntem ve uygulamalar BGYS/BP/12 Erişim Kontrol Prosedüründe tanımlanmış ve uygulanmaktadır.

A.9.3 Kullanıcı Sorumlulukları

A.9.3.1 Gizli Kimlik Doğrulama Bilgisinin Kullanımı

Kullanıcıların, gizli kimlik doğrulama bilgisinin kullanımında uygulaması gereken yöntem ve kurallar BGYS/BP/12 Erişim Kontrol Prosedüründe tanımlanmış ve uygulanmaktadır.

A.9.4 Sistem ve Uygulama Erişim Kontrolü

A.9.4.1 Bilgiye Erişimin Kısıtlanması

Bireysel iş uygulama gereksinimlerini temel Alan bilgi ve uygulama sistem fonksiyonlarına erişimlerin kısıtlanması ile ilgili yöntem ve kontroller BGYS/BP/12 Erişim Kontrol Prosedüründe tanımlanmış ve uygulamaktadır.

Hazırlayan

Birim Kalite Sorumlusu

Yürürlük Onayı

Kalite Koordinatör Yardımcısı

Kalite Sistem Onayı

Kalite Koordinatörü



AKSARAY ÜNİVERSİTESİ BGYS PROSEDÜRÜ

Doküman No	BGYS-PR-001
İlk Yayın Tarihi	17.01.2022
Revizyon Tarihi	01.10.2024
Revizyon No	01
Sayfa No	16/27

A.9.4.2 Güvenli Oturum Açma Prosedürleri

Yetkisiz kullanıcılara yardım sağlamaktan kaçınmak, oturum açılırken sistem ya da uygulama hakkında en az bilgiyi açığa çıkarmak, yetkisiz erişim fırsatlarını asgari düzeye indirmek, bir kullanıcının iddia edilen kimliğini kanıtlamak için gerekli olan güvenli oturum açma ve uygun kimlik doğrulama yöntemleri ile ilgili uygulanabilir tüm sistemlerde kontroller ve uygulamalar BGYS/BP/12 Erişim Kontrol Prosedüründe tanımlanmış ve uygulamaktadır.

A.9.4.3 Parola Yönetim Sistemi

Etkileşimli parola yönetiminin sağlanması ve kaliteli parolaların kullanılması ile ilgili uygulanacak yöntem ve kurallar BGYS/BP/12 Erişim Kontrol Prosedüründe tanımlanmış ve uygulamaktadır.

A.9.4.4 Ayrıcalıklı Destek Programlarının Kullanımı

Sistem ve uygulamaların kontrollerini geçersiz kılma yeteneğine sahip olabilen destek programlarının kullanımı ile ilgili uygulanacak yöntemler ve kontroller BGYS/BP/12 Erişim Kontrol Prosedüründe tanımlanmış ve uygulamaktadır.

A.9.4.5 Program Kaynak Koduna Erişim Kontrolü

Program kaynak kodu ve ilgili öğelere (tasarımlar, özellikler, doğrulama planları ve geçiş planları gibi) erişim, yetkisiz işlevsellik girişini ve istenmeyen değişiklikleri önlemenin yanı sıra değerli fikri mülkiyet haklarının gizliliğini sağlamak için uygulanacak yöntemler ve kontroller BGYS/BP/12 Erişim Kontrol Prosedüründe tanımlanmış ve uygulamaktadır.

A.10 KRİPTOGRAFİ ERİŞİM KONTROLÜ

A.10.1 Kriptografik Kontroller

A.10.1.1 Kriptografik Kontrollerin Kullanımına İlişkin Politika

Aksaray Üniversitesi Bilginin korunmasına ilişkin kullanacağı kriptografik kontroller ile ilgili yöntem ve uygulamaları BGYS/BP/13 Kriptografi Prosedüründe tanımlanmış ve uygulamaktadır.

A.10.1.2 Anahtar Yönetimi

Aksaray Üniversitesi Kriptografik anahtarların kullanımı, korunması ve yaşam süresine dair gerekli yöntem ve metotları BGYS/BP/13 Kriptografi Prosedüründe tanımlanmış ve kriptografik anahtarların tüm yaşam süresince uygulamaktadır.

A.11 FİZİKSEL VE ÇEVRESEL GÜVENLİK

A.11.1 Güvenli Alanlar

A.11.1.1 Fiziksel Güvenlik Sınırı

Aksaray Üniversitesi Hassas veya kritik bilgi ve Bilgi İşleme Tesislerini barındıran alanlarını korumak için güvenlik sınırlarını ve koruma tedbirlerine ilişkin kontrolleri BGYS/BP/14 Fiziksel ve Çevresel Güvenlik Prosedüründe tanımlanmış ve uygulamaktadır.

Hazırlayan

Birim Kalite Sorumlusu

Yürürlük Onayı

Kalite Koordinatör Yardımcısı

Kalite Sistem Onayı

Kalite Koordinatörü



AKSARAY ÜNİVERSİTESİ BGYS PROSEDÜRÜ

Doküman No	BGYS-PR-001
İlk Yayın Tarihi	17.01.2022
Revizyon Tarihi	01.10.2024
Revizyon No	01
Sayfa No	17/27

A.11.1.2 Fiziksel Giriş Kontrolleri

Aksaray Üniversitesi Güvenli alanlara sadece yetkili personele erişim izni verilmesi için gerekli uygun giriş kontrollerini BGYS/BP/14 Fiziksel ve Çevresel Güvenlik Prosedüründe tanımlamış ve uygulamaktadır.

A.11.1.3 Ofislerin, Odaların ve Tesislerin Güvenliğinin Sağlanması

Aksaray Üniversitesi Ofislerin, odaların ve tesislerin fiziksel güvenliğinin sağlanması için gerekli kontrollerini BGYS/BP/14 Fiziksel ve Çevresel Güvenlik Prosedüründe tanımlamış ve uygulamaktadır.

