

MAKÜ

BURDUR MEHMET AKİF ERSOY ÜNİVERSİTESİ

TEDARİKÇİ İLİŞKİLERİNDE BİLGİ GÜVENLİĞİ POLİTİKASI

	TEDARİKÇİ İLİŞKİLERİNDE BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	PL.11
		Yayın Tarihi	01.04.2022
		Revizyon No	00
		Revizyon Tarihi	-
		Sayfa No	: Sayfa 2 / 8

İçindekiler

1. Amaç	3
2. Kapsam.....	3
3. Sorumluluk.....	3
4. Kısaltmalar ve Tanımlar.....	3
5. Tedarikçi İlişkileri Bilgi Güvenliği Politikası.....	4
5.1. Tedarikçi İlişkilerinde Bilgi Güvenliği Gereksinimleri	4
5.2. Tedarikçi Hizmet Sağlama Yönetimi.....	5
5.2.1. Tedarikçi İlişkilerini İzleme ve Gözden Geçirme.....	5
5.2.2. Tedarikçi Hizmetlerindeki Değişiklikleri Yönetme	6
5.3. Tedarik Hizmetlerinin Değerlendirilmesi	6
6. İlgili Dokümanlar	7
6.1. İç Kaynaklı Dokümanlar	7
6.2. Dış Kaynaklı Dokümanlar.....	7

HAZIRLAYAN	ONAYLAYAN
BGYS Yöneticisi	Üst Yönetim Temsilcisi/Üst Yönetim
KURUMA ÖZEL	

	TEDARİKÇİ İLİŞKİLERİNDE BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	PL.11
		Yayın Tarihi	01.04.2022
		Revizyon No	00
		Revizyon Tarihi	-
		Sayfa No	: Sayfa 3 / 8

1. Amaç

Bu doküman, “BGYS Kapsam Analizi Dokümanı”nda belirtilen kuruluşumuza hizmet sağlayan tedarikçiler tarafından erişilen varlıkların korunmasını sağlamak, tedarikçilerin Kurum’un varlıklarına erişimi ile ilgili riskleri azaltmak ve bilgi güvenliği gereksinimlerini karşılamak amacıyla hazırlanmıştır.

2. Kapsam

Bu doküman, “BGYS Kapsam Analizi Dokümanı”nda belirtilen kuruluşumuzdaki tüm tedarikçi yönetimlerini kapsar.

3. Sorumluluk

Rol/Unvan Görev	Üst Yönetim	Üst Yönetim Temsilcisi	BGYS Yöneticisi	BGYS Ekip Üyeleri	Diğer Çalışanlar
Dokümanın Hazırlanması			X	X	
Dokümanın Kontrolü			X	X	
Dokümanın Onaylanması	X	X			
Dokümanın Yayınlanması			X		
Dokümanın Güncellenmesi			X		
Dokümanın Uygulanması	X	X	X	X	X
Dokümanın Uygulamadan Kaldırılması	X	X			

4. Kısaltmalar ve Tanımlar

Terim	Tanım/Açıklama
BGYS	Bilgi Güvenliği Yönetim Sistemi
Kurum	Kuruluşumuzun Kapsam Analizi Dokümanı’nda belirtilen birimleri
Politika	Bir şirket, kurum veya kişinin görüş, felsefe, amaç ve tutumunun belirli şekilde ifadesini, bu görüş, felsefe veya amaç doğrultusunda bir hareket planını içeren doküman tipidir.

HAZIRLAYAN	ONAYLAYAN
BGYS Yöneticisi	Üst Yönetim Temsilcisi/Üst Yönetim
KURUMA ÖZEL	

	TEDARİKÇİ İLİŞKİLERİNDE BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	PL.11
		Yayın Tarihi	01.04.2022
		Revizyon No	00
		Revizyon Tarihi	-
		Sayfa No	: Sayfa 4 / 8

Terim	Tanım/Açıklama
Tedarikçi	Kurum'a sözleşmeler ile mal ve hizmet sağlayan ya da, Kurum adına çalışan yüklenicilere verilen genel isimdir.

5. Tedarikçi İlişkileri Bilgi Güvenliği Politikası

Kurum, iş süreçlerinin işleyişini, devamlılığını ve kalitesini arttırmak için tedarikçiler ile çalışmalar yapmaktadır. Kurum'a ait Tedarikçi Listesi, birlikte çalışılan tüm tarafları kapsar. Yapılan bu çalışmalar esnasında çalışma şartlarının belirlenmesi ve dokümente edilmesi hem Kurum'un hem de tedarikçinin sorumluluğundadır.

Tedarikçi ilişkilerini yönetmek için, alınan mal ya da hizmetler bilgi güvenliğini etkileyecek türde ise, her birim kendi risk eğilimine ve çalışacağı tedarikçinin türüne göre tedarik sürecini planlar, süreç dâhilinde bilgi varlıklarına erişim türünü belirler, verilen erişim izinlerini izler, Kurum politikaları ile prosedürlerine uyumu sağlar ve bilgi güvenliği farkındalığını arttırmak için gerekli uygulamaları gerçekleştirir.

