Revizyon İzleme Tablosu		
Rev. No	**Rev. Tarihi**	**Açıklama**
00	03.09.2018	İlk Yayın
01	07.09.2021	Memnuniyet Durumu ve Performans Yüzdelerinin güncellenmesi

1. AMAÇ

Bu prosedürün amacı, Bilgi Güvenliği Yönetim Sistemi (BGYS) uygulamaları kapsamında iş sürekliliği açısından varlık değeri olan iş bileşenlerine iç veya dış kaynaklı olarak gelebilecek tehlikeler ve bu tehlikelerin gerçekleşmesi durumunda ortaya çıkabilecek maddi veya manevi iş kayıplarını tespit edecek yöntemler ve gerekli önlemlerin planlanması için izlenecek yolu belirlemektir.

2. SORUMLULUK

Bu prosedürün uygulanmasından Bilgi İşlem Daire Başkanı ve BGYS ekibi başta olmak üzere tüm birim çalışanları doğrudan sorumludur.

Ayrıca, Bilecik Şeyh Edebali Üniversitesi Yönetimi tarafından, planlanan BGYS yapısında risk analizi sonucu, risk faktörünün bertaraf tedbirleri sonrasında dahi bertaraf edilemeyen risklerin varlığı Artık Risk Onay Formu uyarınca kabul edilmektedir.

3. PROSEDÜR

3.1. Birim Varlıklarının Belirlenmesi

İşin gerçekleştirilmesi için ve iş sürekliliği için gerekli olan tüm maddi ve manevi varlıklar birim varlıklarını oluştururlar. Bu varlıklar; kullanım amaçları, bilgi içerikleri, işe etkileri, maddi ve manevi değerleri ile zayıflıklara karşı tehdit altında olabilirler. Birim bünyesinde varlıklarımız şu şekilde sınıflandırılır ve tanımlanır.

SIRA NO	VARLIK SINIFI	AÇIKLAMA
1.	Fiziksel Varlıklar	Faaliyetlerimizi gerçekleştirmede kullanılan her türlü bina, ofis, ekipman ve eşyalar, binalar arası bağlantılar, her türlü bilgisayar programı, işletim sistemi ve yardımcı yazılımlar ile sunucular bileşenleri temsil eder.
2.	Doküman Varlıklar	Projelerin gerçekleştirilmesinde kullanılan, birim içinde üretilen ve kurumsal hafızayı oluşturan tüm dokümanları ifade eder.
3.	İnsan Kaynakları	Faaliyetlerimizi gerçekleştirirken farklı pozisyonlarda görev yapan ve iş sonuçlarına direkt veya doğrudan etkisi olan tüm personeli ifade eder.
4.	İlgili (Üçüncü) Taraflar	Faaliyetlerimizi gerçekleştirmede kullanılan,hizmet alınan ve sağlanan tüm paydaşları kapsar.

Kurumumuz Bilgi Güvenliği Envanteri' nde yer alan doküman varlıklar özelliklerine göre (Gizli, İvedi, Günlü vb.)kurumda kullanılan elektronik yazışma sistemi tarafından

"Resmi Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik"e uygun olarak etiketlenirler.

3.2. Varlıkların Keşfi ve Değerlendirilmesi

Kurum içerisindeki tüm varlıklar Varlık envanterinde belirtilir. Varlık değeri belirlenirken BGYS Temeli olan Gizlilik, Bütünlük ve Erişebilirlik açısından değerlendirme yapılır. Bu değerlendirme aşağıdaki yöntem ile belirlenir.

VARLIK DEĞER ARALIĞI (V) =ORT(G , B , E)

3.2.1. Gizlilik Etki Seviyeleri(G)

Çok Yüksek(5)	Çok gizli bilgi içeren varlıklar.
Yüksek (4)	Gizli bilgi içeren varlıklar.
Orta (3)	Birim personelinden ilgili personellerin bu bilgilere sahip olabileceği varlıklar.
Düşük (2)	Tedarikçi ve taşeronların ya da ziyaretçilerle paylaşılması sıkıntı olmayacak bilgi varlıkları.
Çok düşük(1)	Halkın bilgisi dahilinde olabilecek veya herkesle paylaşılabilecek seviyedeki bilgi varlıkları.