A.11.1.4 Dış ve Çevresel Tehditlere Karşı Koruma

Aksaray Üniversitesi Güvenli alanların Doğal felaketler, iklim değişikliği, kötü niyetli saldırılar veya kazalara karşı fiziksel olarak korunmasına yönelik kontrolleri BGYS/BP/14 Fiziksel ve Çevresel Güvenlik Prosedüründe tanımlamış ve uygulamaktadır.

A.11.1.5 Güvenli Alanlarda Çalışma

Aksaray Üniversitesi, Güvenli alanlarda çalışma için gerekli kontrollerini BGYS/BP/14 Fiziksel ve Çevresel Güvenlik Prosedüründe tanımlamış ve uygulamaktadır.

A.11.1.6 Teslimat ve Yükleme Alanları

Aksaray Üniversitesi, Yetkisiz kişilerin tesise giriş yapabildiği, teslimat ve yükleme alanları gibi erişim noktalarının kontrolü ve bu noktalardan Bilgi İşleme Tesislerine yetkisiz erişimi engellemek gerekli kontrollerini BGYS/BP/14 Fiziksel ve Çevresel Güvenlik Prosedüründe tanımlamış ve uygulamaktadır.

A.11.2 Teçhizat

A.11.2.1 Teçhizat Yerleştirme ve Koruma

Aksaray Üniversitesi, Teçhizatın çevresel tehditlerden ve tehlikelerden ve yetkisiz erişim fırsatlarından kaynaklanan riskleri azaltacak şekilde yerleştirilmesi ilişkin kontrolleri BGYS/BP/14 Fiziksel ve Çevresel Güvenlik Prosedüründe tanımlamış ve uygulamaktadır.

A.11.2.2 Destekleyici Alt Yapı Hizmetleri

Aksaray Üniversitesi, Teçhizat destekleyici altyapı hizmetlerindeki hatalardan kaynaklanan enerji kesintileri ve diğer kesintilerden korunmaya ilişkin kontrolleri BGYS/BP/14 Fiziksel ve Çevresel Güvenlik Prosedüründe tanımlamış ve uygulamaktadır.

A.11.2.3 Kablo Güvenliği

Aksaray Üniversitesi, Veri veya destekleyici bilgi hizmetlerini taşıyan enerji ve iletişim kablolarının, dinleme, girişim oluşturma veya hasara karşı korunmasına ilişkin kontrolleri BGYS/BP/14 Fiziksel ve Çevresel Güvenlik Prosedüründe tanımlamış ve uygulamaktadır.

Hazırlayan

Birim Kalite Sorumlusu

Yürürlük Onayı

Kalite Koordinatör Yardımcısı

Kalite Sistem Onayı

Kalite Koordinatörü



AKSARAY ÜNİVERSİTESİ BGYS PROSEDÜRÜ

Doküman No	BGYS-PR-001
İlk Yayın Tarihi	17.01.2022
Revizyon Tarihi	01.10.2024
Revizyon No	01
Sayfa No	18/27

A.11.2.4 Teçhizat Bakımı

Aksaray Üniversitesi Teçhizatın sürekli erişilebilirliğini ve bütünlüğünü temin etmek için bakımları ile ilgili yöntem ve uygulamaları BGYS/BP/14 Fiziksel ve Çevresel Güvenlik Prosedüründe tanımlamış ve uygulamaktadır.

A.11.2.5 Varlıkların Taşınması

Teçhizatın, ön yetkilendirme olmaksızın kuruluş dışına çıkarılmaması ile ilgili kontrol ve önlemlerini BGYS/BP/14 Fiziksel ve Çevresel Güvenlik Prosedüründe tanımlamış ve uygulamaktadır.

A.11.2.6 Teçhizat ve Kuruluş Dışındaki Varlıkların Güvenliği

Kuruluş dışındaki varlıklara, kuruluş yerleşkesi dışında çalışmanın farklı riskleri de göz önünde bulundurularak güvenlik uygulanması ile ilgili kontrol ve önlemler BGYS/BP/14 Fiziksel ve Çevresel Güvenlik Prosedüründe tanımlamış ve uygulamaktadır.

A.11.2.7 Teçhizatın Güvenli Olarak Yok Edilmesi ya da Tekrar Kullanımı

Depolama ortamı içeren teçhizatların tüm parçaları, yok etme veya tekrar kullanımdan önce tüm hassas verilerin ve lisanslı yazılımların kaldırılmasını veya güvenli bir şekilde üzerine yazılmasını temin etmek amacıyla uygulanacak kontroller ve uygulamalar BGYS/BP/14 Fiziksel ve Çevresel Güvenlik Prosedüründe tanımlanmış ve uygulamaktadır.

A.11.2.8 Gözetimsiz Kullanıcı Teçhizatı

Gözetimsiz teçhizatın korunmasını temin etmek amacıyla, tüm kullanıcıların sorumlulukları BGYS/BP/14 Fiziksel ve Çevresel Güvenlik Prosedüründe tanımlanmış ve uygulamaktadır.

A.11.2.9 Temiz Masa Temiz Ekran Politikası

Kâğıtlar ve taşınabilir depolama ortamları için bir temiz masa politikası ve Bilgi İşleme Tesisleri için bir temiz ekran politikası BGYS/BP/14 Fiziksel ve Çevresel Güvenlik Prosedüründe tanımlanmış ve uygulamaktadır.

