1. AMAÇ

Bu prosedürün amacı, Süleyman Demirel Üniversitesi Entegre Yönetim Sistemi (EYS) kapsamında Üniversitenin faaliyetlerini, bilgi varlıklarını, hizmetlerini ve iş süreçlerini etkileyebilecek iç ve dış kaynaklı tehlike ve tehditlerin belirlenmesi, risklerin değerlendirilmesi, önceliklendirilmesi, işlenmesi, izlenmesi ve gerektiğinde yeniden değerlendirilmesine ilişkin yöntem ve esasları belirlemektir.

Bu prosedür ile Üniversitenin faaliyetlerinin sürekliliğini, bilgi varlıklarının gizlilik, bütünlük ve erişilebilirliğini, kişisel verilerin korunmasını, hizmetlerin sürdürülebilirliğini ve EYS amaçlarının gerçekleştirilmesini etkileyebilecek risklerin sistematik şekilde yönetilmesi amaçlanmaktadır.

2. KAPSAM

Bu prosedür, Süleyman Demirel Üniversitesi Daire Başkanlıkları, Genel Sekreterlik ve Araştırma ve Uygulama Hastanesi Bilgi İşlem Birimi dahilinde gerçekleştirilen faaliyet, süreç, hizmet ve bilgi varlıklarına ilişkin risk değerlendirme ve yönetim çalışmalarını kapsar.

Prosedür kapsamında; insan kaynağı, bilgi, yazılım, donanım, fiziksel varlıklar, hizmetler, süreçler ve bunlarla ilişkili diğer varlıklar ile bu varlıklara yönelik tehdit, açıklık, risk, fırsat ve mevcut kontroller değerlendirilir.

3. TANIMLAR

- **EYS (Entegre Yönetim Sistemi):** Süleyman Demirel Üniversitesi bünyesinde uygulanan ISO 9001 Kalite Yönetim Sistemi, ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi, ISO/IEC 27701 Kişisel Veri Yönetim Sistemi, ISO 22301 İş Sürekliliği Yönetim Sistemi ve ISO/IEC 20000-1 Bilgi Teknolojileri Hizmet Yönetim Sisteminin bütünleşik yapısını,
- **Varlık:** Üniversite faaliyetlerinin gerçekleştirilmesi için değeri bulunan ve korunması gereken bilgi, yazılım, donanım, fiziksel unsur, insan kaynağı, hizmet ve benzeri unsurları,
- **Varlık Sahibi:** Varlığın korunması, kullanımından kaynaklanan risklerin yönetilmesi ve varlıkla ilgili gerekli kararların alınmasından sorumlu kişi veya birimi,
- **Gizlilik:** Bilginin yalnızca erişim yetkisi bulunan kişi veya süreçler tarafından erişilebilir olmasını,
- **Bütünlük:** Bilginin doğruluğunun ve bütünlüğünün yetkisiz veya hatalı değişikliklere karşı korunmasını,
- **Erişilebilirlik:** Bilgi, sistem ve hizmetlerin ihtiyaç duyulduğunda yetkili kullanıcılar tarafından erişilebilir ve kullanılabilir olmasını,
- **Tehdit:** Bir varlığa zarar verme veya varlığın gizlilik, bütünlük ya da erişilebilirliğini olumsuz etkileme potansiyeline sahip olay veya durumu,
- **Tehdit Kaynağı:** Bir tehdidin ortaya çıkmasına neden olabilecek insan, sistem, çevresel koşul, teknik durum veya diğer kaynakları,