3.2.2.Bütünlük Etki Seviyeleri(B)

Çok Yüksek(5)	Bilginin %100 bütün halinde ulaşılması gereken bilgi varlıkları.
Yüksek (4)	Bilgi bütünlüğünde yaşanan aksaklığın birimimize etki ettiği, işin durmasına, işin aksamasına veya itibar kaybına sebep olan bilgi varlıkları.
Orta (3)	Bilgi bütünlüğünde yaşanan aksaklığın birimimize kısmen etki ettiği, işin gecikmesine sebep olabilecek fakat kritik seviyede etki etmeyecek bilgi varlıkları.
Düşük (2)	Bilgi bütünlüğünün olmaması sonucu birime etki etmeyen fakat başka varlıklarla ikame edebilecek bilgi varlıkları.
Çok Düşük(1)	Bilginin bütünlüğü önemli olmayan varlıklar.

3.2.3. Erişilebilirlik Etki Seviyeleri(E)

Çok Yüksek(5)	Bilgiye %100 erişilmesi gerekli bilgi varlıkları.
Yüksek (4)	Bilgiye erişilemediğinde yaşanan aksaklığın birimimize etki ettiği, işin durmasına, işin aksamasına veya itibar kaybına sebep olan bilgi varlıkları.
Orta (3)	Bilgiye erişilemediğinde yaşanan aksaklığın birimimize kısmen etki ettiği, işin gecikmesine sebep olabilecek fakat kritik seviyede etki etmeyecek bilgi varlıkları.
Düşük (2)	Bilgiye erişimin olmaması sonucu birime etki etmeyen fakat başka varlıklarla ikame edebilecek bilgi varlıkları.
Çok Düşük(1)	Bilgiye erişiminin önemli olmadığı varlıklar.

Varlık değer aralığı 1-5 arasında değişmektedir. Varlık değerleri aşağıdaki tabloya göre belirlenir.

VARLIK SINIFI	VARLIK DEĞERİ
Çok gizli	5
Gizli	4
İç kullanım	3
Halka açık	2
Önemsiz Bilgi	1

3.3. Risk Analiz Metodolojisi

Kurumumuzda bulunan tüm demirbaşların envanteri, kamu kurumlarınca kullanılan KBS-Taşınır Kayıt ve Yönetim Sistemi üzerinde tutulur. Ofislerde bulunan masa, sandalye vd. ofis malzemeleri ile depoda bulunan (aktif olmayan) her türlü bilişim ürünü birim ayniyat sorumlusu tarafından sayılarak sisteme eklenir ve takibi yapılır. Bunun dışında, personel kullanımında olan bilişim ürünlerinin envanteri ise online envanter yazılımları aracılığıyla toplanarak yine birim ayniyat sorumlusu tarafından KBS sistemine eklenir. Varlıkların özellikleri olabildiğince detaylı yazılır. Varlığın bulunduğu yer (lokasyon olarak) belirtilir.

Varlık envanterinde belirtilen tehditlerin ortalaması alınarak o varlık için BGYS Ekibi tarafından onaylanan iş etki değeri ile çarpılır ve Varlık Envanterindeki Risk Değeri bölümüne çıkan puan işlenir.

Bilgisayar, telefon, projeksiyon cihazlarının yönetimi, kamu sistemleri dışında Bilgi İşlem Daire Başkanlığınca kullanılan BİS, OCS, IPAY, IPTYS sistemlerinden de takip edilmektedir. Varlıklar BİS sisteminde destek kayıtlarıyla da ilişkilendirilir.

Açıklıkların kapatılması için varlıkların üzerlerindeki tehditler ve standardın öngördüğü kontroller risk işleme için öncelikle dikkate alınır.