5.1. Tedarikçi İlişkilerinde Bilgi Güvenliği Gereksinimleri

Tedarikçi ilişkilerini izlemek için, iş veya proje türüne bakılmaksızın alınan mal ya da hizmetler bilgi güvenliği gereksinimlerine göre değerlendirilir.

Bilgi güvenliği gereksinimlerini karşılamak amacıyla aşağıdaki hususlar, uygulanabilirliklerine bakılmak suretiyle sözleşmelere dâhil edilir:

- (1) Sağlanacak ya da erişilecek bilginin tanımı ve bilgi sağlama ve erişim yöntemleri.
- (2) Erişilecek bilginin sınıfı ve yetkilendirilmesi ile ilgili konular.
- (3) Yasal düzenlemeler, bilgi sızdırılması, fikri mülkiyet hakları ve telif hakları gibi konular.
- (4) Kabul edilebilir hizmet kesintisi süreleri.
- (5) Performans değerlendirme, izleme, raporlama ve denetim gibi kontrollerde sözleşme taraflarının yükümlülükleri.
- (6) Kurum varlıklarının kabul edilebilir kullanım kuralları.
- (7) Kurumun bilgi varlıklarına erişecek tedarikçilerin personel listesi.
- (8) Kurum varlıklarına erişecek personelin güvenlik taramaları için bilgilerin temin edilmesi.
- (9) Tedarik sürecinde Kurum bünyesinde çalışacak personelin Kurum politika ve prosedürlerine uyması.
- (10) Sözleşme ile ilgili tedarik süreçlerinin denetim ve değerlendirme hakkının iş/proje sahibi birimine ait olduğu.
- (11) Çatışma ve kusur durumunda çözüm süreçleri.
- (12) Periyodik kontroller ve raporlarda tespit edilen konuların zamanında düzeltilmesi konusunda rapor sunma yükümlülüğü.
- (13) Kurumun güvenlik gerekliliklerine göre tedarikçinin yükümlülükleri.
- (14) Kurum kurallarının, tedarikçilerin alt tedarikçilerine de uygulanacağını belirtilmesi.

HAZIRLAYAN	ONAYLAYAN
BGYS Yöneticisi	Üst Yönetim Temsilcisi/Üst Yönetim
KURUMA ÖZEL	

 BURDUR MEHMET AKİF ERSOY ÜNİVERSİTESİ	TEDARİKÇİ İLİŞKİLERİNDE BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	PL.11
		Yayın Tarihi	01.04.2022
		Revizyon No	00
		Revizyon Tarihi	-
		Sayfa No	: Sayfa 5 / 8

(15) Tedarikçinin, tedarik zinciri boyunca Kurum’un güvenlik gereksinimlerini uygulaması gerektiği.

(16) Kurum tedarik zinciri içinde tedarikçiler arasında olası sorunlar ve uzlaşmalar ile ilgili bilgi paylaşımı için kuralların belirlenmesi.

(17) Sözleşmenin bitmesinden itibaren gizliliğin korunmasına yönelik maddelerin belirtilmesi.

Kurum, tedarikçiler ile yaptığı anlaşmaların yanı sıra “Kurumsal Gizlilik Sözleşmesi” ile güvenlik gereksinimlerini karşılar. Bu konudaki yetki ve sorumluluklar “Roller ve Sorumluluklar Kılavuzu”nda belirtilmiştir.

Tedarik sürecinde, Kurum bünyesinde daimi çalışacak, Gizlilik seviyeli bilgiye erişim yetkisi olan üçüncü taraf personelinin bilgi güvenliği farkındalık eğitimi almış olması zorunludur. Bu eğitimlerde Kurum bilgi güvenliğine uygun çalışma ve davranma kuralları konusunda bilgilendirme yapılır. Bu hususun planlanması ve kontrolü iş veya proje sahibi birimin sorumluluğundadır.

Tedarikçi personelinin bilgi varlıklarına erişimleri “Erişim Kontrol Politikası”na uygun olarak yapılır.

5.2. Tedarikçi Hizmet Sağlama Yönetimi

Kurum, tedarikçiler ile imzaladığı sözleşmeler kapsamında tedarikçi hizmetlerini izler, gözden geçirir ve değişiklikleri yönetir.

5.2.1. Tedarikçi İlişkilerini İzleme ve Gözden Geçirme

Kurum, tedarikçi hizmetlerinin izlenmesi ve gözden geçirilmesini denetlerken en az aşağıdaki hususları kontrol eder ve izler:

- (1) Sözleşmelere uyulduğunu doğrulamak için hizmet performans düzeyinin izlenmesi.
- (2) Tedarikçi tarafından sağlanan hizmetin, raporlarının düzenli toplantılar ile kontrol edilmesi.
- (3) Bilgi güvenliği ihlal olayları hakkında verilen bilgiler.
- (4) Varsa yapılan bağımsız denetim raporlarının ilgili kısımlarının görüşülerek mutabakata varılması.
- (5) Tedarikçinin hizmet sırasında yaşadığı operasyonel sorunlar, başarısızlıklar ve hatalar, teslim hizmeti ile ilgili aksamalar.
- (6) Tedarikçinin, sorunları tespiti ve çözümündeki etkisi.
- (7) Varsa kendi tedarikçileri ile ilişkilerinde bilgi güvenliği yönetiminin işletilmesi.
- (8) Tedarikçinin, hizmet arızaları veya felaket gibi durumlarda sözleşmelerde belirtilen hizmet kalemlerinin sürekliliğini sağlaması.
- (9) Hizmet sürekliliğini sağlayacak kalitede yeterli/yedekli personel bulundurması.

