REVİZYON TABLOSU

REVİZYON NO	REVİZYON GEREKÇESİ	TARİH
01	2022 Versiyon Değişikliği	01.10.2024

1. AMAÇ

Bu prosedür; Aksaray Üniversitesi'nin bilgi varlıkları ve bulundukları ortamlar ile ASÜ bilgi güvenliği süreçlerine ait bilgi güvenliği risk kriterlerinin oluşturulması ve sürdürülmesi, tekrarlanan bilgi güvenliği risk değerlendirmelerinin tutarlı, geçerli ve karşılaştırılabilir sonuçlar üretmesinin temin edilmesi, bilgi güvenliği risklerinin tespit edilmesi, bilgi güvenliği risklerinin analiz edilmesi, bilgi güvenliği risklerinin değerlendirilmesi, bilgi güvenliği risk işleme süreci tanımlanması ve uygulanması, risk değerlendirme sonuçlarını dikkate alarak uygun bilgi güvenliği risk işleme seçeneklerinin seçilmesi ve seçilen bilgi güvenliği risk işleme seçeneklerinin uygulanmasında gerekli olan tüm kontrollerin belirlenmesi için uygulanacak yöntemleri anlatmak amacıyla hazırlanmıştır.

2. KAPSAM

Bu prosedür; bilgi güvenliği kapsamındaki risk değerlendirme ve risk işleme süreçlerine ait faaliyetleri yönetimini kapsar.

3. TANIMLAR

Kurum: Aksaray Üniversitesi

BGYS: ISO IEC 27001 Bilgi Güvenliği Yönetim Sistemi

4. UYGULAMA

4.1. RİSK DEĞERLENDİRMESİ

Süreç analizi yapılarak bilgi varlıkları tespit edilir. Tespit edilen bilgi varlıklarına BGYS/BP/02 Varlık Yönetimi Prosedüründe anlatıldığı şekilde değer atanır. Varlık değerleri BGYS/BF/012 Varlık Envanteri ve Değerleri Formunda belirtilir.

ASÜ bilgi güvenliği risk analizi ve değerlendirme süreçlerini aşağıdaki temel unsurları göz önüne alarak yapmaktadır;

- ✓ Risk analizi ve değerlendirmesi kapsam içindeki tüm birimlere ait bilgi varlıkları için yapılır,
- ✓ Yasal mevzuatta değişiklik olduğunda, kapsam içerisine yeni varlıklar eklendiğinde, varlıkların yeni zafiyeti ve varlıklara yönelik yeni riskler oluştuğunda, varlıkların gizlilik, bütünlük, erişilebilirlik kayıpları (varlık değeri) değiştiğinde, varlıklara yönelik risklere karşı alınan önlemlerin yetersizliği veya ihlal olayı tespit edildiğinde olay araştırması sonrasında, organizasyon veya kullanılan teknoloji

değiştiğinde, tedarikçi sözleşmesi, hizmeti değişikliklerinde Risk analizleri ve değerlendirmesi yeniden yapılır.

Risk analizi yapılırken;

- ✓ Varlıklara ait varlık/risk sahipleri, varlıkların gizlilik, bütünlük ve erişilebilirlik değerleri ile gizlilik, bütünlük ve erişilebilirlik kayıplarının varlıklar üzerinde olabilecek etkileri, varlıklara yönelik tehditler, Tehditlerin kullanabileceği zafiyetler tespit edilir ve tanımlanır.
- ✓ Belirlenen varlıklara karşılık gelen zafiyetler ve tehditler, her varlık ve/veya grubu için ayrı olarak belirlenir ve varlık değerleriyle birlikte BGYS/BF/013 Risk Değerlendirme Formunda listelenir.
- ✓ Bilgi varlıkları ile eşleştirilen zafiyetlere bağlı tehditlerin gerçekleşme olasılığı ve gerçekleşmesi durumundaki etkisi mevcut uygulanan kontroller göz önünde tutularak belirlenir.
- ✓ Olasılık değerleri Tablo-1 de gösterildiği gibi tespit edilir. Keza oluşan güvenlik olaylarının hasar derecesi Tablo-2 de gösterilmiştir. Değerlendirilen olasılıklar ile belirlenen iş hasarları"BGYS /BF/013 Risk Değerlendirme Formu" üzerinde varlıklara ait her tehdit için dokümante edilir. Herhangi bir tehdidin gerçekleşme olasılığı aşağıdaki gibi büyükten küçüğe numaralandırılarak derecelendirilir.

