

GÜVENLİK RİSK ANALİZİ

No	Proses/Yapılan İşlem Adı	Tehlike Sınıfı	Riskin Tanımı	Riskin Potansiyel Etkileri	Riskin Potansiyel Sebepleri	Mevcut Düzeltici ve Önleyici İşlem Kontrolleri	Olma İhtimali	Etki Şiddeti	Risk	Risk Derecesi	Tehditler	Fırsatlar	Risk Kaynakları			Yapılan Faaliyet	Sorumlular	Sonuç	Olma İhtimali	Etki Şiddeti	Risk Büyüklüğü	Risk Derecesi
1	Ürün Girdi Kalite Kontrol	SABOTAJ	Çalışanın ve/veya işletme içerisindeki yabancı kişilerin üretime gidecek işliğe bilerek insan sağlığına zararlı bir kimyasal karıştırması	Halinin son kullanıncı üzerinde olumsuz etkilerine müdahale edilememesi ve müşteri beklentilerini karşılayamama	İşletme içerisinde güvenlik açığı	İşletme içerisine girecek kişilerin veya çalışanların yetkisiz değişim yapamayacağı şekilde güvenlik açıklarını kapatmak, işletme içerisinde kamera izleme sistemi	2	5	10	Yüksek Risk	*Müşteri ihtiyaç ve beklentilerini karşılayamama, *Finansal Kayıp *Zaman Kaybı	İşletme güvenlik açıklarının giderilmesi	*Güvenlik *Üretim			İşletme içerisine açılan tüm kapılarda kartlı geçiş sistemi ve ziyaretçilere refakatsiz dolaşımın yasaklanması, aynı zamanda işletme bilgisayarlarında otomatik kilit sistemi	Bilgi İşlem Direktörü İdari İşler Amiri Kalite Kontrol Yöneticisi	Alınan aksiyon sonrası ilgili sabotaj riski minimize edilmiştir.	1	4	4	ÇOK DÜŞÜK RİSK
2	Ürün Girdi Kalite Kontrol	SABOTAJ	Çalışanın ve/veya işletme içerisindeki yabancı kişilerin kalite kontrol onayından geçmeyen bir ham maddeyi bilerek üretime dahil etmesi	Hatalı ve yanlış dokuma Müşteri termininde gecikme	İşletme içerisinde güvenlik açığı, yetkisiz erişim riski	İşletme içerisine girecek kişilerin veya çalışanların yetkisiz değişim yapamayacağı şekilde güvenlik açıklarını kapatmak, işletme içerisinde kamera izleme sistemi	2	4	8	Orta Risk	*Müşteri ihtiyaç ve beklentilerini karşılayamama, *Finansal Kayıp *Zaman Kaybı	İşletme güvenlik açıklarının giderilmesi	*Güvenlik *Üretim		*Kalite Kontrol	İşletme içerisine açılan tüm kapılarda kartlı geçiş sistemi ve ziyaretçilere refakatsiz dolaşımın yasaklanması, aynı zamanda işletme bilgisayarlarında otomatik kilit sistemi	Bilgi İşlem Direktörü İdari İşler Amiri Kalite Kontrol Yöneticisi	Alınan aksiyon sonrası ilgili sabotaj riski minimize edilmiştir.	2	3	6	DÜŞÜK RİSK
3	Kaynak Planlama	SABOTAJ	Çalışanın veya yabancı bir kimsenin çağ planını bilerek değiştirmesi ve olması gerekenden farklı bir ipin tezgaha gitmesi	Hatalı ve yanlış dokuma, termin gecikmesi	Birimlerin bilgisayarlarına yetkisiz erişim konusunda güvenlik açığı	Bilgisayar erişimlerini önleyici güçlü şifreleme ve otomatik ekran kilidi yönetimlerinin kullanılması	2	4	8	Orta Risk	*Müşteri ihtiyaç ve beklentilerini karşılayamama, *Finansal Kayıp *Zaman Kaybı	*İşletme donanım sistemlerinde güvenlik açıklarının kapatılması	*Güvenlik açığı *Planlama		*Bilgi İşlem	Bilgisayar donanım sisteminde güvenlik açıkları giderildi, koruyucu faaliyetler arttı	Ham Madde Depo Sorumlusu Kaynak Planlama Sorumlusu	Alınan aksiyon sonrası ilgili sabotaj riski minimize edilmiştir.	1	4	4	ÇOK DÜŞÜK RİSK