A.12 İŞLETİM GÜVENLİĞİ

A.12.1 İşletim Prosedürleri ve Sorumlulukları

A.12.1.1 Yazılı İşletim Prosedürleri

Yedekleme, teçhizat bakımı, ortam işleme, elektronik posta işleme yönetimi gibi bilgi işleme ve iletişim araçları ile ilişkili işletim faaliyetleri BGYS/BP/15 İşletim Güvenliği Prosedüründe tanımlanmış ve uygulamaktadır.

A.12.1.2 Değişiklik Yönetimi

Bilgi güvenliğini etkileyen iş prosesleri, Bilgi İşleme Tesisleri ve sistemlerdeki değişikliklerin kontrol edilmesi ile ilgili kontroller ve yöntemler BGYS/BP/15 İşletim Güvenliği Prosedüründe tanımlanmış ve uygulamaktadır.

A.12.1.3 Kapasite Yönetimi

Sistem kaynaklarının kullanımı izlenmekte ve gerekli sistem performansını temin etmek için gelecekteki kapasite

Hazırlayan

Birim Kalite Sorumlusu

Yürürlük Onayı

Kalite Koordinatör Yardımcısı

Kalite Sistem Onayı

Kalite Koordinatörü



AKSARAY ÜNİVERSİTESİ BGYS PROSEDÜRÜ

Doküman No	BGYS-PR-001
İlk Yayın Tarihi	17.01.2022
Revizyon Tarihi	01.10.2024
Revizyon No	01
Sayfa No	19/27

gereksinimleri ile ilgili kestirimler yapılmaktadır. Kapasite planlaması ile ilgili hususlar BGYS/BP/15 İşletim Güvenliği Prosedüründe tanımlanmış ve uygulamaktadır.

A.12.1.4 Geliştirme, Test ve İşletim Ortamlarının Birbirinden Ayrılması

Geliştirme, test ve işletim ortamları, yetkisiz erişim veya işletim ortamlarında değişiklik risklerinin azaltılması için birbirinden ayrılması ile ilgili kontroller BGYS/BP/15 İşletim Güvenliği Prosedüründe tanımlanmış ve uygulamaktadır.

A.12.2 Kötücül Yazılımlardan Korunma

A.12.2.1 Kötücül Yazılımlara Karşı Kontroller

Kötücül yazılımlardan korunmak için tespit etme, engelleme ve kurtarma ile ilgili kontroller BGYS/BP/15 İşletim Güvenliği Prosedüründe tanımlanmış ve uygulamaktadır.

A.12.3 Yedekleme

A.12.3.1 Bilgi Yedekleme

Bilgi yazılım ve sistem imajlarının yedekleme kopyalarının alınması ve alınan yedeklerin düzenli olarak test edilmesi ile ilgili yöntemler ve kurallar BGYS/BP/15 İşletim Güvenliği Prosedüründe tanımlanmış ve uygulamaktadır.

A.12.4 Kaydetme ve İzleme

A.12.4.1 Olay Kaydetme

Kullanıcı faaliyetlerinin, istisnai durumların, hataların ve bilgi güvenliği olaylarına ait olay kayıtlarının tutulması, saklanması ve düzenli olarak gözden geçirilmesi ile ilgili yöntemler ve kurallar BGYS/BP/15 İşletim Güvenliği Prosedüründe tanımlanmış ve uygulamaktadır.

Olay kayıtları

- ✓ Kullanıcı kimlikleri,
- ✓ Sistem faaliyetleri,
- ✓ Oturum açma ve oturum kapatma gibi anahtar olayların tarihleri, saatleri ve detayları,
- ✓ Başarılı ve reddedilmiş, sistem erişim girişimlerinin kayıtları,
- ✓ Başarılı ve reddedilmiş, veri ve diğer kaynaklara erişim girişimlerinin kayıtları,
- ✓ Sistem yapılandırma değişiklikleri,
- ✓ Ayrıcalıkların kullanımı,
- ✓ Erişilen dosyalar ve erişim türü,
- ✓ Ağ adresi ve protokolleri,
- ✓ Uygulamalarda kullanıcılar tarafından yürütülen işlemlerin kayıtları.

A.12.4.2 Kayıt Bilgisinin Korunması

Kayıt bilgilerinin kurcalama ve yetkisiz erişime karşı korunması ile ilgili kontroller BGYS/BP/15 İşletim Güvenliği Prosedüründe tanımlanmış ve uygulamaktadır.

Hazırlayan

Birim Kalite Sorumlusu

Yürürlük Onayı

Kalite Koordinatör Yardımcısı

Kalite Sistem Onayı

Kalite Koordinatörü



AKSARAY ÜNİVERSİTESİ BGYS PROSEDÜRÜ

Doküman No	BGYS-PR-001
İlk Yayın Tarihi	17.01.2022
Revizyon Tarihi	01.10.2024
Revizyon No	01
Sayfa No	20/27

A.12.4.3 Yönetici ve Operatör Kayıtları

Sistem yöneticileri ve sistem operatörlerinin faaliyetlerinin kayıt altına alınması, korunması ve düzenli aralıklarla gözden geçirilmesi ile ilgili yöntemler BGYS/BP/15 İşletim Güvenliği Prosedüründe ve uygulamaktadır.

A.12.4.4 Saat Senkronizasyonu

Tüm ilgili bilgi işleme sistemlerinin saatleri tek bir referans zaman kaynağına göre senkronize edilmesi ile ilgili yöntemler BGYS/BP/15 İşletim Güvenliği Prosedüründe tanımlanmış ve uygulamaktadır.

A.12.5 İşletimsel Yazılımın Kontrolü

A.12.5.1 İşletimdeki Sistemler Üzerine Yazılım Kurulumu

İşletimdeki sistemler üzerine yazılım kurulumu ilgili yöntemler ve kurallar BGYS/BP/15 İşletim Güvenliği Prosedüründe tanımlanmış ve uygulamaktadır.

