1.AMAÇ:
Erzurum Teknik Üniversitesinin ISO/IEC 27001 BGYS çalışmalarında temel teşkil edecek varlık envanterinin oluşturulması ve süreçlerle ilişkin risklerin, değerlendirmesi için yöntem belirlenmesi ve risklerin kontrol altında tutulmasını amaçlamaktadır.

2. KAPSAM
Erzurum Teknik Üniversitesinin Bilgi İşlem Daire Başkanlığı sorumluluğundadır.

3. TANIMLAR ve KISALTMALAR
BGYS: Bilgi Güvenliği Yönetim Sistemi
Varlık: Bir işletme için değeri olan ve bu nedenle uygun olarak korunması gereken tüm unsurlardır.
Risk: Tehlikeli bir olayın meydana gelme olasılığı ile sonuçlarının bileşimi.
Risk değerlendirmesi: Riskin büyüklüğünü tahmin etmek ve riske tahammül edilip edilemeyeceğini karar vermek için kullanılan prosesin tamamı.
DÖF: Düzeltici Önleyici Faaliyet

4. UYGULAMA
4.1 Varlık Tanımı ve Riskleri (ISO/IEC27005 Standardına göre)
4.1.1 Ana Varlıklar
- İş Süreçleri
- Bilgi

4.1.2 Destekleyici Varlıklar
- Donanım
- Yazılımlar
- Ağ
- Personel (Çalışanlar)
- Konum
- Organizasyon

4.1.3 Varlık Envanteri ve Varlık Sahipliğinin Gözden Geçirilmesi
Varlık Envanterindeki varlıklar sahiplenmiş olmalıdır. Varlık sahibi kişiler veya unvanları olabilir. Varlık sahibi ilgili varlığın mülkiyet haklarına sahip olma zorunluluğu yoktur. Varlık sahibi kısmi olarak varlığa ilişkin sorumlulukları kurum içi organizasyonda yer alan kişilerle paylaşabilir fakat ana sorumluluk varlık sahibinde olacaktır. Varlık sahipliği belirleme çalışmaları bir süreç olarak değerlendirilmeli ve yeni bir varlık envantere eklendiğinde, değiştirildiğinde ya da kuruma transfer edildiğinde varlıkların sahipleri atanmalıdır.

ISO/IEC27005:2011 Standardında belirtilen ilgili varlıklara göre varlık envanteri ve risk değerlendirme tablosu hazırlanır.

4.1.3 Varlık Değerinin Belirlenmesi

Gizlilik: Bilginin içeriğinin görüntülenmesinin, sadece bilgiyi/veriyi görüntülemeye izin verilen kişilerin erişimi ile kısıtlanmasıdır. (Ör: Şifreli e-posta gönderimi ile e-postanın ele geçmesi halinde dahi yetkisiz kişilerin e-postaları okuması engellenebilir)

Bütünlük: Bilginin yetkisiz veya yanlışlıkla değiştirilmesinin, silinmesinin veya eklemeler

çıkarmalar yapılmasının tespit edilebilmesi ve tespit edilebilirliğin garanti altına alınmasıdır. (Ör: Veri tabanında saklanan verilerin özet bilgileri ile saklanması, dijital imza)

Erişilebilirlik/Kullanılabilirlik: Varlığın ihtiyaç duyulduğu her an kullanıma hazır olmasıdır. Diğer bir ifade ile, sistemlerin sürekli hizmet verebilir halde bulunması ve sistemlerdeki bilginin kaybolmaması ve sürekli erişilebilir olmasıdır. (Ör: Sunucuların güç hattı dalgalanmalarından ve güç kesintilerinden etkilenmemesi için kesintisiz güç kaynağı ve şasilerinde yedekli güç kaynağı kullanımı). Bu dokümanda "**Erişilebilirlik**" olarak kullanılacaktır.

ERİŞİLEBİLİRLİK		
OLASILIK		**DERECELENDİRME BASAMAKLARI**
1	**DÜŞÜK**	Varlığa bir zarar gelmesi durumunda GİZLİ bilgiye erişilebilir. Erişilebilirliğine zarar gelen GİZLİ seviyesi altındaki bilgi kurumu etkilemez / çok az etkiler.
2	**ORTA**	Varlığa bir zarar gelmesi durumunda GİZLİ bilgiye erişilebilir. Erişilebilirliğine zarar gelen GİZLİ seviyesi altındaki bilgi kurumu etkiler. Etki orta vadede telafi edilebilir.
3	**YÜKSEK**	Varlığa bir zarar gelmesi durumunda GİZLİ bilgiye erişilemez. Erişilebilirliğine zarar gelen bilgi kurumu etkiler. Etki telafi edilemez ya da uzun vadede telafi edilebilir.