4	Planlama	SABOTAJ	Planlama departmanının bilgisayarlarına yetkisiz erişen kişi veya kişilerin planlama takvimine müdahale etmesi, tezgah programlamalarını değiştirmesi	Hatalı ve yanlış dokuma, termin gecikmesi	Birimlerin bilgisayarlarına yetkisiz erişim konusunda güvenlik açığı	Bilgisayar erişimlerini önleyici güçlü şifreleme ve otomatik ekran kilidi yönetimlerinin kullanılması	2	4	8	Orta Risk	*Müşteri ihtiyaç ve beklentilerini karşılayamama, *Finansal Kayıp *Zaman Kaybı	*İşletme donanım sistemlerinde güvenlik açıklarının kapatılması	*Güvenlik açığı *Planlama		*Bilgi İşlem	Bilgisayar sistemlerinde güvenlik açıkları giderildi, koruyucu ve önleyici sistemler arttı	Bilgi İşlem Direktörü Planlama Müdürü	Alınan aksiyon sonucu ilgili risk minimize edilmiştir	2	3	6	DÜŞÜK RİSK
5	Dokuma	SABOTAJ	Dokuma tezgahından sorumlu personelin planlanan dokuma dışında bilerek kaliteye zarar verecek şekilde dokuma programını değiştirmesi	Hatalı ve yanlış dokuma Termin gecikmesi	İşletme içerisindeki donanım sistemlerinde güvenlik açığı, işletme içerisinde yetkisiz erişim	Sistem erişimlerini engelleyici güçlü şifreleme ve koruma sistemleri, işletme içerisine yetkisiz erişimi kısıtlayıcı şifre ve kartlı kapılar	2	4	8	Düşük Risk	*Üretim ve işletme içerisindeki güvenliğin sağlanamaması *Müşteri beklentilerini karşılayamama *Finansal kayıp *Zaman kaybı	Güvenlik açıklarının tespit edilip giderilmesi	*Bilgi Güvenliği Açıkları		Üretim	İşletme içerisine açılan tüm kapılarda kartlı geçiş sistemi ve ziyaretçilere refakatsiz dolaşımın yasaklanması, aynı zamanda işletme bilgisayarlarında otomatik kilit sistemi	Bilgi İşlem Sorumlusu Dokuma Sorumlusu	Güvenlik açıkları giderildi, önleyici faaliyetler takip ve kontrol ediliyor.	1	4	4	ÇOK DÜŞÜK RİSK
6	Dokuma	SABOTAJ	İşletme içerisine yetkisiz erişen bir yabancının dokuma tezgahlarındaki verilere müdahale etmesi, çalışan tezgahları durdurması	Hatalı ve yanlış dokuma Termin gecikmesi	İşletme içerisindeki donanım sistemlerinde güvenlik açığı, işletme içerisinde yetkisiz erişim	Sistem erişimlerini engelleyici güçlü şifreleme ve koruma sistemleri, işletme içerisine yetkisiz erişimi kısıtlayıcı şifre ve kartlı kapılar	1	4	4	Çok Düşük Risk	*Üretim ve işletme içerisindeki güvenliğin sağlanamaması *Müşteri beklentilerini karşılayamama *Finansal kayıp *Zaman kaybı	Güvenlik açıklarının tespit edilip giderilmesi	*Bilgi Güvenliği Açıkları		Üretim	İşletme içerisine açılan tüm kapılarda kartlı geçiş sistemi ve ziyaretçilere refakatsiz dolaşımın yasaklanması, aynı zamanda işletme bilgisayarlarında otomatik kilit sistemi	Bilgi İşlem Sorumlusu Dokuma Birim Amiri	Güvenlik açıkları giderildi, önleyici faaliyetler takip ve kontrol ediliyor.	1	4	4	ÇOK DÜŞÜK RİSK
7	Konfeksiyon Etiket Barkod	SABOTAJ	İşletme içerisine yetkisiz erişim sağlayan bir yabancının veya bir çalışanın müşteriye ait etiket bilgilerini ifşa etmesi veya rakip kurumlarla paylaşması	Müşteri gizliliğinin ihlal edilmesi, cezal yaptırımlar ve itibar kaybı	Birimlerin bilgisayarlarına yetkisiz erişim konusunda güvenlik açığı, işletme içerisine yetkisiz erişim	İşletme kapılarının denetimi şeklinde şifre veya kartla açılır olması	4	4	16	Katılanamaz Risk	*Müşteri ihtiyaç ve beklentilerini karşılayamama, *Finansal Kayıp	*Artan müşteri memnuniyeti *İşletmedeki güvenlik açıklarının kapatılması	*Bilgi Güvenliği Açıkları		Üretim (İçsel) Operasyonel (İçsel) Müşteriler (dışsal)	İşletme içerisindeki güvenlik açıkları giderilmiş yetkisiz erişim engellenmiştir.	İşletme Müdürü Konfeksiyon Etiket Sorumlusu	Bilgi güvenliğine ait risk azaltılmıştır	2	4	8	ORTA RİSK