3.4. Risk Değerlendirme Metodolojisi

İş etkisi değerlendirilirken varlığın iş üzerindeki kesinti etkisi, yerine koyma maliyeti, bilginin gizliliği, kurum itibarına olan etkisi, yasal ve hukuki yükümlülükler bakımından yaratacağı zarar (kullanıcıya ait bilgi gibi) konuları ele alınmalıdır.

Olasılık aralığı tespit edilirken zayıflıkların çokluğu ve var olan kontrollerin bu zayıflıkları ne kadar kapatabildiği, tehdit biçiminin uygulanma kolaylığı, bilginin cazibesi, personelin psikolojisi, uygulamanın hassas ve kontrol edilemeyen (politikaya uymama-kuralın etrafından dolaşma) çalışan davranışı gibi unsurlar değerlendirilmelidir.

3.5. RİSK BÜYÜKLÜĞÜNÜN HESAPLANMASI

KRİTİK VARLIK DEĞERİ		OLASILIK (B)			ETKİ (C)		
Varlık Değer Aralığı	Varlık Değeri (A)						
5	5	Çok Yüksek	Ayda bir	5	Çok Büyük	Prestij Kaybı	5
4	4	Yüksek	Üç ayda bir	4	Büyük	Maddi zarar	4
3	3	Ara sıra	Altı ayda bir	3	Normal	Veri(belge) Kaybı	3
2	2	Az	Yılda bir	2	Küçük	Bilgide Zedelenme	2
1	1	Çok az	Yılda bir den daha az	1	Çok Küçük	Bilgi Ulaşımında Gecikme	1
Risk (R) = A x B x C							

3.6. RİSK ETKİ BÜYÜKLÜKLERİNİN SINIFLANDIRILMASI VE DEĞERLENDİRİLMESİ

Risk Büyüklüğü (R)	Risk Derecesi	Değerlendirme	Renk
126-100	Çok Yüksek Risk	Acil Önlem Alınmalı	KIRMIZI
99-60	Yüksek Risk	Hemen Çalışma Yapılmalı	MAVİ
59-27	Dikkate Değer Risk	Mümkün Olduğunca Çabuk Müdahale Edilmeli	YEŞİL
26-0	Kabul Edilebilir Risk	Acil Tedbir Gerektirmeyebilir, Dikkatli Olunmalı	ŞEFFAF

Bulunan iş etki değeri ile risk puanı yüksek, orta ve düşük seviyelerde Risk Değerlendirme Tablosu üzerinde ilgili aralıkta puanlanır. Kabul edilebilir risk seviyesinden yukarı çıkması durumunda düzeltici tedbirler alınarak yeniden risk değerlendirmesi yapılır ve kabul edilebilir risk seviyesine düşürülür. Kabul edilebilir risk seviyesine çekilemeyen riskler artık risk olarak değerlendirilir ve artık risk onayıyla kurum yetkilisi tarafından onaylanır.

3.7. Risk İşleme Metodolojisi

Risk değerlendirme sonucunda tüm varlıklarla ilgili risk değerleri tespit edilir. Bu değerlendirme sürekli olarak yapısal, organizasyonel ve uygulama değişiklikleri çerçevesinde izlenir veya en az yılda 1 kez gözden geçirilir ve değişken risk sürekli yeniden hesaplanır. Risk işleme seçenekleri şunlardır: Risk kabul, riskten kaçınma, riskin işlenmesi ve riskin transferi.

Kabul edilebilir risk seviyesi yönetim tarafından 0-26 puan arası (26 dahil) riskler olarak tanımlanmıştır. Tüm varlıklar için hedefimiz riskleri bu aralığa çekmektir. Aksi belirtilmedikçe bütün risklerin işlenmesi ve azaltılması birincil aksiyondur. Bazı riskler bu seviyeye çekilemediğinde bunların göze alınması ve riskin kabulü yönetim tarafından yapılabilir.

Uygulama düzeyinde riski azaltamadığımız ve yönetimce kabul edilemez riskler için riskten kaçınma opsiyonu geçerlidir. Riske neden olan uygulamadan vazgeçilmesi ve iş sürecinin ve prosedürünün farklılaştırılması risk işleme seçeneklerinden bazılarıdır.