A.12.6 Teknik Açıklıkların Yönetilmesi

A.12.6.1 Teknik Açıkların Yönetimi

Kullanılmakta olan bilgi sistemlerinin teknik açıklıklarına dair bilginin zamanında elde edilmesi, bu tür açıklıklara karşı zafiyetlerin değerlendirilmesi ve ilgili riskin ele alınması için gerekli tedbirler ve uygulamalar BGYS/BP/15 İşletim Güvenliği Prosedüründe tanımlanmış ve uygulamaktadır.

A.12.6.2 Yazılım Kurulumu Kısıtlamaları

Kullanıcıların en az ayrıcalık ilkesi uygulanarak hangi yazılım türünü kurabilecekleri ve/veya kuramayacakları ile ilgili hususlar BGYS/BP/15 İşletim Güvenliği Prosedüründe tanımlanmış ve uygulamaktadır.

A.12.7 Bilgi Sistemleri Tetkik Hususları

A.12.7.1 Bilgi Sistemleri Tetkik Kontrolleri

İşletimdeki sistemlerin doğrulanmasını kapsayan tetkik gereksinimlerin ve faaliyetlerin iş proseslerindeki kesintileri, asgariye indirmek için planlanması ile ilgili yöntemler BGYS/BP/15 İşletim Güvenliği Prosedüründe tanımlanmış ve uygulamaktadır.

A.13 HABERLEŞME GÜVENLİĞİ

A.13.1 Ağ Güvenliği Yönetimi

A.13.1.1 Ağ Kontrolleri

Sistemlerdeki ve uygulamalardaki bilgiyi korumak amacıyla ağların yönetilmesi ve kontrol edilmesi ilgili yöntem ve kurallar BGYS/BP/16 Haberleşme Güvenliği Prosedüründe tanımlanmış ve uygulamaktadır.

A.13.1.2 Ağ Hizmetlerinin Güvenliği

Ağ hizmetlerinin güvenliği ile ilgili yöntem ve kurallar BGYS/BP/16 Haberleşme Güvenliği Prosedüründe tanımlanmış ve uygulamaktadır.

Hazırlayan

Birim Kalite Sorumlusu

Yürürlük Onayı

Kalite Koordinatör Yardımcısı

Kalite Sistem Onayı

Kalite Koordinatörü



AKSARAY ÜNİVERSİTESİ BGYS PROSEDÜRÜ

Doküman No	BGYS-PR-001
İlk Yayın Tarihi	17.01.2022
Revizyon Tarihi	01.10.2024
Revizyon No	01
Sayfa No	21/27

A.13.1.3 Ağlarda Ayrım

Sistemlerdeki ve uygulamalardaki bilgiyi korumak amacıyla ağların yönetilmesi ve kontrol edilmesi ilgili yöntem ve kurallar BGYS/BP/16 Haberleşme Güvenliği Prosedüründe tanımlanmış ve uygulamaktadır.

A.13.2 Bilgi Transferi

A.13.2.1 Bilgi Transfer Politikaları ve Prosedürleri

Tüm iletişim olanağı türlerinin kullanımıyla bilgi transferini korumak amacıyla bilgi transferi için haberleşme tesisleri kullanımına yönelik yöntem ve kurallar BGYS/BP/16 Haberleşme Güvenliği Prosedüründe tanımlanmış ve uygulamaktadır.

A.13.2.2 Bilgi Transferindeki Anlaşmalar

Aksaray Üniversitesi ve dış taraflar arasında; iş bilgilerinin güvenli transferini, dış taraf sorumluluklarını, hassas bilginin (korunacak bilgi) tanımını ve korunması ile ihlal olaylarındaki sorumluluk ve yükümlülükleri içeren gizlilik sözleşmesi oluşturulmuş, tüm hizmet tedarikçilerine ve üçüncü taraflara imzalatılmaktadır.

A.13.2.3 Elektronik Mesajlaşma

Elektronik mesajlaşmadaki bilginin korunmasına yönelik yöntem ve kurallar BGYS/BP/16 Haberleşme Güvenliği Prosedüründe tanımlanmış ve uygulamaktadır.

A.13.2.4 Gizlilik ya da İfşa Etmeme Anlaşmaları

Bilginin korunması için gerekli kurallar, sorumluluklar, yaptırımlar Gizlilik Sözleşmelerinde tanımlanmış, tüm Firma ve Tedarikçi Çalışanları ile Üçüncü Taraflara imzalatılmaktadır.

A.14 SİSTEM EDİNİMİ, GELİŞTİRME VE BAKIMI

A.14.1 Bilgi Sistemlerinin Güvenlik Gereksinimleri

A.14.1.1 Bilgi Güvenliği Gereksinimleri Analizi ve Belirtimi

Yeni ya da var olan bilgi sistemlerinin bilgi güvenliği ile ilgili gereksinimlerinin belirlenmesi ve uygulanması ile ilgili yöntem ve kurallar BGYS/BP/17 Sistem Temini, Geliştirme ve Bakım Prosedüründe tanımlanmış ve uygulamaktadır.

A.14.1.2 Halka Açık Ağlarda Uygulama Hizmetlerinin Güvenliğinin Sağlanması

Halka açık ağlar üzerinden geçen uygulama hizmetlerindeki bilginin, hileli faaliyetlerden, sözleşme ihtilafından ve yetkisiz ifşadan ve değiştirmeden korunmasına yönelik yöntem ve kurallar BGYS/BP/17 Sistem Temini, Geliştirme ve Bakım Prosedüründe tanımlanmış ve uygulamaktadır.