OLASILIK DERECESİ	OLASILIK	AÇIKLAMA
5	**Çok Yüksek**	**Tehdit kaçınılmazdır**
4	**Yüksek**	**Tehdit sıkça tekrarlanır**
3	**Orta**	**Tehdit gerçekleşebilir**
2	**Düşük**	**Tehdit nadiren gerçekleşir**
1	**Çok Düşük**	**Tehdit yok denecek kadar azdır**

Tablo 1: Tehdidin Olma Olasılık Dereceleri

Herhangi bir tehdidin gerçekleşmesi durumunda oluşabilecek hasarlar aşağıdaki gibi büyükten küçüğe numaralandırılarak derecelendirilir.

HASAR DERECESİ	HASAR	AÇIKLAMA
5	Çok Yüksek	İş sürekliliğinde yaşamsal kesintiler, bilginin ifşa edilmesi, ele geçirilmesi, bozulması, silinmesi, yasal veya müşteriyaptırımları, müşteri kaybı yaşanır. ❖ Çalışanın ölümü ❖ Çok ciddi finansal kayıp ❖ Ciddi itibar kaybı nedeniyle uzun süreli düşüşler ❖ Rekabet avantajını uzun süre kaybetmek, doluluk oranlarında ciddi düşüş ❖ Uluslararası medyada olumsuz olarak uzun süreli yer almak

4	Yüksek	İş sürekliliğinde uzun sureli kesintiler, bilginin ifşa edilmesi, ele geçirilmesi, bozulması, silinmesi, yasal veya müşteriyaptırımları, müşteri kaybı yaşanır. ❖ Çalışanların ciddi yaralanmaları, uzuv kaybı ❖ Ciddi finansal kayıp ❖ İtibarın zayıflaması nedeniyle orta vadeli düşüşler ❖ Rekabet avantajını kaybetmek, doluluk oranlarında ciddi düşüş ❖ Uluslararası medyada olumsuz olarak kısa süreli yer almak
3	Orta	İş sürekliliğinde orta sureli kesintilere,bilginin ifşa edilmesine, ele geçirilmesine, bozulmasına, silinmesine,yasal veya müşteri yaptırımlarına, müşteri kaybına yol açabilir. ❖ Çalışanların tedavi görmesini gerektirecek yaralanmalar ❖ Öneli finans kayıpları ❖ İtibarın zayıflaması nedeniyle kısa vadeli düşüşler ❖ Doluluk oranlarında ufak bir düşüş ❖ Ulusal medyada kısa vadeli olumsuz olarak yer almak
2	Düşük	İş sürekliliğinde kısa süreli kesintilere, bilginin ifşa edilmesine, ele geçirilmesine, bozulmasına, silinmesine,yasal veya müşteri yaptırımları ihtimalineyol açabilir. ❖ İlkyardım gerektirebilecek küçük yansımalar ❖ Önemli olmayan finansal kayıplar ❖ İtibar kaybına yol açmayacak durum ❖ Doluluk oranlarında düşük oranda düşüş ❖ Yerel medyaya olumsuz yansıma
1	Çok Düşük	İş sürekliliğinde herhangi bir kesintiye neden olmaz, bilgi kaybı yaşanmaz. ❖ Çalışana zarar gelmesi söz konusu değil ❖ Finansal kayıplar var ❖ İtibar kaybı yaratmayacak durum

Tablo 2: Tehdidin Hasar Dereceleri

Etki Değeri

Olayların etki değerleri üç boyutta (etkileme süresi, kullanıcıların etkilenme oranı ve ekonomik kayıptır) varlık sahiplerinden gelen bilgilere göre BGYS Yöneticisi tarafından belirlenir. Belirlenen üç etki boyutuna ilişkin kullanılan ölçütler ve derecelendirme seviyelerinin açıklamaları aşağıda listelenmiştir.