8	Konfeksiyon Paketleme	SABOTAJ	Markanın talep etmediği bir ambalajlamanın çalışan tarafından kasti şekilde ürüne uygulanması	Müşteri taleplerini karşılayamama ve olası para cezası uygulamaları	Çalışanın kötü niyetli yaklaşımı	Çalışanların ilgili konuya yönelik bilgilendirilmesi ve kötü niyetle sabotajda bulunan çalışan hakkında disiplin cezası uygulanması	2	4	8	Orta Risk	*Müşteri beklentilerini karşılayamama *İtibar kaybı *Finansal kayıp	*Artan müşteri memnuniyeti *Olası müşteri yaptırımların önüne geçilmesi	*Personel		*Üretim *İnsan Kaynakları	İlgili personele ilişkin disiplin cezası ve idari yaptırımlar uygulanması	Konfeksiyon Birim Amiri İşletme Müdürü İnsan Kaynakları Direktörü	İşletme içerisindeki sabotaj riski disiplin uygulamaları ile caydırıcı hale gelmiştir	1	4	4	ÇOK DÜŞÜK RİSK

No	Proses/Yapılan İşlem Adı	Tehlike Sınıfı	Riskin Tanımı	Riskin Potansiyel Etkileri	Riskin Potansiyel Sebepleri	Mevcut Düzeltici ve Önleyici İşlem Kontrolleri	Olma İhtimali	Etki Şiddeti	Risk	Risk Derecesi	Tehditler	Fırsatlar	Risk Kaynakları			Yapılan Faaliyet	Sorumlular	Sonuç	Olma İhtimali	Etki Şiddeti	Risk Büyüklüğü	Risk Derecesi
9	Konfeksiyon Paketleme	SABOTAJ	Shrink makinasının ısı ayarının bilekerek değiştirilmesi ve ambalajlamada hataya sebebiyet verme	Müşteri taleplerini karşılayamama ve olası para cezası uygulamaları	Çalışanın kötü niyetli yaklaşımı	Çalışanların ilgili konuya yönelik bilgilendirilmesi ve kötü niyetle sabotajda bulunan çalışan hakkında disiplin cezası uygulaması	2	5	10	Yüksek Risk	*Müşteri beklentilerini karşılayamama *İtibar kaybı *Finansal kayıp	*Artan müşteri memnuniyeti *Olası müşteri yaptırımlarının önüne geçilmesi	*Personel		*Üretim *İnsan Kaynakları	İlgili personele ilişkin disiplin cezası ve idari yaptırımlar uygulanması	Konfeksiyon Birim Amiri İşletme Müdürü İnsan Kaynakları Direktörü	İşletme içerisindeki sabotaj riski disiplin uygulamaları ile caydırıcı hale gelmiştir	1	5	5	DÜŞÜK RİSK
10	Konfeksiyon Paketleme	SABOTAJ	İşletme içerisine yetkisiz erişen bir çalışanın veya bir çalışanın paketlenme aşamasındaki bir ürünün içerisine yasadışı bir madde koyması (uyuşturucu, silah vb.)	Gümrük Kanunu'na istinaden sorumlu kişilere ceza ve yasal yaptırımlar	İşletme içerisindeki güvenlik açıkları	Tespit edilen maddenin kolluk kuvvetlerine bildirilmesi, işletme içerisindeki güvenlik açıklarının hızla giderilmesi	3	5	15	Katlanılamaz Risk	*İtibar kaybı *Finansal kayıp *Müşteri kaybı	*İşletmedeki güvenlik açıklarının tespit edilip giderilmesi	*Güvenlik açıkları *Personel *Güvenlik Birimi		*Üretim *İnsan Kaynakları *İşletme	İşletme içerisinde oluşturulan kısıtlı alanlar ve kart sistemleriyle güvenlik açıkları giderilmiş, kamera izleme sistemleri artırılmıştır	İşletme Müdürü İnsan Kaynakları Direktörü Bilgi İşlem Direktörü	İşletme içerisindeki ilgili sabotaj riski güvenlik önlemleriyle azaltılmıştır	1	5	5	DÜŞÜK RİSK
11	Sevkiyat	SABOTAJ	Sevkiyat alanına görevli personel haricinde izinsiz giriş olması ve yüklenecek araç ve ürünlere müdahale edilmesi	Ürün güvenliği tehdidi Eksik-hatalı sevkiyat Gümrük güvenliğini tehdit edici faaliyetler	Güvenlik açığı Erişimi kısıtlı alanların duyurulmaması	Erişimi kısıtlı alanların tüm çalışan ve ziyaretçilere duyurulması	2	5	10	Yüksek Risk	* Finansal kayıp *Rakiplerde imaj sarsılmasının oluşması (kaza v.b. Olaylarda) * Ceza ve Kayıplar	*Tesis ve ürün güvenliğinde artış	*Erişim *Güvenlik		Operasyonel (İçsel) Yasal Otorite (Dışsal)	Erişimi kısıtlı alanların tüm çalışan ve ziyaretçilere duyurulması	Sevkiyat Sorumlusu Güvenlik Amiri	Düzenli takibi yapılmaktadır.	2	3	6	ORTA RİSK