- **Açıklık/Zafiyet:** Bir varlığın, sistemin, sürecin veya kontrolün tehditler tarafından kullanılmasına neden olabilecek zayıflık, hata veya eksikliği,
- **Olasılık:** Bir riskin belirlenen zaman dilimi içerisinde gerçekleşme ihtimalini,
- **Etki:** Bir riskin gerçekleşmesi halinde Üniversitenin faaliyetleri, hizmetleri, bilgi varlıkları, kişisel verileri, yasal yükümlülükleri veya diğer hedefleri üzerindeki etkisini,
- **Risk:** Tehditlerin mevcut açıklıklardan yararlanması sonucunda ortaya çıkabilecek olumsuz sonuçların olasılığı ve etkisini,
- **Risk Değerlendirmesi:** Risklerin belirlenmesi, analiz edilmesi ve belirlenen kriterlere göre değerlendirilmesi sürecini,
- **Risk Analizi:** Risklerin olasılık ve etkilerinin belirlenerek risk seviyesinin hesaplanmasını,
- **Risk İşleme:** Belirlenen risklere karşı uygulanacak yöntem ve kontrollerin seçilmesi ve uygulanmasını,
- **Risk Sahibi:** Belirli bir riskin yönetilmesi, izlenmesi ve gerekli aksiyonların alınmasından sorumlu kişi veya birimi,
- **Artık Risk:** Risk işleme faaliyetleri ve kontroller uygulandıktan sonra kalan riski,
- **Risk Kabulü:** Belirlenen riskin mevcut veya planlanan kontrollerle birlikte kabul edilebilir seviyede olduğuna karar verilmesini,
- **Fırsat:** EYS amaçlarının, süreçlerin veya performansın geliştirilmesine katkı sağlayabilecek koşul veya imkânı ifade eder.

4. SORUMLULUK

- **Üst Yönetim:** Risklerin yönetilmesi için gerekli kaynak ve desteği sağlamak ve gerektiğinde artık risklerin kabulüne ilişkin kararları vermek.
- **Yönetim Temsilcisi:** Risk değerlendirme ve yönetim faaliyetlerinin EYS kapsamında koordinasyonunu sağlamak ve sonuçlarını izlemek.
- **Birim Yöneticileri:** Birim faaliyetleri ve varlıklarına ilişkin risklerin belirlenmesini, değerlendirilmesini ve gerekli aksiyonların yürütülmesini sağlamak.
- **Varlık Sahipleri:** Sorumlu oldukları varlıkların değerini belirlemek, varlığa yönelik riskleri değerlendirmek ve gerekli kontrollerin uygulanmasını sağlamak.
- **Risk Sahipleri:** Sorumlu oldukları riskler için risk işleme faaliyetlerinin planlanmasını, uygulanmasını ve izlenmesini sağlamak.
- **Bilgi İşlem Daire Başkanlığı:** Bilgi teknolojileri ve bilgi güvenliği kapsamında teknik risklerin değerlendirilmesine ve gerekli teknik kontrollerin uygulanmasına destek olmak.
- **Çalışanlar:** Görevleri kapsamında karşılaştıkları risk, tehdit ve zafiyetleri ilgili birimlere bildirmek ve belirlenen kontrollere uymak.

5. UYGULAMA

5.1. Risk Yönetiminin Genel Esasları

Risk yönetimi; varlıkların ve süreçlerin belirlenmesi, tehdit ve zafiyetlerin değerlendirilmesi, risklerin analiz edilmesi, risk işleme yöntemlerinin belirlenmesi, kontrollerin uygulanması, artık risklerin değerlendirilmesi ve risklerin izlenmesi aşamalarından oluşur.

Risk değerlendirmelerinde;

- amaç ve hedefler,
- EYS kapsamındaki süreçler,
- Yasal ve mevzuat şartları,
- İlgili tarafların ihtiyaç ve beklentileri,
- Bilgi varlıklarının gizlilik, bütünlük ve erişilebilirliği,
- İş sürekliliği,
- Kişisel verilerin korunması,
- Bilgi teknolojileri hizmetleri,
- Mevcut güvenlik ve kontrol uygulamaları,
- Geçmişte meydana gelen olaylar ve uygunsuzluklar,
- İç ve dış tehditler,
- Değişiklikler ve yeni faaliyetler dikkate alınır.