ETKİ DEĞERİ		
Etkileme Süresi	**Kullanıcıların Etkilenme Oranı**	**Ekonomik Kayıp**
2	5	2
	Etki Değeri	
	3	

ETKİ DEĞERİ = Ort. (Etkileme Süresi, Kullanıcıların etkilenme oranı, Ekonomik kayıp)

Etkileme Süresi: Varlık üzerinde herhangi bir problem olduğu takdirde bilgi sistemlerinin bu problemden ne kadar süre etkileneceği aşağıdaki tabloya göre 1-5 arasında bir rakam ile belirlenir.

ES

0-1 Saat Arası (1)	**Sistem 1 saate kadar etkilenir**
1-2 Saat Arası (2)	**Sistem 2 saate kadar etkilenir**

2-3 Saat Arası (3)	**Sistem 3 saate kadar etkilenir**
3-4 Saat Arası (4)	**Sistem 4 saate kadar etkilenir**
4 Saat Üzeri (5)	**Sistem 4 saatin üzerinde etkilenebilir.**

Kullanıcıların etkilenme oranı: Varlık üzerinde bir problem olduğu takdirde kullanıcıların etkilenme oranı 1-5 arasında bir rakam verilerek aşağıdaki tabloya göre belirlenir.

EO

0 - % 20 si Etkilenir (1)	**Kullanıcıların 5'te 1'i etkilenir.**
%20-40 arası Etkilenir (2)	**Kullanıcıların 5'te 2'si etkilenir.**
%40-60 arası Etkilenir (3)	**Kullanıcıların 5'te 3'ü etkilenir.**
%60-80 arası Etkilenir (4)	**Kullanıcıların 5'te 4'ü etkilenir.**
%100 Etkilenir (5)	**Kullanıcıların tamamı etkilenir.**

Ekonomik kayıp: Varlık üzerinde bir problem olduğu takdirde firmanın uğrayacağı ekonomik zararın ne oranda olacağı aşağıdaki tabloya göre belirlenir.

EK

10.000$ (1)	**10.000$ a kadar zarar uğrayabilir.**
100.000$ (2)	**100.000$ kadar zarar uğrayabilir.**
300.000$ (3)	**300.000$ a kadar zarar uğrayabilir.**
500.000$ (4)	**500.000$ a kadar zarar uğrayabilir.**
500.000$ ve üstü(5)	**500.000$ ve üstü zarara uğrayabilir.**

Gizlilik Etki Seviyeleri (G)

VARLIĞIN GİZLİLİK DERECESİ		
Çok Yüksek	5	Çok Gizli Bilgileri içeren varlık
Yüksek	4	Gizli Bilgiler içeren bir varlık
Orta	3	Şirket personelinden ilgili personellerin bu bilgilere sahip olabileceği varlık
Düşük	2	Tedarikçi ve Taşeronlerın bilebileceği yâda ziyaretçilerle paylaşılması sıkıntı olmayacak bilgi varlıkları
Çok Düşük	1	Halkın bilgisi dahilinde olabilecek veya herkesle paylaşılabilecek seviyedeki bilgi varlığı

Bütünlük Etki Seviyeleri (B)

VARLIĞIN BÜTÜNLÜK DERECESİ		
Çok Yüksek	5	Bilginin %100 bütün halinde ulaşılması gereken bilgi varlığı
Yüksek	4	Bilgi Bütünlüğünde yaşanan aksaklığın kuruluşumuza etki ettiği, işin durmasına, işin aksamasına veya prestij kaybına sebep olan bilgi varlıkları.
Orta	3	Bilgi Bütünlüğünde yaşanan aksaklığın kuruluşumuza kısmen etki ettiği, işin gecikmesine sebeb olabilecek fakat kritik seviyede etki etmeyecek bilgi varlıkları
Düşük	2	Bilgi bütünlüğünün olmaması sonucu kuruluşa etki etmeyen fakat başka varlıklarla ikame edilebilecek bilgi varlıkları
Çok Düşük	1	Bilginin Bütünlüğü önemli olmayan varlıklar

Erişilebilirlik Etki Seviyeleri (E)

VARLIĞIN ERİŞİLEBİLİRLİK DERECESİ		
Çok Yüksek	5	Bilgiye %100 erişilmesi gerekli bilgi varlıkları
Yüksek	4	Bilgiye erişilemediğinde yaşanan aksaklığın kuruluşumuza etki ettiği, işin durmasına, işin aksamasına veya prestij kaybına sebeb olan bilgi varlıkları.
Orta	3	Bilgiye erişimde yaşanan aksaklığın kuruluşumuza kısmen etki ettiği, işin gecikmesine sebeb olabilecek fakat kritik seviyede etki etmeyecek bilgi varlıkları
Düşük	2	Bilgiye erişimin olmaması sonucu kuruluşa etki etmeyen fakat başka varlıklarla ikame edilebilecek bilgi varlıkları

Çok Düşük	1	Bilgi erişiminin önemli olmadığı varlıklar

Varlık değer aralığı aşağıdaki formülle belirlenir.