12	Sevkiyat	FİZİKSEL	Sevk esnasında yükleme yapılan aracın kontrol edilmemesi	Ürün güvenliği ve kalitesinde bozulma Gümrük güvenliğini tehdit edici faaliyetler	Personel bilinçsizliği	Personelin konuyla ilgili bilgilendirilmesi	2	5	10	Yüksek Risk	* Finansal kayıp *Rakiplerde imaj sarsılmasının oluşması (kaza v.b. Olaylarda) * Ceza ve Kayıplar	*Tesis ve ürün güvenliğinde artış	*Erişim *Kalifiye Eleman		Operasyonel (İçsel) Yasal Otorite (Dışsal)	Personelin konuyla ilgili bilgilendirilmesi	Sevkiyat Sorumlusu Güvenlik Amiri	Düzenli takibi yapılmaktadır.	2	3	6	ORTA RİSK
13	Sevkiyat	FİZİKSEL	Sevk alanındaki personelin yetkili giriş kartını kaybetmesi	Ürün güvenliği tehdidi Eksik-hatalı sevkiyat Gümrük güvenliğini tehdit edici faaliyetler	Personel dikkatsizliği Güvenlik zaaflılığı	Personelin konuyla ilgili bilgilendirilmesi	3	4	12	Yüksek Risk	* Finansal kayıp *Rakiplerde imaj sarsılmasının oluşması (kaza v.b. Olaylarda) * Ceza ve Kayıplar	*Tesis ve ürün güvenliğinde artış	*Erişim *Kalifiye Eleman		Operasyonel (İçsel) Yasal Otorite (Dışsal)	Personelin konuyla ilgili bilgilendirilmesi	Sevkiyat Sorumlusu Güvenlik Amiri	Düzenli takibi yapılmaktadır.	2	3	6	ORTA RİSK
14	Sevkiyat	SABOTAJ	Sevk edilecek ürünün içerisine görevli personel tarafından veya yetkisiz erişim sağlayan bir yabancı tarafından yasadışı ürünlerin karıştırılması (uyuşturucu, silah vb)	Gümrük Kanunu'na istinaden sorumlu kişilere ceza ve yasal yaptırımlar	İşletme içerisindeki güvenlik açıkları	Tespit edilen maddenin kolluk kuvvetlerine bildirilmesi, işletme içerisindeki güvenlik açıklarının hızla giderilmesi	3	5	15	Katlanılamaz Risk	*İtibar kaybı *Finansal kayıp *Müşteri kaybı	*İşletmedeki güvenlik açıklarının tespit edilip giderilmesi	*Güvenlik açıkları *Personel *Güvenlik Birimi		*Üretim *İnsan Kaynakları *İşletme	İşletme içerisinde oluşturulan kısıtlı alanlar ve kart sistemleriyle güvenlik açıkları giderilmiş, sevk personellerinde periyodik adli sicil kontrolü yapılmakta	İşletme Müdürü İnsan Kaynakları Direktörü Bilgi İşlem Direktörü	İşletme içerisindeki ilgili sabotaj riski güvenlik önlemleriyle azaltılmıştır	1	5	5	DÜŞÜK RİSK
15	Sevkiyat	FİZİKSEL	Mühürlerin ISO 17712 standardına uygun olmaması	Mühür güvenliğini sağlanamaması, sevkiyat güvenliğinde zaaflılık	Temin edilen tedarikçiden doğru bilgi alamama	Mevcut tedarikçiden standart temin edilmeye çalışılır, yanıt alınmazsa tedarikçiyle ilişki kesilir	2	4	8	Orta Risk	*Müşteri beklentilerini karşılayamama *İtibar kaybı *Finansal kayıp	*Tedarik zinciri güvenliğinin korunması	*Tedarikçi		*Satın Alma	İlgili tedarikçiyle ilişikisinin kesilmesi	Genel Müdür Mali Kıymeter Direktörü	Riskin bertaraf edilmesi	1	4	4	ÇOK DÜŞÜK RİSK