5.2. Varlıklarının Belirlenmesi

İşin gerçekleştirilmesi için ve iş sürekliliği için gerekli olan tüm maddi ve manevi varlıklar birim varlıklarını oluştururlar. Bu varlıklar kullanım amaçları, işe etkileri, maddi ve manevi değerleri ile zayıflıklara karşı tehdit altında olabilirler.

Kurum bünyesinde varlıklarımız şu şekilde sınıflandırılır ve tanımlanır.

VARLIK SINIFI	AÇIKLAMA
Fiziksel Varlıklar:	Birimde kullanılan fiziksel varlıklardır. **Alt kategoriler:** a) Bilgisayar ekipmanları (bilgisayar, sunucu, işlemci, diz üstü bilgisayarlar, modemler vb.); b) İletişim ekipmanları (yönlendirici, telefon, faks vb.); c) manyetik kayıt ortamları (teyp, kartuş, disket, disk, cd vb.); d) Diğer teknik ekipmanlar (güç kaynakları, adaptör, havalandırma üniteleri vb.);
Yazılım Varlıkları:	Projelerin gerçekleştirilmesinde kullanılan her türlü bilgisayar programı, işletim sistemi ve yardımcı yazılımlar **Alt kategoriler:** e) Uygulama yazılımları f) Sistem yazılımları g) Geliştirme araç ve yazılımları; h) Diğer

Bilgi Varlıkları:	Kurumun tüm bilgi sistemlerinde, çalışanlarında, kütüphanelerinde tutulan ve kurumun iş süreçlerinde değişik formlarda işlenen veridir. **Alt kategoriler:** i) Veritabanları; j) Veri dosyaları; k) Basılı materyal (sistem belgeleri, kullanıcı el kitapları, eğitim malzemeleri materyalleri, işlemsel ve destek uygulamaları, devamlılık (süreklilik) planları, yedek anlaşmaları, sözleşmeler; vb.) l) Arşivlenmiş bilgi; m) Diğer (Yukarıdaki alt kategoriler dışında bulunan bilgi varlıklarıdır.)
Servisler (Hizmetler)	Bilgi işleme ve haberleşme servisleri (web servisi, ftp servisi)
İnsan Kaynağı	Faaliyetlerimizi gerçekleştirirken farklı pozisyonlarda görev yapan ve iş sonuçlarına doğrudan veya dolaylı etkisi olan tüm personelimiz
Süreçler	Faaliyetleri ve hizmetleri gerçekleştirmek amacıyla yürütülen süreçler.

Varlıklar **Varlık Envanteri** kapsamında kayıt altına alınır.

Yeni bir varlık oluşturulması, mevcut varlığın kullanım amacının değişmesi veya varlığın önem seviyesini etkileyen bir değişiklik meydana gelmesi halinde varlık değerlendirmesi gözden geçirilir. Her varlık için, varlığın kullanımından ve korunmasından sorumlu varlık sahibi belirlenir.