HAZIRLAYAN	ONAYLAYAN
BGYS Yöneticisi	Üst Yönetim Temsilcisi/Üst Yönetim
KURUMA ÖZEL	

	TEDARİKÇİ İLİŞKİLERİNDE BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	PL.11
		Yayın Tarihi	01.04.2022
		Revizyon No	00
		Revizyon Tarihi	-
		Sayfa No	: Sayfa 6 / 8

5.2.2. Tedarikçi Hizmetlerindeki Değişiklikleri Yönetme

Tedarikçiler tarafından sağlanan hizmetlerin devamlılığı ve iyileştirilmesi için; değişen iş bilgileri, politikalar ve prosedürler, bilgi sistemleri ve ilgili süreçlerin hassasiyeti dikkate alınarak, risklerin yeniden değerlendirilmesi de dâhil olmak üzere tüm değişiklikler kontrol edilir.

Hizmet değişiklikleri yönetimi yapılırken en az aşağıdaki adımlar kontrol edilir:

Kurum tarafında:

- (1) Sunulan hizmetteki gelişmeler.
- (2) Kurumdaki teknolojik ve görevsel değişiklikler.
- (3) Kurumun politika ve prosedürlerindeki değişiklikler.
- (4) Güvenlik kontrollerindeki değişiklikler.

Tedarikçi tarafında;

- (1) Kullanılan teknolojilerdeki değişiklikler.
- (2) Yeni ürün veya sürümlerdeki değişiklikler.
- (3) Hizmet tesislerindeki değişiklikler.
- (4) Yeni alt yükleniciler ile yapılan sözleşmeler.
- (5) Hizmet veren personeldeki değişiklikler.

5.3. Tedarik Hizmetlerinin Değerlendirilmesi

Kurum, tedarik süreci boyunca gerektiği durumlarda tedarikçiyi denetleme hakkına sahiptir ve denetim hizmet alan birimin sorumluluğundadır.

Kurum, tedarikçileri sözleşmelerde belirlenen süreler ve kriterlere göre değerlendirir. Bilgi güvenliğini sağlamak için Teknik Şartname veya Gizlilik Sözleşmesine eklenen 5.1 Tedarikçi İlişkilerinde Bilgi Güvenliği Gereksinimleri başlığında belirtilen ilgili maddelerin yerine getirilip getirilmediği kontrol edilir.

Tedarikçi değerlendirme kriterleri “Onaylı Tedarikçi Listesi” üzerinde tanımlanmıştır.

Olumsuz bir durum var ise yükleniciye yazılı olarak bilgilendirme yapılır ve şartname/sözleşme koşullarına göre gerekli yaptırımlar uygulanır.

HAZIRLAYAN	ONAYLAYAN
BGYS Yöneticisi	Üst Yönetim Temsilcisi/Üst Yönetim
KURUMA ÖZEL	

 BURDUR MEHMET AKİF ERSOY ÜNİVERSİTESİ	TEDARİKÇİ İLİŞKİLERİNDE BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	PL.11
		Yayın Tarihi	01.04.2022
		Revizyon No	00
		Revizyon Tarihi	-
		Sayfa No	: Sayfa 7 / 8

6. İlgili Dokümanlar

6.1. İç Kaynaklı Dokümanlar

- (1) KA.01 BGYS Kapsam Analizi
- (2) PL.07 Erişim Kontrol Politikası
- (3) KL.01 Roller ve Sorumluluklar Kılavuzu
- (4) SZL.01 Kurumsal Gizlilik Sözleşmesi
- (5) LS.09 Tedarikçi Listesi
- (6) FR.08 Tedarikçi Değerlendirme Formu

6.2. Dış Kaynaklı Dokümanlar

- (1) TS ISO/IEC 27001:2013 Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler

HAZIRLAYAN	ONAYLAYAN
BGYS Yöneticisi	Üst Yönetim Temsilcisi/Üst Yönetim
KURUMA ÖZEL	

 BURDUR MEHMET AKİF ERSOY ÜNİVERSİTESİ	TEDARİKÇİ İLİŞKİLERİNDE BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	PL.11
		Yayın Tarihi	01.04.2022
		Revizyon No	00
		Revizyon Tarihi	-
		Sayfa No	: Sayfa 8 / 8

Revizyon Kayıtları

Rev. No	Tarih	Hazırlayan	Revizyon Nedeni /Sayfa No	Onaylayan	İmza
1					
2					
3					
4					
5					

HAZIRLAYAN	ONAYLAYAN
BGYS Yöneticisi	Üst Yönetim Temsilcisi/Üst Yönetim
KURUMA ÖZEL	