16	Sevkiyat	FİZİKSEL	Mühür envanter kaydının tutulmaması	Sevkiyat güvenliğinde zaaflılık, ürün tesliminde takip sisteminin olmaması	Personel bilgi eksikliği ve dikkatsizlik	Kullanılan tüm mühürler envanter kaydı tutularda 2-3 ayrı noktadan teyit edilebilecek şekilde kayıt altına alınır	3	4	12	Yüksek Risk	*Müşteri beklentilerini karşılayamama *Güvenlik Zaaflılığı *Finansal kayıp	*Tedarik zinciri güvenliğinin korunması	*Personel *Bilgi Eksikliği		*İşletme *Müşteri	Tüm mühürler satın alım aşamasında ve sonrasında kullanım aşamasında kayıt altına alınır	Sevkiyat Sorumlusu İşletme Müdürü	İlgili risk azaltılmıştır	2	4	8	ORTA RİSK
17	Sevkiyat	FİZİKSEL	Mühürsüz Konteyner/Tır Çıkışı	Sevkiyat ve gümrük güvenliğinde zaaflılık	Personel bilgi eksikliği, dikkatsizlik, ihmâl veya sabotaj	İşletme içerisinde yüklemesi yapılan tüm araçların mühürlenmesine dair güvenlik kontrolü yapılır ve fotoğraflı kanıtlar kambyoya iletilir	3	5	15	Katlanılamaz Risk	* Finansal kayıp *Rakiplerde imaj sarsılmasının oluşması (kaza v.b. Olaylarda) * Ceza ve Kayıplar	*Güvenlik açıklarının giderilmesi	*Personel *Bilgi ve İletişim Eksikliği		*İşletme *Müşteri	İşletme içerisinde yüklemesi yapılan tüm araçların mühürlenmesine dair güvenlik kontrolü yapılır ve fotoğraflı kanıtlar kambyoya iletilir	Sevkiyat Sorumlusu İşletme Müdürü	İlgili risk azaltılmıştır	2	4	8	ORTA RİSK

No	Proses/Yapılan İşlem Adı	Tehlike Sınıfı	Riskin Tanımı	Riskin Potansiyel Etkileri	Riskin Potansiyel Sebepleri	Mevcut Düzeltici ve Önleyici İşlem Kontrolleri	Olma İhtimali	Etki Şiddeti	Risk	Risk Derecesi	Tehditler	Fırsatlar	Risk Kaynakları			Yapılan Faaliyet	Sorumlular	Sonuç	Olma İhtimali	Etki Şiddeti	Risk Büyüklüğü	Risk Derecesi
18	Satın Alma	SABOTAJ	Yetkisiz erişim sağlayan bir yabancının veya bir çalışanın ham madde temin sürecine bilerek kötü niyetle müdahale etmesi	Ham madde tedarikinde hata ve eksikler, üretimde ve termin sürelerinde aksama	Birimlerin bilgisayarlarına yetkisiz erişim konusunda güvenlik açığı, işletme içerisine yetkisiz erişim	Bilgisayar erişimlerinin kısıtlanması ve şifrelerin periyodik değişimi, İşletme kapılarının denetimli şekilde şifre veya kartla açılır olması	3	4	12	Yüksek Risk	*Müşteri ihtiyaç ve beklentilerini karşılayamama, *Finansal Kayıp	*Artan müşteri memnuniyeti *İşletmedeki güvenlik açıklarının kapatılması	*Bilgi Güvenliği açıkları		Üretim (İçsel) Operasyonel (İçsel) Müşteriler (Dışsal)	İşletme içerisindeki güvenlik açıkları giderilmiş yetkisiz erişim engellenmiştir.	İşletme Müdürü Konfeksiyon Etiket Sorumlusu	Bilgi güvenliğine ait risk azaltılmıştır	2	4	8	ORTA RISK
19	İnsan Kaynakları	FİZİKSEL	Sabikalı kişilerin işe alınması	İşletme içerisinde güvenlik zaafliyeti	Personel dikkatsizliği veya ihmal	İşe alımlardan önce referans kontrolleri yapılarak kayıt altına alınmalı. Kritik bölgede çalışanlar için 6 ayda bir adli sicil kaydı taraması yapılmalı.	2	5	10	Yüksek Risk	*İtibar Kaybı *Yasal yaptırımlar	Güvenlik açıklarının tespit edilip giderilmesi	*Personel		İnsan Kaynakları	Kritik bölgelerde işe alım yapılırken referans kontrol formudol	İnsan Kaynakları Uzmanı İşletme Müdürü	Düzenli takibi yapılmaktadır.	1	5	5	DÜŞÜK RISK
20	İnsan Kaynakları	SABOTAJ	Yetkisiz erişim sağlayan bir kişi tarafından personel özük bilgilerine erişilmesi ve ifşa edilmesi	KVKK kapsamında korunan çalışan bilgilerinin kötü niyetli kişilere ulaşması, yasal yaptırımlar	Birimlerin bilgisayarlarına yetkisiz erişim konusunda güvenlik açığı, işletme içerisine yetkisiz erişim	Bilgisayar erişimlerinin kısıtlanması ve şifrelerin periyodik değişimi, İşletme kapılarının denetimli şekilde şifre veya kartla açılır olması	3	4	12	Yüksek Risk	*İtibar Kaybı *Yasal yaptırımlar	*Bilgi güvenliği açıklarının tespiti *İşletmedeki güvenlik açıklarının kapatılması	*Bilgi Güvenliği açıkları		*İnsan Kaynakları (İçsel)	İşletme içerisindeki güvenlik açıkları giderilmiş yetkisiz erişim engellenmiştir.	İnsan Kaynakları TKY Çalışan Temsilcileri Üst Yönetim	Bilgi güvenliğine ait risk azaltılmıştır	2	4	8	ORTA RISK