5.3. Varlık Değerinin Belirlenmesi

Güvenlik Hedefi	Düşük (1)	Orta (2)	Yüksek (3)	Çok Yüksek (4)
Gizlik	Varlığa bir zarar gelmesi durumunda veya kritik bilgi açığa çıkmaz. Açığa çıkan bilginin kritiklik seviyesi çok az etkiler veya etkilemez. Etki kısa vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda veya kritik bilgi açığa çıkmaz. Açığa çıkan bilginin kritiklik seviyesi kurumu etkiler. Etki orta vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda veya kritik bilgi açığa çıkar. Açığa çıkan bilginin kritiklik seviyesi kurumu etkiler. Etki orta vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda veya kritik bilgi açığa çıkar. Açığa çıkan bilginin kritiklik seviyesi kurumu etkiler. Etki telafi edilemez ya da uzun vadede telafi edilebilir.
Bütünlük	Varlığa bir zarar gelmesi durumunda veya kritik bilgi kontrol dışı değişmez. Kontrol dışı değişen bilginin kritiklik seviyesi çok az etkiler veya etkilemez. Etki kısa vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda veya kritik bilgi kontrol dışı değişmez. Kontrol dışı değişen bilginin kritiklik seviyesi kurumu etkiler. Etki orta vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda veya kritik bilgi kontrol dışı değişir. Kontrol dışı değişen bilginin kritiklik seviyesi kurumu etkiler. Etki orta vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda veya kritik bilgi kontrol dışı değişir. Kontrol dışı değişen bilginin kritiklik seviyesi kurumu etkiler. Etki telafi edilemez ya da uzun vadede telafi edilebilir.
Erişilebilirlik	Varlığa bir zarar gelmesi durumunda veya kritik bilgiye erişilebilir. Erişilebilirliğine zarar gelen bilginin kritiklik seviyesi çok az etkiler veya etkilemez. Etki kısa vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda veya kritik bilgiye erişilebilir. Erişilebilirliğine zarar gelen bilginin kritiklik seviyesi kurumu etkiler. Etki orta vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda veya kritik bilgiye erişilemez. Erişilebilirliğine zarar gelen bilginin kurumu etkiler. Etki orta vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda veya kritik bilgiye erişilemez. Erişilebilirliğine zarar gelen bilginin kritiklik seviyesi kurumu etkiler. Etki telafi edilemez ya da uzun vadede telafi edilebilir.

Varlık değeri belirlenirken Bilgi Güvenliği Yönetim Sisteminin Temeli olan **Gizlilik, Bütünlük ve Erişilebilirlik** açısından değerlendirme yapılır. Bu değerlendirme aşağıdaki yöntem ile belirlenir.

VARLIK DEĞERİ= GİZLİLİK X BÜTÜNLÜK X ERİŞİLEBİLİRLİK

Bu hesaplama Sonucunda varlık değeri 1-64 arasında olabilir.

5.4. Bilgi{ XE "Bilgi" } Varlıklarının Güvenlik Sınıflandırması

Bilgi{ XE "Bilgi" } varlığı aşağıdaki kategorilerde sınıflandırılabilir:

Varlık Değeri	Sınıflandırma Seviyesi	Bilgi Sınıflandırma Karşılığı	Tanımlama
50 – 64	**Çok Yüksek**	**Çok Gizli**	Sadece üst yönetim ve belirli yetkililer erişebilir. İfşası kurumun bekasını tehlikeye atar. Bilgi varlıkları; güvenliği sağlanmış ve sadece yetkili kişilerin girebileceği odalarda bulunan kasa ya da kilitli dolaplarda saklanan bilgilerdir. Kopyalama, iletme, imha için yetkili kişinin onayı alınmalıdır. Bu varlıklar yakılarak ya da birleştirilemeyecek derecede parçalanarak imha edilmelidir.
25 – 49	**Yüksek**	**Gizli**	Kurumun faaliyetini devam ettirebilmesi için kritik olan ve yetkisiz kişilerin eline geçmesi durumunda güvenliği, saygınlığı ve çıkarları ciddi derecede zedeler. Sadece ilgili birim ve süreç sahipleri erişebilir. İfşası yasal yaptırım veya yüksek zarar doğurur. Kasa ya da kilitli ortamda saklanmalı; kopyalama, iletme, imha için yetkili kişinin onayı alınmalıdır. Bu varlıklar, yakılarak ya da birleştirilmeyecek derecede parçalanarak imha edilmelidir
10 - 24	**Orta**	**Kuruma Özel**	Kurum dahilin de üretilen; yönergeler, standartlar, prosedürler, politikalar ve bu bilgilerin bulunduğu ortamlar vb. gibi, Kurum dışına çıkarılması için üst yönetimden onay alınması gereken bilgi varlıklarıdır. Kurum içinde kullanımında, kopyalanmasında sakınca yoktur. Ancak yukarıda belirtilen dokümanlardan içeriği itibarı ile sadece kurumdaki yetki verilmiş kişilerin erişebileceği dokümanların gizlilik derecesinin kuruma özel olarak değil, uygun olan şekilde (çok gizli, gizli, gibi) verilmesi gerekir.