BÜTÜNLÜK		
OLASILIK		**DERECELENDİRME BASAMAKLARI**
1	**DÜŞÜK**	Varlığa bir zarar gelmesi durumunda GİZLİ bilgi kontrol dışı değişmez. Kontrol dışı değişen GİZLİ seviyesi altındaki bilgi kurumu etkilemez / çok az etkiler.
2	**ORTA**	Varlığa bir zarar gelmesi durumunda GİZLİ bilgi kontrol dışı değişmez. Kontrol dışı değişen GİZLİ seviyesi altındaki bilgi kurumu etkiler. Etki orta vadede telafi edilebilir.

3	**YÜKSEK**	Varlığa bir zarar gelmesi durumunda GİZLİ bilgi kontrol dışı değişir. Kontrol dışı değişen GİZLİ bilgi kurumu etkiler. Etki telafi edilemez ya da uzun vadede telafi edilebilir.
GİZLİLİK		
OLASILIK		**DERECELENDİRME BASAMAKLARI**
1	**DÜŞÜK**	Varlığa bir zarar gelmesi durumunda GİZLİ bilgi açığa çıkmaz. Açığa çıkan GİZLİ seviyesi altındaki bilgi kurumu etkilemez /çok az etkiler.
2	**ORTA**	Varlığa bir zarar gelmesi durumunda GİZLİ bilgi açığa çıkmaz. Açığa çıkan GİZLİ seviyesi altındaki bilgi kurumu etkiler. Etki orta vadede telafi edilebilir.
3	**YÜKSEK**	Varlığa bir zarar gelmesi durumunda GİZLİ bilgi açığa çıkar. Açığa çıkan GİZLİ bilgi kurumu etkiler. Etki telafi edilemez ya da uzun vadede telafi edilebilir.

Varlık Değeri : Gizlilik * Bütünlük * Erişilebilirlik hesaplamasına denk gelir.

4.1.3 Varlık Değerlemesine Göre Sınıflandırma-Etiketleme

4.1.3.1 Kurum sistemlerinde ve kullanıcı bilgisayar ve cihazlarında tutulan dijital ve yazılı tüm bilgi, veri gizliliği sınıflandırmasına tabidir ve "Gizli", "Hizmete Özel" ve "Kamuya Açık" olmak üzere üç seviyeye ayrılmıştır. Bilginin türüne göre gizlilik seviyesinin belirlenmesi **Resmi Yazışmalarda Uygulanacak Usul Ve Esaslar Hakkındaki Yönetmeliğe** ve ilgili mevzuat hükümlerine göre yapılacaktır.

"Temiz Masa Politikası" gereğince çalışanlardan gün sonunda masalarında, printer ve fax makinalarında, ortak kullanım alanları ve toplantı salonlarında hiçbir bilgi varlığı bırakmamaları, dolap ve çekmecelerinde belirtilen şekilde saklamaları beklenmektedir.

4.2 Risk Değerlendirme Yöntemi

4.2.1 Varlık Envanteri ve Risk Analizinde kapsam dahilindeki tüm birimler BGYS yi tehdit eden tehlikeler için risk puanı hesaplanır.

4.2.2 Risk puanının değerlendirilmesi, risk derecelendirme tablosuna göre yapılır:

Risk Derecelendirme (Risk Seviyesi) Tablosu:

	ŞİDDET				
OLASILIK	**1**	**2**	**3**	**4**	**5**
1	**Düşük seviye risk 1**	**Düşük seviye risk 2**	**Düşük seviye risk 3**	**Düşük seviye risk 4**	**Düşük seviye risk 5**

2	**Düşük seviye risk 2**	**Düşük seviye risk 4**	**Düşük seviye risk 6**	**Orta seviye risk 8**	**Orta seviye risk 10**
3	**Düşük seviye risk 3**	**Düşük seviye risk 6**	**Orta seviye risk 9**	**Orta seviye risk 12**	**Orta seviye risk 15**
4	**Düşük seviye risk 4**	**Orta seviye risk 8**	**Orta seviye risk 12**	**Yüksek seviye risk 16**	**Yüksek seviye risk 20**
5	**Düşük seviye risk 5**	**Orta seviye risk 10**	**Orta seviye risk 15**	**Yüksek seviye risk 20**	**yüksek seviye risk 25**

4.2.3 Hesaplanan risk puanı sonucunda tüm tehlikeler için riskin tolere edilebilirliğine karar vermek için aşağıdaki tablo kullanılır:

EYLEM MATRİSİ	
SONUÇ	**EYLEM**
16-25	**KABUL EDİLEMEZ RİSK** **Bu risklerle ilgili hemen çalışma yapılmalı**
8-15	**DİKKATE DEĞER RİSK** **Risklere mümkün olduğunca çabuk müdahale edilmeli**
1-6	**KABUL EDİLEBİLİR RİSK** **Acil tedbir gerekmeyebilir**

-Risk puanı 1 ile 6 arasında olan tüm tehditler "Kabul Edilebilir Risk" olarak tanımlanmıştır ve Acil tedbir gerekmeyebilir.
-Risk Puanı 8 ile 15 arasında olan tüm tehditler için "Dikkate Değer Risk" olarak tanımlanmıştır ve Risklere mümkün olduğunca çabuk müdahale edilmelidir.
-Risk Puanı 16 ile 25 arasında olan tüm tehditler "Kabul Edilemez Risk" olarak tanımlanmıştır ve Bu risklerle ilgili hemen çalışma yapılmalıdır.