21	İnsan Kaynakları	SABOTAJ	Bir çalışanın kötü niyetle ve bilerek personel özük bilgilerini ifşa etmesi veya 3. kişilerle paylaşması	KVKK kapsamında korunan çalışan bilgilerinin kötü niyetli kişilere ulaşması, yasal yaptırımlar	Birimlerin bilgisayarlarına yetkisiz erişim konusunda güvenlik açığı, işletme içerisine yetkisiz erişim	Bilgisayar erişimlerinin kısıtlanması ve şifrelerin periyodik değişimi, İşletme kapılarının denetimli şekilde şifre veya kartla açılır olması	3	4	12	Yüksek Risk	*İtibar Kaybı *Yasal yaptırımlar	*Bilgi güvenliği açıklarının tespiti *İşletmedeki güvenlik açıklarının kapatılması	*Bilgi Güvenliği açıkları *Personel		*İnsan Kaynakları (İçsel)	İşletme içerisindeki güvenlik açıkları giderilmiş yetkisiz erişim engellenmiştir.	İnsan Kaynakları TKY Çalışan Temsilcileri Üst Yönetim	Bilgi güvenliğine ait risk azaltılmıştır	2	4	8	ORTA RISK
22	İnsan Kaynakları	FİZİKSEL	Olası güvenlik zaafliyeti ve ihlallerin bildirilmemesi	Olası güvenlik risklerinin tespit edilememesi veya müdahalede gecikme	Personel bilçsizliği	Personellerin bilinçlendirilmesi	3	4	12	Yüksek Risk	*Müşteri beklentilerini karşılayamama *Güvenlik Zaafliyeti *Finansal kayıp	*Bilgi güvenliği açıklarının tespiti *İşletmedeki güvenlik açıklarının kapatılması	*Bilgi Güvenliği açıkları *Personel Bilgi Eksikliği		*İnsan Kaynakları (İçsel)	Personele konuyla ilgili bilgi verilmiş ve ihlallerin bildirimiyle ilgili duyuru yapılmıştır	İnsan Kaynakları TKY Çalışan Temsilcileri Üst Yönetim	İlgili risk azaltılmıştır	2	4	8	ORTA RISK
23	İnsan Kaynakları İdari İşler	FİZİKSEL	Fabrika içerisinde taşeron ve misafirlerin refakatçi olmadan dolaşması	Yetkisiz erişim riski, İşletme güvenliğini tehdit edici faaliyetler	Güvenlik açığı Personel dikkatsizliği veya ihmal	Gelen kişilerin bilgileri kayıt defterine işlenerek giriş-çıkışları takip altına alınacak. Misafirler için yaka kartları temin edilecek ve kullanılması sağlanacak İçerde yaka kartsız yabancı kişilerin tespit edilmesi durumunda güvenliğe bilgi verilecek	2	5	10	Yüksek Risk	*İşletme güvenliğinde zaafliyet	*İşletmedeki güvenlik açıklarının kapatılması	*Personel *Bilgi Eksikliği		İnsan Kaynakları (İçsel) Ziyaretçiler (Dışsal)	Güvenlik görevlileri bilgilendirilmiş ve refakatçi olmadan işletme girişleri engellenmiştir	İnsan Kaynakları Direktörü İdari İşler Amiri	İlgili risk azaltılmıştır	1	5	5	DÜŞÜK RISK
24	İnsan Kaynakları İdari İşler	SABOTAJ	Yetkisiz erişim sağlayan bir kişi tarafından yemekhanedeki yemeklere insan sağlığına zararlı maddelerin (zehirli ve ağır kimyasallar) eklenmesi	Personellerde ciddi sağlık problemleri, yasal soruşturma süreçleri	İşletme içerisinde yetkisiz erişim ve güvenlik açıkları	İlgili sabotajla ilgili kamera kayıtlarının incelenmesi ve güvenlik açıklarının giderilmesi	3	5	15	Katlanılmaz Risk	*Sağlık Sorunları *İtibar kaybı *Yasal yaptırımlar	*İşletmedeki güvenlik açıklarının tespit edilip giderilmesi	*Güvenlik açıkları *Personel *Güvenlik Birimi		*İnsan Kaynakları (İçsel)	İşletme içerisindeki güvenlik açıkları giderilmiş yetkisiz erişim engellenmiştir.	İnsan Kaynakları TKY Çalışan Temsilcileri Üst Yönetim	İlgili risk azaltılmıştır	2	5	10	YÜKSEK RISK