Riskin kuruluşumuz kontrollerini aştığı durumlarda (yangın, deprem, sabotaj, afet, soygun vb.) emniyet güçleri, kamu acil durum kurumları, sigorta kurumlarına risk transfer edilir.

Risk işlemede birincil aksiyon kontrollerin seçilmesidir. Kontroller; uygulayıcısının ve bu uygulamayı izleyip ölçecek ilgili amirin görüşlerinin alınması, konuyla ilgili teknik iç-dış uzmanların ve danışmanların görüşlerinin alınması ile seçilir. Seçilen kontroller ISO 27001 Standardının EK-A bölümündeki 11 başlıktan ve 133 alt maddeden seçilmeye çalışılır. Burada kontrol amaçları ve kontrollerin ifadesi yer alır. Bu kontrollerin teknik düzeyde nasıl uygulanacağı konu uzmanları ve kontrolü uygulayacak kişilerin seçimiyle oluşturulur. Seçilen en uygun kontrolün maliyeti tespit edilir ve riski azaltılacak varlıkla ilgili yapılan varlık değerlemesi ve iş etkisinden dolayı potansiyel mali zararla kıyaslaması yapılır. Fayda maliyet analizi sonucu seçilen kontrolün uygulanabilir olup olmadığına karar verilir. Uygulanabilir kontroller hayata geçirilir. Uygulanabilir olmayan kontroller için tekrar gözden geçirme yapılarak fayda maliyet dengesi sağlanana kadar araştırma süreci devam eder.

Uygulanan kontrol ile ilgili kayıtlar risk işleme planında belirtilir. Maliyetler ve alınan sonuçlar BGYS forumlarında görüşülür ve riskin yeni durumda ölçüm sonucu risk işleme planındaki ilgili yere yazılır.

Risk puanı kabul edilebilir seviyeye çekilene kadar gerekiyorsa yeni kontroller uygulanır ve ölçümlere devam edilir.

3.8. Tedarikçi Performans Değerlendirme

Tedarikçiler, hız, teslimat süresi, yanlış/hatalı ürün kategorilerine göre 1-5 arasında puanlanır. Puanlamada, 1 en düşük (olumsuz), 5 ise en yüksek (en olumlu) durumu ifade etmektedir. Yapılan değerlendirmeler “Tedarikçi Değerlendirme Formu”na işlenir.

Aşağıdaki tablo kullanılarak A firması için örnek bir performans değerlendirmesi yapılmıştır:

A firması	**5**	**4**	**3**	**2**	**1**
Hız		X			
Teslimat süresi	X				
Doğru ürün teslimi			X		
TOPLAM	12				
PERFORMANS (%)	(12/15)*100				

Memnuniyet Durumu/Performans Yüzdesi

Memnuniyet Durumu	**Performans Yüzdesi (%)**
Çok kötü	0-20
Kötü	21-40
Orta	41-60
İyi	61-80
Çok iyi	81-100

3.9. Tehdit Listesi

TEHDİT	T. No
Ataklar	T.01
Bakım Hataları	T.02
Bilgi alışverişindeki yetersiz anlaşmalar	T.03
Bilgi Güvenliği farkındalık eksikliği	T.04
Bilgi içeren dokumanların çöpe atılması	T.05
Bilgi İçeren elektronik verilerin çöpe atılması	T.06
Bilgi işlem olanaklarının yetkisiz veya yanlış kullanımı	T.07
Bilginin sınıfılandırılması hatası	T.08
Yetkisiz fiziksel erişim	T.09
Yetkisiz erişim	T.10
Müdahale / Kasıtlı zarar	T.11
Cross-site scripting attacks (XSS) / SQL enjeksiyonu	T.12
Çalışanın güvenlik ihlaleri	T.13