VARLIK DEĞER ARALIĞI*(V)* = Ort (G x B x E)

Varlık değeri hesaplanan varlıklar aşağıdaki tabloda verilen değer aralıklarından hangi aralığa ait ise varlık değeri 1 ile 5 arasında seçilerek risk hesaplaması yapılır.

VARLIK SINIFI	VARLIK DEĞERİ (V)
Çok Kritik	5
Kritik	4
İç kullanım	3
Halka açık	2
Önemsiz Bilgi	1

Risk Derecesi (R) = V x O x E

V: Varlık Değeri **O:** Olasılık Değeri **E:** Etki Değeri

RİSK ETKİ BÜYÜKLÜKLERİNİN SINIFLANDIRILMASI VE DEĞERLENDİRİLMESİ

Risk Büyüklüğü (R)	Risk Derecesi	Değerlendirme	Renk
125-100	Çok Yüksek Risk	Acil Önlem Alınmalı	KIRMIZI
99-60	Yüksek Risk	Hemen Çalışma Yapılmalı	MAVİ
59-28	Dikkate Değer Risk	Mümkün Olduğunca Çabuk Müdahale Edilmeli	SARI
0-27	Kabul Edilebilir Risk	Acil Tedbir Gerektirmeyebilir, Dikkatli Olunmalı	YEŞİL

Risk değerlendirmesi yapılırken;

- ✓ Risk analizi sonuçlarının oluşturulan risk kriterleri ile karşılaştırılması ve analiz edilen risklerin risk işleme için öncelikle dirilmesi yapılır.

Risk Formülü:

RİSK = VARLIK DEĞERİ x TEHDİDİN OLMA OLASILIĞI x TEHDİDİN ETKİSİ

Not: Bu yöntem sonucunda max. Risk değeri 125, min. Risk değeri 1'dir. (Varlık değeri 1-5, olasılık 1-5, hasar derecesi 1-5 arasında değişir.)

BGYS kapsamında yönetim tarafından belirlenmiş olan kabul edilebilir risk seviyesi uyarınca, hesaplanan risk düzeylerinin kabul edilebilir olup olmadığına karar verilerek, tespit edilmiş olan kriterlere göre iyileştirme gereklilikleri belirlenir.

Kabul Edilebilir Risk Seviyesi:

Kabul edilebilir risk seviyesi tespit edilirken, varlıkların her tehdit için risk seviyesi formül kullanılarak hesap edilir.

Yukarıdaki açıklamaya göre ASÜ'nün kabul edilebilir risk seviyesi **27** olarak belirlenmiştir. Varlık envanteri listesi içerisinde yer alan varlıkların risk değerlendirmesi yapılacaktır.

4.2 RİSK İŞLEME

Değerlendirme sonucunda varlıklara ait risk skorları kabul edilebilir risk seviyesi olan 27'ün altında kalıyorsa kontrollerin yeterli olduğu değerlendirilecektir. Aksi halde, kontroller kullanılarak varlığa ait tehdit için risk seviyesinin 27'nin altına çekilmesi için risk işleme aksiyonları uygulanır. Risk işleme aksiyonlarından sonra kabul edilebilir risk değerininüzerinde kalan riskler artık risk olarak yönetimin onayına sunulur.

Alınan aksiyonlar Risk İşleme tablosuna da yazılır.

5. SORUMLULUK

Kapsam dâhilindeki tüm personel Risk Yönetimi Prosedürü uygulama esaslarına uygun hareket etmekle yükümlüdür.

6. EK:

BGYS/BP/02 Varlık Yönetimi Prosedürü

BGYS/BF/012 Varlık Envanteri ve Değerleri Formu

BGYS /BF/013 Risk Değerlendirme Formu