A.14.1.3 Uygulama Hizmet İşlemlerinin Korunması

Uygulama hizmet işlemlerindeki bilginin; eksik iletme, yanlış yönlendirmeye, yetkisiz mesaj değiştirmeye, yetkisiz ifşaya, yetkisiz mesaj çoğaltmaya ya da mesajı yeniden oluşturmaya karşı korunması için gerekli yöntem ve kurallar BGYS/BP/17 Sistem Temini, Geliştirme ve Bakım Prosedüründe tanımlanmış ve uygulamaktadır.

Hazırlayan

Birim Kalite Sorumlusu

Yürürlük Onayı

Kalite Koordinatör Yardımcısı

Kalite Sistem Onayı

Kalite Koordinatörü



AKSARAY ÜNİVERSİTESİ BGYS PROSEDÜRÜ

Doküman No	BGYS-PR-001
İlk Yayın Tarihi	17.01.2022
Revizyon Tarihi	01.10.2024
Revizyon No	01
Sayfa No	22/27

A.14.2 Geliştirme ve Destek Proseslerinde Güvenlik

A.14.2.1 Güvenli Geliştirme Politikası

Güvenli yazılım geliştirme kuralları BGYS/BP/17 Sistem Temini, Geliştirme ve Bakım Prosedüründe belirlenmiş ve uygulanmaktadır. Geliştirme dış kaynaklı ise, güvenli geliştirme için bu kuralların dış tarafça uygulandığı kontrol ve takip edilmektedir.

Yeni ve güncellenmiş sistemler geliştirme süreci boyunca teste ve doğrulamaya tabi tutulmaktadır.

- ✓ Geliştirme ortamının güvenliği,
- ✓ Yazılım geliştirme yaşam döngüsü içinde güvenlik konusunda kılavuzluk,
- ✓ Yazılım geliştirme metodolojisinde güvenlik,
- ✓ Tasarım aşamasında güvenlik gereksinimleri,
- ✓ Proje aşamaları içinde güvenlik kontrol noktaları,
- ✓ Geliştiricilerin güvenlik açıklıklarını kaçınma, bulma ve onarma yeteneği.

A.14.2.2 Sistem Değişiklik Kontrolü Prosedürleri

Geliştirme yaşam döngüsü içerisindeki sistem değişikliklerinin takip edilmesi ile ilgili gerekli kural ve yöntemler BGYS/BP/17 Sistem Temini, Geliştirme ve Bakım Prosedüründe belirlenmiş ve uygulanmaktadır.

A.14.2.3 İşletim Platformu Değişikliklerinden Sonra Uygulamaların Teknik Gözden Geçirilmesi

İşletim platformları değiştirildiğinde, kurumsal işlemlere ya da güvenliğe hiçbir kötü etkisi olmamasını sağlamak amacıyla iş kritik uygulamalar gözden geçirilmesi ve test edilmesi ile ilgili gerekli kural ve yöntemler BGYS/BP/17 Sistem Temini, Geliştirme ve Bakım Prosedüründe belirlenmiş ve uygulanmaktadır.

- ✓ İşletim platformu değişikliklerinden zarar görmediğinden emin olmak için uygulama kontrol ve bütünlük prosedürlerinin gözden geçirilmesi,
- ✓ İşletim platformu değişikliklerine ilişkin uygulama öncesinde, uygun test ve gözden geçirmelere imkân tanımak için değişiklik bildirimlerinin zamanda yapılmasının temin edilmesi,
- ✓ İş sürekliliği planlarına ilişkin uygun değişikliklerin yapılmasının temin edilmesi

A.14.2.4 Yazılım Paketlerindeki Değişikliklerdeki Kısıtlamalar

Yazılım paketlerine yapılacak değişikliklerin gerek duyulanlar hariç önlenmesi ve tüm değişikliklerin sıkı bir biçimde kontrol edilmesi ile ilgili gerekli kural ve BGYS/BP/17 Sistem Temini, Geliştirme ve Bakım Prosedüründe belirlenmiş ve uygulanmaktadır.

A.14.2.5 Güvenli Sistem Mühendisliği Esasları

Aksaray Üniversitesi Güvenli sistem mühendisliği esasları BGYS/BP/17 Sistem Temini, Geliştirme ve Bakım Prosedüründe belirlemiş, yazılı hale getirmiş ve uygulamaktadır.

A.14.2.6 Güvenli Geliştirme Ortamı

Aksaray Üniversitesi tüm sistem geliştirme yaşam döngüsünü kapsayan sistem geliştirme ve bütünleştirme girişimleri için güvenli geliştirme ortamlarının kurulması ve uygun bir şekilde korunması ile ilgili gerekli yöntem ve kuralları BGYS/BP/17 Sistem Temini, Geliştirme ve Bakım Prosedüründe belirlemiş, yazılı hale getirmiş ve uygulamaktadır.

Hazırlayan

Birim Kalite Sorumlusu

Yürürlük Onayı

Kalite Koordinatör Yardımcısı

Kalite Sistem Onayı

Kalite Koordinatörü



AKSARAY ÜNİVERSİTESİ BGYS PROSEDÜRÜ

Doküman No	BGYS-PR-001
İlk Yayın Tarihi	17.01.2022
Revizyon Tarihi	01.10.2024
Revizyon No	01
Sayfa No	23/27

A.14.2.7 Dışarıdan Sağlanan Geliştirme

Aksaray Üniversitesi dışarıdan sağlanan sistem geliştirme faaliyetinin denetlenmesi ve izlenmesi ile ilgili gerekli yöntem ve kuralları BGYS/BP/17 Sistem Temini, Geliştirme ve Bakım Prosedüründe belirlemiş, yazılı hale getirmiş ve uygulamaktadır.