Çalışma Ortamı, nem, sıcaklık, toz, kir	T.14
Çıktı halindeki bilginin yetkisiz kişilerce okunması	T.15
Destek servislerinin kesintisi	T.16
Dış kaynaklı ilgili güvenlik ihlaleri (destek firmaları)	T.17
Doğal afetler, yangın, su baskını, yıldırım	T.18
Donanım arızası	T.19
Elektrik kesintisi	T.20
Elektrostatik yükleme	T.21
Elektriksel dalgalanmalar	T.22
Fiziksel etki (düşme, kırılma)	T.23
Gizli bilgilerin personel tarafından dışarıya bildirilmesi	T.24
Güvenlik kontrolleri ile uyumsuzluk	T.25
Güvenlik politikası ile ilgili ihlaller	T.26
Hatalı bilgi çıkışı	T.27
Hırsızlık	T.28
Internet kesintisi	T.29
Kablo hasarları	T.30
Kamera görüntülerinin kurum dışına sızması	T.31
Kapasite aşımı	T.32
Kaza veya arızalardan oluşabilecek hasar	T.33
Kemirgen / haşereler	T.34
Kötü niyetle istifade (Fraud)	T.35
Kriptografi (Şifreleme) politikası eksikliği	T.36
Kullanıcı hataları	T.37
Yönetici hataları	T.38
Kuruma ait bilgilerin özel amaçlarla kullanımı	T.39
Log Dosyalarının yanlışlıkla yada kasten değiştirilmesi	T.40
Onaylanmamış doğru olmayan bilginin yayınlanması	T.41
Onaylanmamış ve test edilmemiş bilgi sistem değişiklikleri	T.42
Operasyonel zorluklar, tedarik zincirinde eksiklik, yoğun işgücü	T.43
Su ile temas	T.44
Şifreleme anahtarının ele geçirilmesi	T.45
Şifreleme anahtarının/algoritmasının yetersiz duzeyde olması	T.46
Taşıma sırasında yedekleme medyasına gizli ulaşım veya kopyalama	T.47

Unutulmuş erişim hakları	T.48
Unutma	T.49
Uygun olmayan kimlik tanıma mekanizması (authenticate)	T.50
Veri medyalarının elden çıkarılması sırasında güvenlik eksikliği	T.51
Veri tabanının zarar görmesi	T.52
Virüs, solucan vb. tehditler	T.53
Yanlış ve yeniden yönlendirilen mesajlar (re-route)	T.54
Yasal düzenlemelerle uyumsuzluk	T.55
Yasal olmayan dosya yükleme	T.56
Yazılım kaynak kitaplığına yetkisiz erişim	T.57
Yazılım lisans bilgilerini yetkisiz kopyalama	T.58
Yetersiz ve test edilmemiş veri yedekleri	T.59
Yazılımda değişiklik	T.60
Zararlı ActiveX kurulumu	T.61
Zararlı dosya yükleme	T.62
Tayin / Terfi / Yer değişikliği	T.63
Hastalık geçici iş görememezlik	T.64
Bakım / Kalibrasyon hataları	T.65
Bakım Hataları / Test eksikliği	T.66
Bilgi güvenliği farkındalık eksikliği	T.67
Bilgi Güvenliği İhlalleri-Sistem yedeği	T.68
Bilgi Güvenliği İhlalleri-Fiziksel güvenlik	T.69
Bilgi Güvenliği İhlalleri-VPN erişimi	T.70
Bilgi Güvenliği İhlalleri-İnternet erişimi	T.71
Bilgi Güvenliği İhlalleri-Personel tecrübesi	T.72
Bilgi Güvenliği İhlalleri-3.Taraf yazılımlar	T.73
Bilgi Güvenliği İhlalleri-3.Taraf ortak ağ	T.74
Bilgi Güvenliği İhlalleri-Yama yönetimi	T.75
Bilgi Güvenliği İhlalleri-Yetersiz ağ	T.76
Bilgi Güvenliği İhlalleri-Yetersiz erişim	T.77
Bilgi Güvenliği İhlalleri-Yetki ve sorumluluklar	T.78
Bilgi güvenliğine yönelik saldırıların gelmesi	T.79
Bilgi işlem olanaklarının yetkisiz veya yanlış kullanımı	T.80
Bilgi işlem olanaklarının yetkisiz veya yanlış kullanımı	T.81