4.2.4 Risk Puanının Hesaplanması: Risk Analiz Metodolojisinde;

Risk puanının hesaplanmasında; **Risk Puanı = Olasılık * Şiddet** formülü kullanılır.

Bu formüle göre teorik olarak elde edilebilecek en yüksek değer 25 puandır.

Mevcut risk analiz çalışmaları neticesinde maksimum kabul edilebilir risk puanı 6 olarak belirlenmiştir.

Mevcut Riskler gizlilik, bütünlük, erişebilirlik (G,B,E) bakımından ayrı ayrı şiddetleri değerlendirilir.

Üst yönetim ile yapılacak değerlendirme neticesinde; risk üst yönetim tarafından kabul edilir ve gerekli iyileştirme çalışmalarının başlatılması için onay verilir. Onay verilmesi halinde, ilgili varlık sahibi bölüm / birim yönetimi öncülüğünde iyileştirici faaliyetler planlanarak hayata geçirilir.

İyileştirici faaliyet neticesinde risk değerlendirmesi tekrarlanır. Söz konusu risk puanının kabul edilebilir seviyenin üzerinde kalması durumunda aynı süreç tekrarlanır veya bütçe, altyapı, personel durumu uygun değilse Üst Yönetim bu risk sonucunu kabul eder.

Olasılık (Sıklık) derecesi: Faaliyet sırasında riskin meydana gelme, oluşma sıklığını ifade eder.

Şiddetin derecesi: Faaliyet sırasında meydana gelebilecek riskin şiddetini ifade eder.

Olasılık ve Şiddet için puan verilirken aşağıdaki tablolar kullanılır:

BİR RİSK OLAYININ GERÇEKLEŞME OLASILIĞI

OLASILIK		DERECELENDİRME BASAMAKLARI
1	ÇOK KÜÇÜK	HEMEN HEMEN HİÇ
2	KÜÇÜK	ÇOK AZ (YILDA 1 KEZ), SADECE ANORMAL DURUMLARDA
3	ORTA	AZ (YILDA BİRKAÇ KEZ)
4	YÜKSEK	SIKLIKLA (AYDA BİR)
5	ÇOK YÜKSEK	ÇOK SIKLIKLA (HERGÜN, HAFTADA BİR) NORMAL ÇALIŞMA ŞARTLARINDA

ŞİDDET TABLOSU

DEĞER	ANLAM	AÇIKLAMA		
		GİZLİLİK	BÜTÜNLÜK	ERİŞİLEBİLİRLİK
1	ÇOK HAFİF	Gizli bilgiye erişim imkanı vermez.	Bilgi bütünlüğü bozulmaz	Erişilebilirlik etkilenmez
2	HAFİF	Şirkete açık bilgiler şirket dışına çıkabilir	Bilgi bütünlüğü kısmen ve geri dönüşü kolay olacak şekilde bozulabilir	Erişilebilirlik kısmen ve kabul edilebilir kesinti süresi dahilinde gerçekleşebilir

3	**ORTA**	Gizli seviyeli bilgiler kısmen dışarı çıkar	Bilgi bütünlüğü kabul edilebilir veri kaybı dahilinde bozulabilir	Kesinti kabul edilebilir kesinti süresi içinde giderilemez fakat maksimum kesinti süresi içerisinde kesinti son bulur
4	**CİDDİ**	Çok gizli bilgiler dışarı çıkabilir ve kontrol edilemez	Bilgi varlıkları kaybolmaya/yetkisiz değiştirmeye açık hale gelir, kontrol edilemez	Erişilebilirlik kabul edilebilir seviyelerin üzerinde hasar görür, kontrol edilemez.
5	**ÇOK CİDDİ**	Çok gizli bilgilere direk erişim verir, yıkıcı olur	Bilgi bütünlüğü geri dönülemez şekilde bozulur, yıkıcı olur	Sistem erişimi tamamen ve kabul edilemez bir süre durur, yıkıcı olur

4.3 Risk işleme Planının Hazırlanması
Risk analizi dokümanında risklerin işlenmesine ilişkin varsa Düzeltici Faaliyet numarası yer alır. Üst yönetim Risk Analiz Raporunu değerlendirir.