A.14.2.8 Sistem Güvenlik Testi

Aksaray Üniversitesi Kabul test programları ve ilgili kriterleri, yeni bilgi sistemleri, yükseltmeler ve yeni versiyonlar için BGYS/BP/17 Sistem Temini, Geliştirme ve Bakım Prosedüründe belirlemiş, yazılı hale getirmiş ve uygulamaktadır.

A.14.3 Test Verisi

A.14.3.1 Test Verisinin Korunması

Test verisinin dikkatli bir şekilde seçilmesi, korunması ve kontrol edilmesi ile ilgili yöntem ve kuralları BGYS/BP/17 Sistem Temini, Geliştirme ve Bakım Prosedüründe belirlenmiş ve uygulanmaktadır.

A.15 TEDARİKÇİ İLİŞKİLERİ

A.15.1 Tedarikçi İlişkilerinde Bilgi Güvenliği

A.15.1.1 Tedarikçi İlişkileri İçin Bilgi Güvenliği Yönetim Sistemi Politikası

Aksaray Üniversitesi bilgi varlıklarına (bilgilerine) tedarikçilerin erişimi ile ilgili riskleri azaltmak için gerekli bilgi güvenliği gereksinimleri BGYS/BP/18 Tedarikçi İlişkileri Prosedüründe tanımlanmış ve uygulanmaktadır.

A.15.1.2 Tedarikçi Anlaşmalarında Güvenliği İfade Etme

Aksaray Üniversitesi ile tedarikçileri arasında yanlış anlaşılma olasılığını kaldırmak, bilgi varlıklarına (bilgilerine) erişebilen, bunu işletebilen, depolayabilen, iletebilen veya bilgi teknolojileri altyapı bileşenlerini temin edebilen tedarikçiler ile gerekli tüm bilgi güvenliği gereksinimlerini karşılamak için her iki tarafın yükümlülüklerinden emin olmak amacıyla tedarikçi anlaşmaları ve gizlilik sözleşmeleri yapılmaktadır. Tespit edilen bilgi güvenliği gereksinimlerini karşılamak için anlaşmalara dahil edilen konular BGYS/BP/18 Tedarikçi İlişkileri Prosedüründe tanımlanmış ve uygulanmaktadır.

A.15.1.3 Bilgi ve İletişim Teknolojileri Tedarik Zinciri

Tedarikçiler ile yapılan anlaşmalarda, bilgi ve iletişim teknolojileri hizmetleri ve ürün tedarik zinciri ile ilgili bilgi güvenliği risklerini ifade eden şartlar BGYS/BP/18 Tedarikçi İlişkileri Prosedüründe belirlenmiş ve tedarikçi sözleşmelerinde de uygulanmaktadır.

A.15.2 Tedarikçi Hizmetleri Sağlama Yönetimi

A.15.2.1 Tedarikçi Hizmetlerini İzleme ve Gözden Geçirme

Aksaray Üniversitesi Tedarikçi hizmet sunumlarının izlenmesi, gözden geçirilmesi ve tetkik edilmesi ile ilgili yöntem ve metotları BGYS/BP/18 Tedarikçi İlişkileri Prosedüründe tanımlanmış ve uygulanmaktadır.

Hazırlayan

Birim Kalite Sorumlusu

Yürürlük Onayı

Kalite Koordinatör Yardımcısı

Kalite Sistem Onayı

Kalite Koordinatörü



AKSARAY ÜNİVERSİTESİ BGYS PROSEDÜRÜ

Doküman No	BGYS-PR-001
İlk Yayın Tarihi	17.01.2022
Revizyon Tarihi	01.10.2024
Revizyon No	01
Sayfa No	24/27

A.15.2.2 Tedarikçi Hizmetlerindeki Değişiklikleri Yönetme

Aksaray Üniversitesi Tedarikçi hizmetlerinde değişiklikleri yönetmek için gerekli yöntem ve kuralları BGYS/BP/18 Tedarikçi İlişkileri Prosedüründe tanımlanmış ve uygulamaktadır.

A.16 BİLGİ GÜVENLİĞİ İHLAL OLAYI YÖNETİMİ

A.16.1 Bilgi Güvenliği İhlal Olaylarının ve İyileştirmelerin Yönetimi

A.16.1.1 Sorumluluklar ve Prosedürler

Aksaray Üniversitesi Bilgi güvenliği ihlal olaylarına hızlı, etkili ve düzenli bir yanıt verilmesini sağlamak için gerekli yöntem ve kuralları BGYS/BP/19 Bilgi Güvenliği İhlal Olayı Yönetimi Prosedüründe tanımlanmış ve uygulamaktadır.

A.16.1.2 Bilgi Güvenliği Olaylarının Raporlanması

Aksaray Üniversitesi Bilgi Güvenliği İhlal Olaylarının uygun yönetim kanalları aracılığı ile olabildiğince hızlı bir şekilde raporlanması için gerekli yöntem ve kuralları BGYS/BP/19 Bilgi Güvenliği İhlal Olayı Yönetimi Prosedüründe tanımlanmış ve uygulamaktadır.

A.16.1.3 Bilgi Güvenliği Açıklıklarının Raporlanması

Aksaray Üniversitesi Bilgi sistemlerini ve hizmetlerini kullanan çalışanlardan ve yüklenicilerden, sistemler veya hizmetlerde gözlenen veya şüphelenilen herhangi bir bilgi güvenliği açıklığına dikkat etmeleri ve bunları mümkün olduğu kadar çabuk iletişim noktasına raporlamaları gerektiği duyurulmuş ve uygulanmaktadır.

Bilgi güvenliği açıklıklarının raporlanmasına yönelik metodlar ve iletişim kanalları ile bilgi güvenliği yetkilileri BGYS/BP/19 Bilgi Güvenliği İhlal Olayı Yönetimi Prosedüründe belirlenmiş ve uygulanmaktadır.