No	Proses/Yapılan İşlem Adı	Tehlike Sınıfı	Riskin Tanımı	Riskin Potansiyel Etkileri	Riskin Potansiyel Sebepleri	Mevcut Düzeltici ve Önleyici İşlem Kontrolleri	Olma İhtimali	Etki Şiddeti	Risk	Risk Derecesi	Tehditler	Fırsatlar	Risk Kaynakları			Yapılan Faaliyet	Sorumlular	Sonuç	Olma İhtimali	Etki Şiddeti	Risk Büyüklüğü	Risk Derecesi
25	İnsan Kaynakları İdari İşler	SABOTAJ	Yetkisiz erişim sağlayan bir kişi veya personelin işme suyuna insan sağlığına zararlı maddeleri eklemesi (zehirlili ve ağır kimyasallar)	Personellerde ciddi sağlık problemleri, yasal soruşturma süreçleri	İşletme içerisinde yetkisiz erişim ve güvenlik açıkları	İlgili sabotajla ilgili kamera kayıtlarının incelenmesi ve güvenlik açıklarının giderilmesi	3	5	15	Katlanılamaz Risk	*Sağlık Sorunları *İtibar kaybı *Yasal yaptırımlar	*İşletmedeki güvenlik açıklarının tespit edilip giderilmesi	*Güvenlik açıkları *Personel *Güvenlik Birimi		*İnsan Kaynakları (içsel)	İşletme içerisindeki güvenlik açıkları giderilmiş yetkisiz erişim engellenmiştir.	İnsan Kaynakları TKY Çalışan Temsilcileri Üst Yönetim	İlgili risk azaltılmıştır	2	5	10	YÜKSEK RİSK
26	Bilgi İşlem	FİZİKSEL	Server odasının yeterli derecede soğutulmaması veya soğutucu cihazların arızalanması	Server odasında yangın riski, tüm tesis bilgilerinin kaybedilmesi	Sorumlu personel dikkatsizliği veya ihmal	Server odasındaki yangın sisteminin doğru çalıştığından emin olmak, odaya derece uyarı sistemi kurmak	3	5	15	Katlanılamaz Risk	*Bilgi arşivi kaybı *Finansal kayıp *Üretim kaybı	*Bilgi güvenliğini korumaya yönelik faaliyetlerin artması	*Personel Bilinçsizliği *Teknik yetersizlik		*Bilgi İşlem	Server odasındaki FM200 yangın sistemi için periyodik kontrol ve derece uyarı sistemi	Bilgi İşlem Direktörü ISG Uzmanı	İlgili risk azaltılmıştır	1	5	5	DÜŞÜK RİSK
27	Bilgi İşlem	FİZİKSEL	Güvenlik yazılımları ve uyarı sistemlerin devre dışı kalması	Bilgi güvenliği tehdidi, bilgisayar sistemlerinde çökme riski	Personel dikkatsizliği	Tespit edilen durumun giderilmesi ve bu süreçte güvenlik tehdidiyle ilgili bir problem yaşanmış mı kontrol edilmesi	3	4	12	Yüksek Risk	*Bilgi güvenliği açığı *Sistem güvenliği	*Bilgi güvenliğini korumaya yönelik faaliyetlerin artması	*Personel Bilinçsizliği *Teknik yetersizlik		*Bilgi İşlem	İlgili durum giderilmiş ve kontrol edilmesi sağlanmıştır	Bilgi İşlem Direktörü	İlgili risk azaltılmıştır	2	4	8	ORTA RİSK
28	Bilgi İşlem	SABOTAJ	Tesis güvenlik duvarının saldırıya uğraması, sistemsel saldırı	Bilgi güvenliği tehdidi, bilgisayar sistemlerinde çökme riski	Personel dikkatsizliği	Tespit edilen durumun giderilmesi ve bu süreçte güvenlik tehdidiyle ilgili bir problem yaşanmış mı kontrol edilmesi	3	4	12	Yüksek Risk	*Bilgi güvenliği açığı *Sistem güvenliği	*Bilgi güvenliğini korumaya yönelik faaliyetlerin artması	*Personel Bilinçsizliği *Teknik yetersizlik		*Bilgi İşlem	İlgili durum giderilmiş ve kontrol edilmesi sağlanmıştır	Bilgi İşlem Direktörü	İlgili risk azaltılmıştır	2	4	8	ORTA RİSK