Bilgi Sızması-Yedeklilik	T.82
Bilgi Sızması-Dış Kaynaklı Personel	T.83
Bilgi Sızması-Domaine Dahil Olmama	T.84
Bilgi Sızması-Fiziksel güvenlik	T.85
Bilgi Sızması-VPN erişimi	T.86
Bilgi Sızması-İnternete açık olma	T.87
Bilgi Sızması-Düzenli bakım yapılmama	T.88
Bilgi Sızması- 3.Taraf entegresyon	T.89
Bilgi Sızması-Ortak ağ	T.90
Bilgi Sızması-Yama yönetimi	T.91
Bilgi Sızması-Ağ güvenliği	T.92
Bilgi Sızması-Erişim denetimi	T.93
Bilgi Sızması-Etiketleme	T.94
Bilgi Sızması-Yazıcı çıktıları	T.95
Bilgi Sızması-Gizlilik anlaşmalarının olmaması	T.96
Bilgi Sızması-Güvenlik açığı	T.97
Bilgi Sızması-İmha edilme	T.98
Bilginin Değiştirilmesi-Sistem yedekliliği	T.99
Bilginin Değiştirilmesi-Düzenli yedek almama	T.100
Bilginin Değiştirilmesi-Fiziksel güvenlik	T.101
Bilginin Değiştirilmesi-İnternete açık	T.102
Bilginin Değiştirilmesi-Log yönetimi	T.103
Bilginin Değiştirilmesi-Personel tecrübesi	T.104
Bilginin Değiştirilmesi-3.Taraflar ortak ağ	T.105
Bilginin Değiştirilmesi-Erişim Denetimi	T.106
Bilginin Kaybolması-Yedek Almama	T.107
Bilginin Kaybolması-Fiziksel Güvenlik	T.108
Bilginin Kaybolması-VPN Erişimi	T.109
Bilginin Kaybolması-Mobil Olması	T.110
Bilginin Kaybolması-Düzenli Bakım	T.111
Bilginin Kaybolması-Tecrübe Eksikliği	T.112
Bilginin Kaybolması-Personel Yetersizliği	T.113
Bilginin Kaybolması-Personel Yedeği	T.114
Bilginin Kaybolması-3.Taraf Sorunlar	T.115

Bilginin Kaybolması-Erişim Denetimi	T.116
Bilginin Silinmesi-Dış Kaynaklı Personel	T.117
Bilginin Silinmesi-Domaine Dahil Olmama	T.118
Cihazların Çalışmaması-Yedeklemeler	T.120
Cihazların Çalışmaması-Dış Kaynaklı Personel	T.121
Cihazların Yanması-Yedekliliğin Olmaması	T.124
Çalışma Ortamı (Toz, Kir, Nem, Sıcaklık)	T.125
Veri tutarsızlığı	T.126
Destek servislerinin kesintisi	T.127
Enerji Kesintisi	T.128
Evrak Kaybolması	T.129
Giriş ve çıkış kablolarına müdahele	T.130
Gizli bilgilerin paylaşılması	T.131
Görüntü ve görüntü kayıtlarına yetkisiz erişim	T.132
Güvenlik Açıkları	T.133
Güvenlik kontrolleri eksiklikleri	T.134
Hasar Görme (Yanma, Islanma, Küflenme vb.)	T.135
Hatalı Ağ Konfigürasyon-Personel Tecrübesi	T.136
Hatalı Ağ Konfigürasyon-3.Taraf Yazılım Entegrasyonu	T.138
Hatalı Ağ Konfigürasyon-Yama Yönetimi	T.139
Hatalı Kurulum/Entegrasyon-Sistem Yedekliliği	T.141
Hatalı Kurulum/Entegrasyon-Düzenli Yedek Almama	T.142
Hatalı Yazılım Geliştirme/Yükleme-Dış Kaynaklı Personel	T.143
Hatalı Yazılım Geliştirme/Yükleme-Düzenli Yedekleme	T.144
Hatalı Yazılım Geliştirme/Yükleme-Fiziksel Güvenlik	T.145
Hatalı Yazılım Geliştirme/Yükleme-VPN Erişimi	T.146
Hatalı Yazılım Geliştirme/Yükleme-İnternete Açık Olması	T.147
Hatalı Yazılım Geliştirme/Yükleme-Log Yönetimi	T.149
Hatalı Yazılım Geliştirme/Yükleme-Personel Tecrübesi	T.150
Hatalı Yazılım Geliştirme/Yükleme-Personelin İşten Ayrılması	T.151
Hatalı Yazılım Geliştirme/Yükleme-3.Taraf Yazılım Entegrasyonu	T.152
Hatalı Yazılım Geliştirme/Yükleme-Yetersiz Ağ Güvenliği	T.153
Hizmet Yavaşlığı-İş Süreçleri	T.154
Hizmet Yavaşlığı-Personel Tecrübesi	T.155