A.16.1.4 Bilgi Güvenliği Olaylarında Değerlendirme ve Karar Verme

Bilgi Güvenliği Olaylarının Değerlendirilmesi ve Bilgi Güvenliği İhlal Olayı olarak sınıflandırılıp sınıflandırılmayacağına dair karar verilmesi ile ilgili yöntem ve kurallar BGYS/BP/19 Bilgi Güvenliği İhlal Olayı Yönetimi Prosedüründe tanımlanmış ve uygulanmaktadır.

A.16.1.5 Bilgi Güvenliği İhlal Olaylarına Müdahale

Bilgi Güvenliği İhlal Olaylarına müdahale yöntemleri BGYS/BP/19 Bilgi Güvenliği İhlal Olayı Yönetimi Prosedüründe belirlenmiş ve uygulanmaktadır.

A.16.1.6 Bilgi Güvenliği İhlal Olaylarından Ders Çıkarma

Bilgi Güvenliği İhlal Olaylarının analizi ve çözümlenmesinden kazanılan bilgi birikimi gelecekteki ihlal olaylarının gerçekleşme olasılığını veya etkilerini azaltmak için gerekli yöntemler BGYS/BP/19 Bilgi Güvenliği İhlal Olayı Yönetimi Prosedüründe belirlenmiş ve uygulanmaktadır.

A.16.1.7 Kanıt Toplama

Aksaray Üniversitesi Bilgi Güvenliği İhlal Olaylarının kanıtları olarak kullanılacak bilginin tespiti,

Hazırlayan

Birim Kalite Sorumlusu

Yürürlük Onayı

Kalite Koordinatör Yardımcısı

Kalite Sistem Onayı

Kalite Koordinatörü



AKSARAY ÜNİVERSİTESİ BGYS PROSEDÜRÜ

Doküman No	BGYS-PR-001
İlk Yayın Tarihi	17.01.2022
Revizyon Tarihi	01.10.2024
Revizyon No	01
Sayfa No	25/27

toplanması, edinimi ve korunması için gerekli yöntem ve kuralları BGYS/BP/19 Bilgi Güvenliği İhlal Olayı Yönetimi Prosedüründe belirlemiş ve uygulamaktadır.

A.17 BİLGİ GÜVENLİĞİ İHLAL OLAYI YÖNETİMİ

A.17.1 İŞ SÜREKLİLİĞİ YÖNETİMİNİN BİLGİ GÜVENLİĞİ HUSUSLARI

A.17.2 Bilgi Güvenliği Sürekliliği

A.17.2.1 Bilgi Güvenliği Sürekliliğinin Planlanması

Aksaray Üniversitesi olumsuz durumlarda (Kriz ve felaket durumunda) bilgi güvenliği ve bilgi güvenliği yönetimi sürekliliğinin gereksinimlerini BGYS/BP/20 İş Sürekliliği Yönetimi Prosedüründe tanımlanmış ve uygulamaktadır.

A.17.2.2 Bilgi Güvenliği Sürekliliğinin Uygulanması

Aksaray Üniversitesi olumsuz bir olay süresince bilgi güvenliği için istenen düzeyde sürekliliğin sağlanması amacıyla gerekli yöntem ve kuralları BGYS/BP/20 İş Sürekliliği Yönetimi Prosedüründe tanımlanmış, uygulamakta ve sürdürmektedir.

A.17.2.3 Bilgi Güvenliği Sürekliliğinin Doğrulanması, Gözden Geçirilmesi ve Değerlendirilmesi

Aksaray Üniversitesi oluşturulan ve uygulanan bilgi güvenliği sürekliliği kontrollerinin, olumsuz olaylar durumunda geçerli ve etkili olduğundan emin olmak için belirli aralıklarda doğruluğunu sağlanması ile ilgili yöntem ve kuralları BGYS/BP/20 İş Sürekliliği Yönetimi Prosedüründe tanımlanmış ve uygulamaktadır.

A.17.3 Yedek Fazlalıkları

A.17.3.1 Bilgi İşleme Tesislerinin Erişilebilirliği

Aksaray Üniversitesi, Bilgi İşleme Tesisleri, erişilebilirlik gereksinimlerini karşılamak için gerekli yeterli fazlalıklarının tespit edilip, bulundurulması ile ilgili hususlar BGYS/BP/20 İş Sürekliliği Yönetimi Prosedüründe tanımlanmış ve uygulamaktadır.

A.18 UYUM

A.18.1 Yasal ve Sözleşmeye Tabi Gereksinimlere Uyum

A.18.1.1 Uygulanabilir Yasaları ve Sözleşmeye Tabi Gereksinimleri Tanımlama

Aksaray Üniversitesi ilgili tüm yasal, meşru, düzenleyici, sözleşmeden doğan gereksinimleri ve kuruluşun bu gereksinimleri karşılama yaklaşımını her bilgi sistemi ve kuruluşu için BGYS/BP/21 Uyum Prosedüründe tanımlanmış, yazılı hale getirmiş ve güncelliğini sağlamaktadır.

A.18.1.2 Fikri Mülkiyet Hakları

Aksaray Üniversitesi Fikri Mülkiyet hakları ve tescilli yazılım ürünlerinin kullanımı üzerindeki yasal, düzenleyici ve anlaşmalardan doğan gereksinimlere uyum sağlamak için gerekli yöntem ve kuralları BGYS/BP/21 Uyum Prosedüründe tanımlanmış ve uygulamaktadır.