5 - 9	**Orta**	**Hizmete Özel**	Sadece belli bir grup tarafından örneğin proje ekibi, belli bir birim gibi görülebilecek olan bilgi varlıklarıdır. İçerdiği konular itibariyle, diğer gizlilik dereceli konular dışında olan ancak güvenlik işlemine ihtiyaç gösteren bilgi varlıkları hizmete özel olarak sınıflandırılır. Projeler özelinde üretilen proje planı, tasarım ve gerekli dokümanları, kaynak kodlar ve bu bilgilerin bulunduğu ortamlar vb örnek olarak verilebilir. Gizli varlıklar gibi, yetkili kişi izni ile kopyalama, iletme ve imha işlemi yapılmalıdır.
0 - 4	**Düşük**	**Yayınlanabilir, umumi (Kamuya açık)**	Kullanılması güvenlik açısından önemli olmayan, kurumdaki veya kurum dışındaki her kişiye açık bilgilerdir. Örneğin duyurular vb.

5.5. Tehdit ve Zafiyetlerin Belirlenmesi

Varlıkların maruz kalabileceği tehditler ve mevcut zafiyetler belirlenir. Değerlendirme sırasında aşağıdaki hususlar dikkate alınabilir:

- İnsan kaynaklı tehditler,
- Siber saldırılar,
- Kötücül yazılımlar,
- Yetkisiz erişim,
- Veri kaybı veya bozulması,
- Donanım ve yazılım arızaları,
- Enerji kesintileri,
- Yangın, sel, deprem ve benzeri afetler,
- Tedarikçi veya üçüncü taraf kaynaklı tehditler,
- Mevzuat ve düzenleyici değişiklikler,
- Süreç veya organizasyon değişiklikleri,
- İnsan hataları,
- Yetersiz veya etkisiz kontroller.

Belirlenen tehditler **Tehdit Listesi**, zafiyetler ise **Zayıflık Listesi** kapsamında takip edilir.

5.6. Risk Değerlendirme Metodolojisi

Risk değerlendirmesinde varlığın değeri, olayın gerçekleşme olasılığı ve gerçekleşmesi halinde oluşabilecek etki birlikte değerlendirilir. Risk değeri aşağıdaki formül ile hesaplanır:

RİSK (R) = VARLIK DEĞERİ X OLASILIK X ETKİ

Varlık değeri 1–64**, olasılık** 1–5**, etki** 1–5 arasında değerlendirilir.

Risk değeri 1–1600 aralığında oluşabilir.

5.7. Olasılık Değerinin Belirlenmesi

Risklin gerçekleşme olasılığı, bu riskin kurumda gün, hafta, ay, yıl gibi bir zaman dilimi içerisinde gerçekleşme durumunu ifade eder. Riskin analizi yapılırken "Olasılık" sütunu aşağıdaki tablo dikkate alınarak doldurulur.

Risk Olasılık Derecesi	Olasılık Tanımı	Gerçekleşme Sıklığı	Detaylı Açıklama
1	Çok Düşük	Yılda bir den daha az	Kurumda geçmişte hiç yaşanmamış veya yalnızca teorik olarak mümkün olan olaylardır. Güçlü ve etkin kontroller mevcuttur. Olayın gerçekleşmesi olağan dışı koşullara bağlıdır.
2	Düşük	Yılda bir	Nadiren gerçekleşir. Geçmişte istisnai olarak yaşanmış olabilir. Mevcut kontroller genel olarak etkilidir ancak kontrol zafiyeti oluşması durumunda risk ortaya çıkabilir.
3	Orta	Altı ayda bir	Benzer olaylar kurum içinde veya sektörde yaşanmıştır. Kontroller mevcuttur ancak insan hatası, süreç eksiklikleri veya çevresel faktörler nedeniyle riskin gerçekleşmesi mümkündür.
4	Yüksek	Üç ayda bir	Olayların daha önce tekrar ettiği veya sık yaşandığı görülmüştür. Kontroller yetersizdir ya da tutarlı şekilde uygulanmamaktadır. Riskin gerçekleşmesi beklenen bir durumdur.
5	Çok Yüksek	Ayda bir veya daha sık	Olaylar düzenli olarak yaşanmaktadır veya yaşanması kaçınılmazdır. Kontroller yoktur veya etkisizdir. Acil iyileştirme aksiyonları gereklidir.