Aşağıdaki seçeneklerden birini o risk satırı için seçer. Eğer "İşleme" seçeneği seçilirse o seçenek için seçilmiş kontrol kriterleri ve kriterler için tanımlanmış önlemler, planlar, faaliyetler, satın alımı önerilen donanım, yazılım, ekipman veya hizmetlerin kurum tarafından dahili veya harici olarak tedarik edileceği anlamına gelir.

Yönetim onayı olmadan Risk İşleme Planı uygulanamaz. Karar verilirken iş etkileri ve öncelikleri dikkate alınır. Risk işleme için dört seçenek mevcuttur.

4.3.1 İşleme (azaltma, hafifletme, tedavi): Riskleri azaltmak için uygun kontrollerin seçilmesi ve uygulanmasıdır. Açıklanan kontrol önerileri de dikkate alınarak uygun kontroller seçilir. Seçilen kontrollerin maliyet-fayda karşılaştırmasına, uygulanabilirliğine, sürdürülebilirliğine ve yönetilebilirliğine bakılarak uygun olanları seçilir ve uygulanır.

4.3.2 Kabul: Kabul seçeneği içinde üç farklı değerlendirmeyi taşımaktadır:

1-Kurumun politikalarını ve risk kabul kriterlerine uymak koşuluyla bazı riskler kabul edilebilir. Risk puanı kabul edilebilir seviyenin altında olanlar ve kabul edilebilir seviyeye yakın olanlar bu işleme tabi tutulurlar.

2-Risk değeri "Kabul edilebilir Risk Seviyesinin üstünde olabilir. Ancak "(Risk Önleme Maliyeti / Risk sonucu) bütçe, altyapı, personel durumu uygun değilse Yönetim bu risk sonucunu kabul edebilir.

3-Risk İşleme sonucu bile risk kabul edilebilir seviyenin altına inmiyorsa "Artık Risk Üstlenme Beyanı" ile riskin sonuçlarını üstlenerek kabul edebilir.

4.3.3 Kaçınma: Risklerin çeşitli nedenlerle kontrol edilememesi ve kabul edilememesi durumunda uygulanır. Riskin kaynağı olan tehdidin gerçekleşme olasılığının ve iş etkisinin çok yüksek olduğu durumlarda riskten uzaklaşmak için her tür çaba, düzenleme, donanım, yazılım, ekipman, hizmet alımları gerçekleştirilir veya risk kaynağı uygulamalar devreden çıkarılır. İnternet saldırıları için internet bağlantısının kesilmesi gibi, deprem tehdidinden dolayı çalışma ortamını değiştirmek, taşımak gibi.

4.3.4 Transfer: Kurumun yönetiminde ve kontrolünde olmayan varlık ve fonksiyonlarla ilgili ve kurumun müdahale edemeyeceği konularla ilgili riskler başka kurumlara transfer edilir. Örneğin

yangın, doğal afet, hırsızlık gibi tehditlerin azaltılması için yapılan kontrollerden sonra kalan artık risk itfaiye, sigorta şirketi, AKUT, emniyet güçleri vb. kurumlara aktarılır.

Seçilen uygun risk işleme kararları risklerin takibi için risk işleme planına kaydedilir. Risk işleme planı sürekli güncellenerek uygulanan kontrollerin durumu kayıt altına alınır.

4.4 Artık Risk Onayı

Düzeltici faaliyet çalışması tamamlandıktan sonra bile kabul edilen risk seviyesinin altına düşmeyen riskler için

"Artık Risk Üstlenme beyanı" üst yönetim tarafından yapılır. Bir önceki yılda hazırlanmış beyandaki artık riskler devam ettirilebilir, çıkarılabilir veya yeni artık riskler eklenebilir. Artık Risk Üstlenme Beyanının tüm sorumluluğu ve sonuçları üst yönetime aittir.

4.5 Gözden geçirme ve izleme

Risk işleme planı her yıl en az bir kez veya majör mekân, altyapı, personel, teknik, yasal değişikliklerden sonra yapılacak olan risk değerlendirmeleri çalışması ile birlikte gözden geçirilir. Riskler uygun seviyelerin altına inmesinden sonra rutin kontrol seviyesinde takip edilirler.

İç denetim sırasında BGYS sistemini etkileyen uygunsuzluklar düzeltici faaliyet ile izlenebilir ya da risk işleme planına dahil edilir.

	HAZIRLAYAN	ONAYLAYAN
ÜNVANI	BGYS YÖNETİM TEMSİLCİSİ (DAİRE BAŞKANI)	GENEL SEKRETER
ADI SOYADI	Dr. Naci BAYRAK	Prof.Dr. Ahmet DUMLU
İMZA		