Hazırlayan

Birim Kalite Sorumlusu

Yürürlük Onayı

Kalite Koordinatör Yardımcısı

Kalite Sistem Onayı

Kalite Koordinatörü



AKSARAY ÜNİVERSİTESİ BGYS PROSEDÜRÜ

Doküman No	BGYS-PR-001
İlk Yayın Tarihi	17.01.2022
Revizyon Tarihi	01.10.2024
Revizyon No	01
Sayfa No	26/27

A.18.1.3 Kayıtların Korunması

Aksaray Üniversitesi kayıtların kaybedilmeye, yok edilmeye, sahteciliğe, yetkisiz erişime ve yetkisiz yayımlamaya karşı yasal, düzenleyici, sözleşmeden doğan gereksinimlere ve iş şartlarına uygun olarak korunması ile ilgili gerekli yöntem ve kuralları BGYS/BP/21 Uyum Prosedüründe tanımlamış ve uygulamaktadır.

A.18.1.4 Kişi Tespit Bilgisinin Mahremiyeti ve Korunması

Aksaray Üniversitesi Kişi tespit bilgisinin mahremiyeti ve korunmasına ilişkin yöntem ve kuralları BGYS/BP/21 Uyum Prosedüründe tanımlamış ve uygulamaktadır.

A.18.1.5 Kriptografik Kontrollerin Düzenlenmesi

Aksaray Üniversitesi Kriptografik kontrollerin tüm ilgili sözleşmelere, yasalara ve düzenlemelere uyumlu bir şekilde kullanılması ile ilgili yöntem ve kuralları BGYS/BP/21 Uyum Prosedüründe tanımlamış ve uygulamaktadır.

A.18.2 Bilgi Güvenliği Gözden Geçirmeleri

A.18.2.1 Bilgi Güvenliğinin Bağımsız Gözden Geçirilmesi

Aksaray Üniversitesi bilgi güvenliğine ve uygulamasının yönetimine olan yaklaşımını, belirli aralıklarla veya önemli değişiklikler meydana geldiğinde, bağımsız bir şekilde gözden geçirilmesi ile ilgili yöntem ve kuralları BGYS/BP/21 Uyum Prosedüründe tanımlamış ve uygulamaktadır.

A.18.2.2 Güvenlik Politikaları ve Standartları ile Uyum

Aksaray Üniversitesi birim yöneticilerinin kendi sorumluluk alanlarında bulunan, bilgi işleme ve prosedürlerin, uygun güvenlik politikaları, standartları ve diğer güvenlik gereksinimleri ile uyumunu düzenli bir şekilde gözden geçirmesi ile ilgili yöntem ve kuralları BGYS/BP/21 Uyum Prosedüründe tanımlamış ve uygulamaktadır.

A.18.2.3 Teknik Uyum Gözden Geçirmesi

Aksaray Üniversitesi Bilgi Güvenliği Yönetim Sistemi Politika ve standartları ile uyumluluğu, bilgi sistemlerini düzenli bir şekilde gözden geçirmesi ile ilgili yöntem ve kuralları BGYS/BP/21 Uyum Prosedüründe tanımlamış ve uygulamaktadır.

5. SORUMLULUK

Bilgi güvenliği yöneticisi; bu prosedürün amaç bölümünde yer alan tüm faaliyetlerle ilgili olarak bölümler arası koordinasyonu sağlamak ve takibini yapmaktan sorumludur. Kapsam içindeki tüm bölümler; bu prosedür de belirtilen maddelerin eksiksiz uygulanmasından sorumludur.

6. EKLER

- 6.1 BGYS İlgili taraf Beklentiler ve İletişim Formu
- 6.2 Bilgi Güvenliği Yönetim Sistemi Politikası
- 6.3 Bilgi güvenliği Risk Yönetimi Prosedürü
- 6.4 BGYS Etkinlik Ölçümü ve Amaçlar Formu
- 6.5 Doküman ve Kayıtların Kontrolü Prosedürü
- 6.6 BGYS Risk Değerlendirme Formu

Hazırlayan

Birim Kalite Sorumlusu

Yürürlük Onayı

Kalite Koordinatör Yardımcısı

Kalite Sistem Onayı

Kalite Koordinatörü



AKSARAY ÜNİVERSİTESİ BGYS PROSEDÜRÜ

Doküman No	BGYS-PR-001
İlk Yayın Tarihi	17.01.2022
Revizyon Tarihi	01.10.2024
Revizyon No	01
Sayfa No	27/27

- 6.7 İç Denetim Prosedürü
- 6.8 Düzeltici Faaliyetler Prosedürü
- 6.9 Bilgi Güvenliği Organizasyonu Prosedürü
- 6.10 Proje Risk Yönetim Değerlendirme Test ve Kabul Formu
- 6.11 Mobil Cihazlar ve Uzaktan Çalışma Prosedürü
- 6.12 İnsan Kaynakları Güvenliği Prosedürü
- 6.13 Varlık Yönetimi Prosedürü
- 6.14 Erişim Kontrol Prosedürü
- 6.15 Kriptografi Prosedürü
- 6.16 Fiziksel ve Çevresel Güvenlik Prosedürü
- 6.17 İşletim Güvenliği Prosedürü
- 6.18 Haberleşme Güvenliği Prosedürü
- 6.19 Tedarikçi İlişkileri Prosedürü
- 6.20 Sistem Temini, Geliştirme ve Bakım Prosedürü
- 6.21 Bilgi Güvenliği İhlal Olayı Prosedürü
- 6.22 BGYS İş Sürekliliği Yönetimi Prosedürü
- 6.23 Uyum Prosedürü

Hazırlayan

Birim Kalite Sorumlusu

Yürürlük Onayı

Kalite Koordinatör Yardımcısı

Kalite Sistem Onayı

Kalite Koordinatörü