Olasılık değerlendirmesinde geçmiş olaylar, mevcut kontroller, tehditlerin niteliği, zafiyetler ve ilgili çevresel veya operasyonel koşullar dikkate alınır.

5.8. Etki Değerinin Belirlenmesi

Riskin oluşması durumunda birime vereceği zararı, hedef ve faaliyetler üzerindeki etkisini gösterir. Aşağıdaki tabloya göre riskin etki değeri belirlenerek "Etki Faktörü" sütununa işlenir.

Risk Etki Derecesi	Riskin Etkisi	Etki Tanımı
1	Çok Düşük	İhmal edilebilir düzeyde etki vardır. Kurumsal faaliyetler, hizmetler ve itibar üzerinde anlamlı bir etkisi yoktur. Riskin gerçekleşmesi, finansal kayıplar, mevzuata aykırılık ve de itibar ve saygınlığın kaybedilmesine sebep olmaz.
2	Düşük	Küçük çaplı operasyonel aksaklıklar oluşur. Kısa sürede telafi edilebilir, hizmet sürekliliği etkilenmez.
3	Orta	Süreçlerde aksama veya gecikme yaşanır. Hizmetler devam eder ancak düzeltici faaliyet gerektirir. İtibar etkisi sınırlıdır.
4	Yüksek	Temel hizmetlerde önemli kesinti yaşanır. Mali kayıp oluşur. Bilgi güvenliği ihlali veya paydaş memnuniyetsizliği meydana gelir.
5	Çok Yüksek	Kurum faaliyetleri ciddi şekilde durur. Yasal yaptırım, ağır mali kayıp veya ciddi kişisel veri ihlali meydana gelir. Kurumsal itibar ağır zarar görür.

Etki değerlendirmesinde;

- Hizmet ve faaliyetlerin sürekliliği,
- Mali sonuçlar,
- Yasal ve mevzuat yükümlülükleri,
- Bilgi güvenliği,
- Kişisel verilerin korunması,
- Kurumsal itibar,
- Paydaşlar üzerindeki etkiler dikkate alınır.

5.9. Risk Seviyelerinin Sınıflandırılması

- **Varlık Değeri = Gizlilik (1–4) × Bütünlük (1–4) × Erişilebilirlik (1–4)**
- **Risk Büyüklüğü (R) = Varlık Değeri × Olasılık (1–5) × Etki (1–5)**

Hesaplanan risk büyüklüğü **1–1600** aralığındadır ve aşağıdaki kriterlere göre sınıflandırılır.

Risk Değeri Aralığı	Risk Seviyesi	Yönetim / Aksiyon	Renk
1 – 192	**Etkisiz Risk (Kabul Edilebilir)**	Mevcut kontroller yeterlidir. Risk izlenir, ilave aksiyon gerektirmez.	Açık Yeşil
193 – 384	**Düşük Risk**	Risk sahibi tarafından değerlendirilir; gerekli görülmesi halinde ilave kontrol uygulanır veya risk kabul edilir.	Sarı
385 – 768	**Orta Risk**	Riskin azaltılması amacıyla aksiyon planı hazırlanır ve uygulanır.	Turuncu
769 – 1024	**Yüksek Risk**	Riskin azaltılması için öncelikli ve ivedi kontroller uygulanır.	Kırmızı
1025 – 1600	**Çok Yüksek Risk**	Risk kabul edilemez seviyede değerlendirilir. Derhal aksiyon alınır ve gerekli görülmesi halinde faaliyet geçici olarak durdurulur.	Koyu Kırmızı

5.10. Risk İşleme Metodolojisi

Risk değerlendirme sonucunda tüm varlıklarla ilgili risk değerleri tespit edilir. Bu değerlendirme sürekli olarak yapısal, organizasyonel ve uygulama değişiklikleri çerçevesinde izlenir ve değişken risk sürekli yeniden hesaplanır.