29	Bilgi İşlem	SABOTAJ	Yetkisiz erişim sağlayan bir personel veya bir yabancının bilgi işlem odasına girmesi ve sistem kontrolü olan bilgisayarlara erişmesi	Tesis bilgi güvenliğinin ihlal edilmesi, bilgilerin ifşalanması tehdidi	Birimlerin bilgisayarlarına yetkisiz erişim konusunda güvenlik açığı, işletme içerisine yetkisiz erişim	İşletme kapılarının denetimli şekilde şifre veya kartla açılır olması, bilgisayarlarda otomatik ekran kilidi ve periyodik şifre değişimleri	4	4	16	Katlanılamaz Risk	*Bilgi güvenliği açıkları *İtibar kaybı *Finansal kayıp	*İşletmedeki güvenlik açıklarının kapatılması	*Bilgi Güvenliği açıkları *Tesis güvenliği		*Bilgi İşlem *İşletme	İşletme içerisindeki güvenlik açıkları giderilmiş yetkisiz erişim engellenmiştir.	Bilgi İşlem Direktörü İşletme Müdürü	Bilgi güvenliğine ait risk azaltılmıştır	2	4	8	ORTA RİSK
30	Bilgi İşlem	SABOTAJ	Yetkisiz erişim sağlayan personel veya yabancının server odasına erişmesi ve müdahalede bulunması	Tesis bilgi güvenliğinin ihlal edilmesi, bilgilerin ifşalanması tehdidi	Birimlerin bilgisayarlarına yetkisiz erişim konusunda güvenlik açığı, işletme içerisine yetkisiz erişim	İşletme kapılarının denetimli şekilde şifre veya kartla açılır olması, kasa şifresini sadece sorumlu personelin bilmesi	4	4	16	Katlanılamaz Risk	*Bilgi güvenliği açıkları *İtibar kaybı *Finansal kayıp	*İşletmedeki güvenlik açıklarının kapatılması	*Bilgi Güvenliği açıkları *Tesis güvenliği		*Bilgi İşlem *İşletme	İşletme içerisindeki güvenlik açıkları giderilmiş yetkisiz erişim engellenmiştir.	Bilgi İşlem Direktörü İşletme Müdürü	Bilgi güvenliğine ait risk azaltılmıştır	2	4	8	ORTA RİSK
31	Finans	SABOTAJ	Finans departmanının bulunduğu alan ve şirket kasasına yetkisiz erişim	Hırsızlık ya da bilgi güvenliği tehdidi	İşletme ve bilgi güvenliğinde yetkisiz erişim konusunda güvenlik açığı	İşletme kapılarının denetimli şekilde şifre veya kartla açılır olması, kasa şifresini sadece sorumlu personelin bilmesi	3	4	12	Yüksek Risk	*Bilgi güvenliği açıkları *İtibar kaybı *Finansal kayıp	*İşletmedeki güvenlik açıklarının kapatılması	*Bilgi Güvenliği açıkları *Tesis güvenliği		*Finans *Bilgi İşlem	İşletme içerisindeki güvenlik açıkları giderilmiş yetkisiz erişim engellenmiştir.	Mali Kıymetler Direktörü Bilgi İşlem Direktörü	İlgili risk azaltılmıştır	2	3	6	ORTA RİSK

No	Proses/Yapılan İşlem Adı	Tehlike Sınıfı	Riskin Tanımı	Riskin Potansiyel Etkileri	Riskin Potansiyel Sebepleri	Mevcut Düzeltici ve Önleyici İşlem Kontrolleri	Olma İhtimali	Etki Şiddeti	Risk	Risk Derecesi	Tehditler	Fırsatlar	Risk Kaynakları			Yapılan Faaliyet	Sorumlular	Sonuç	Olma İhtimali	Etki Şiddeti	Risk Büyüklüğü	Risk Derecesi
32	Finans	SABOTAJ	Finans yetkilisine ait bilgisayar ve mobil cihazlar yetkisiz erişim ve hassas bilgilerin ifşası (ödemeler, banka şifreleri, para hareketleri vb)	Hırsızlık ya da bilgi güvenliği tehdidi	İşletme ve bilgi güvenliğinde yetkisiz erişim konusunda güvenlik açığı	İşletme kapılarının denetimli şekilde şifre veya kartla açılır olması, kasa şifresini sadece sorumlu personelin bilmesi	3	5	15	Katlanamaz Risk	*Bilgi güvenliği açıkları *İtibar kaybı *Finansal kayıp	*İşletmedeki güvenlik açıklarının kapatılması	*Bilgi Güvenliği açıkları *Tesis güvenliği		*Finans *Bilgi İşlem	İşletme içerisindeki güvenlik açıkları giderilmiş yetkisiz erişim engellenmiştir.	Mali Kıymetler Direktörü Bilgi İşlem Direktörü	İlgili risk azaltılmıştır	2	4	8	ORTA RISK