İş Sürekliliğinin Sağlanamaması-Dış Kaynaklı Personel	T.156
İş Sürekliliğinin Sağlanamaması-Düzenli Yedek	T.157
İş Sürekliliğinin Sağlanamaması-Enerji Destek	T.158
İş Sürekliliğinin Sağlanamaması-Personel Tecrübesi	T.159
İş Sürekliliğinin SağlanamamasıPersonel Yetersizliği	T.160
İş Sürekliliğinin Sağlanamaması-Personel Yedeği	T.161
Kapasite aşımı	T.162
Kodların Çalınması-Dış Kaynaklı Personel	T.163
Kodların Çalınması-Domaine Dahil Olmama	T.164
Kodların Çalınması-Fiziksel Güvenlik	T.165
Kodların Çalınması-İş Süreçleri	T.166
Kodların Çalınması-Yetersiz Ağ Güvenliği	T.167
Kodların Çalınması-Yetersiz Erişim Denetimi	T.168
Kötü Amaçlı Kullanım-VPN Erişimi	T.169
Kötü Amaçlı Kullanım-İnternete Açık Olması	T.170
Siber Saldırı-Personel Tecrübesi	T.172
Siber Saldırı-3.Taraf Yazılımlar	T.173
Siber Saldırı-Yama Yönetimi	T.174
Siber Saldırı-Yetersiz Ağ Güvenliği	T.175
Siber Saldırı-Yetki ve Sorumluluklar	T.176
Siber Saldırı-Teknik Açıklık	T.177
Sistem Kesintisi-Domaine Dahil Olmama	T.178
Sisteme Virüs Bulaşması	T.179
Sistemlere Sızılması	T.180
Sistemlere Sızılması/Ele Geçirilmesi	T.181
Sistemlerin Çalışmaması-Yedekleme Olmaması	T.182
Sistemlerin Çalışmaması-Dış Kaynaklı Personel	T.183
Sistemlerin Çalışmaması-İnternete Açık Olması	T.184
Sistemlerin Çalışmaması-Yetki ve Sorumluluklar	T.185
Sistemlerin Çökmesi-Ddos Saldırı	T.186
Sosyal Medyada Kurum aleyhine propaganda yapılması	T.189
Standart Şartlarının Sağlanmaması	T.190
Tayin / Terfi / Yer Değişikliği	T.191
İşten ayrılma	T.192

Dosya formatlarının uyum sorunu	T.193
FM200 tüpü gaz sızıntısı	T.194
Şef sekreter yapısının bozulması	T.195
Yetkisiz yazılım kurma veya yazılımda değişiklik	T.196
Telefon trafiğinden dolayı görüşmelerin yapılamaması	T.197

4. PROSES SAHİBİ

- Daire Başkanı
- BGYS Yönetim Temsilcisi
- BGYS Ekibi
- Tüm Çalışanlar

5. İLGİLİ DOKÜMANLAR

- Varlık Envanteri
- Risk Değerlendirme Tablosu — BGYS Yazılımı
- Tedarikçi Değerlendirme Formu — BGYS.FRM.04.02
- Artık Risk Onay Formu — BGYS.FRM.08.01