Risk işleme seçenekleri şunlardır:

- **Riskin Kabulü:** Riskin var olduğunu kabul ederek BT sistemlerini kullanmaya devam etmektir.
- **Riskten Kaçınma:** Riski yaratan sebebi ortadan kaldırmak, İşi gerçekleştirmenin başka yollarını aramak, Var olan hizmeti sonlandırmak, bazı faaliyetleri durdurmak olarak tanımlanabilir. (örneğin bir yazılımın risk yaratan kısmının yüklenmemesi ve kullanılmaması gibi)
- **Riskin Azaltılması:** Açıklığın gerçekleşmesi halinde oluşacak etkinin uygulanan kontroller ile azaltılması. Karşılaşılabilecek riskler tanımlandıktan sonra bu risklerin etkisini veya gerçekleşme olasılıklarını azaltmak için ek önlemler alarak, riske yanıt verme planı oluşturma çalışmasıdır.

- **Riskin Transferi**: Riskin gerçekleşmesi durumunda oluşabilecek zararı karşılayacak çözümler bularak (örneğin sigorta yaptırmak), Riski bir başka kuruma veya bireye devretme. Bu uygulamada aslında risk yok edilmiş olmayacaktır, sadece riskin sorumluluğunun başkası tarafından yüklenilmesi sağlanacaktır. Risk, riskin transfer edildiği birimde analiz edilmelidir

5.11. Risk İşleme Planlarının Takibi

Risk işleme faaliyetleri için gerektiğinde;

- Alınacak önlem,
- Sorumlu kişi veya birim,
- Termin tarihi,
- Gerekli kaynak,
- Uygulama yöntemi,
- Beklenen risk seviyesi belirlenir.

Uygulanan kontroller sonrasında risk yeniden değerlendirilir. Riskin kabul edilebilir seviyeye indirilmesi hedeflenir. Kabul edilebilir seviyeye indirilemeyen riskler artık risk olarak değerlendirilir.

5.12. Risk Sahiplerinin Belirlenmesi

Her bir risk için risk sahibi belirlenir.

Risk sahibi;

- Riskin izlenmesinden,
- Risk işleme yönteminin belirlenmesine katkı sağlamaktan,
- Aksiyonların uygulanmasını takip etmekten,
- Risk seviyesindeki değişiklikleri değerlendirmekten sorumludur.

Risk sahibi ile varlık sahibi aynı kişi veya birim olabileceği gibi farklı kişi veya birimler de olabilir.

5.13. Artık Risklerin Yönetimi

Risk işleme faaliyetlerinden sonra tamamen ortadan kaldırılamayan riskler artık risk olarak değerlendirilir.

Riskin kabul edilebilir seviyeye indirilemediği durumlarda artık risk kayıt altına alınır ve yetkili yönetim tarafından değerlendirilerek kabul edilmesi sağlanır. **Artık Risk Formu** bu amaçla kullanılır.

5.14. Fırsatların Belirlenmesi

Risk değerlendirmesi sırasında risklerin azaltılması veya ortadan kaldırılması sonucunda ortaya çıkabilecek fırsatlar da değerlendirilir.

Fırsatlar;

- Süreçlerin iyileştirilmesi,
- Hizmet kalitesinin artırılması,
- Kaynakların daha etkin kullanılması,
- Bilgi güvenliğinin geliştirilmesi,
- Hizmet sürekliliğinin güçlendirilmesi,
- Teknolojik gelişmelerden yararlanılması gibi alanlarda ele alınabilir.

Belirlenen fırsatlar ilgili süreçler kapsamında değerlendirilir ve gerekli görüldüğünde iyileştirme faaliyetlerine dönüştürülür.

5.15. Risklerin Gözden Geçirilmesi ve Yeniden Değerlendirmesi

Risk değerlendirmeleri aşağıdaki durumlarda gözden geçirilir ve gerektiğinde yeniden yapılır:

- Yeni bir faaliyet veya hizmet başlatılması,
- Mevcut hizmet veya süreçte önemli değişiklik yapılması,
- Yeni bilgi sistemi veya teknoloji kullanılması,
- Önemli organizasyonel değişiklik yapılması,
- Yeni tehdit veya zafiyet tespit edilmesi,
- Kişisel veri ihlali veya bilgi güvenliği olayı meydana gelmesi,
- İç tetkik veya dış denetimlerde önemli bulgu tespit edilmesi,
- Mevzuat veya yasal şartların değişmesi,
- Tedarikçi veya üçüncü taraf kaynaklı önemli bir değişiklik olması,
- İlgili tarafların ihtiyaç veya beklentilerinde önemli değişiklik olması,
- Risk işleme faaliyetlerinin tamamlanması,
- Fırsata yönelik aksiyonların uygulanması,
- Yüksek veya çok yüksek riskler için belirlenen aksiyonların tamamlanması veya etkinliğinin değerlendirilmesi gerektiğinde,
- Herhangi bir değişiklik bulunmasa dahi en az yılda bir kez.

5.16. Risk İzleme ve Raporlama

Risk değerlendirmesi sonucunda belirlenen riskler, risk seviyelerine göre izlenir ve gerekli görülen durumlarda yeniden değerlendirilir. Yüksek ve çok yüksek seviyedeki riskler Risk İzleme Listesi'ne alınarak düzenli olarak izlenir ve bu risklere ilişkin alınan aksiyonların gerçekleşme durumu takip edilir.

Yüksek ve çok yüksek riskler için belirlenen risk işleme faaliyetlerinin uygulanması, sorumluları ve hedef tarihleri izlenir. Alınan önlemler sonrasında risk seviyesinde değişiklik meydana gelmesi halinde risk yeniden değerlendirilir ve Risk İzleme Listesi güncellenir.

Orta ve düşük seviyedeki riskler, ilgili süreç ve birim sorumluları tarafından değerlendirilir ve gerekli görülmesi halinde risk işleme faaliyetleri planlanır. Bu riskler, yüksek ve çok yüksek riskler için kullanılan Risk İzleme Listesi kapsamında takip edilmez.

6. İLGİLİ DOKÜMANLAR

- Artık Risk Formu
- Risk ve Fırsat İzleme ve Değerlendirme Tablosu
- Risk İzleme Tablosu
- Tehdit Listesi
- Zayıflık Listesi
- Varlık Envanteri
- Risk Analizi İş Akışı

7. REVİZYON TAKİP TABLOSU

REVİZYON NO	TARİH	AÇIKLAMA
000	22.01.2020	İlk yayın.
001	09.09.2022	Prosedür içeriği değiştirilmiş ve entegre yönetim sistemlerine geçildiğinden Tek bir Risk değerlendirme ölçümü belirlenmiş ve uygulanmaktadır.
002	22.01.2024	Kontrol kısmı güncellenmiştir.
003	22.12.2024	Tanımlar kısmında EYS: Entegre Yönetim Sistemi (BGYS, KYS, HYS, İSYS, KVYS) olarak güncellenmiştir.
004	24.12.2025	Risk olasılık tanımlamaları güncellendi.
005	16.09.2026	SDÜ EYS yapısına uyum sağlanması; kapsam, sorumluluklar, tanımlar, varlık değerlendirmesi, bilgi sınıflandırması, risk değerlendirme ve risk işleme metodolojileri, artık risk, fırsatlar, risk izleme ve yeniden değerlendirme süreçlerinin güncellenmesi.