



Tedarikçi Yönetimi Prosedürü

Doküman No	PR.07
İlk Yayın Tarihi	20.02.2018
Revizyon No	0
Revizyon Tarihi	
Sayfa No	

1. AMAÇ

Bu prosedür, Karamanoğlu Mehmetbey Üniversitesine Bilgi İşlem Daire Başkanlığı dış kaynak kullanımı, kuruluşun temel yetkinliklere eğilme, finansal fayda sağlama ve rekabet üstünlüğü sağlama konularında uygulanacak kuralları oluşturmayı amaçlar.

2. KAPSAM

Bu prosedür, Karamanoğlu Mehmetbey Üniversitesinin Bilgi İşlem Daire Başkanlığı tüm dış kaynak ve tedarikçileri kapsar.

3. SORUMLULAR

- Bilgi İşlem Daire Başkanlığı

4. TANIMLAR

5. UYGULAMA

5.1 Dış Kaynak Kullanım (Outsourcing) Prosedürleri

5.1.1 Amaçlar ve Hedefler

Bilgi İşlem Daire Başkanlığı ve ilgili iş birimleri (Bkz. Sistem Kabulü Prosedürleri) dış kaynak kullanım girişiminin amaç ve hedeflerini sunar ve sürecin kuruluşu nasıl bir fayda sağlayacağını belirtir. Dış kaynak kullanımı, kuruluşun temel yetkinliklere eğilme, finansal fayda sağlama ve rekabet üstünlüğü sağlama amaçlarına hizmet eder.

5.1.2 Ekibin Oluşturulması

Ekibin oluşturulması ve dış kaynak kullanımının değerlendirilmesi için gerekli koordinasyonu Bilgi İşlem Yöneticisi sağlar. Ekip finans bölümünden en az bir kişi içerir ve Bilgi İşlem Yöneticisi tarafından yönetilir.

5.1.3 Kurum Gerekçeleri

Teknolojik altyapı planlamalarında, Bilgi İşlem Yöneticisi/Bilgi Güvenliği Yöneticisi ve ilgili süreç sahibi bir faaliyet için dış kaynak kullanımının gerekçelerini tanımlar ve dokümante eder ve dış kaynak kullanımı için maliyet-fayda analizi gerçekleştirir.

Hazırlayan		Onaylayan



Tedarikçi Yönetimi Prosedürü

Doküman No	PR.07
İlk Yayın Tarihi	20.02.2018
Revizyon No	0
Revizyon Tarihi	
Sayfa No	

5.1.4 Bilgi Talebi

Maliyet-fayda analizinin hazırlanmasına ve teklif detaylarının belirlenmesi için gerekli teknik bilginin edinilmesine olanak sağlamak amacıyla, ekip, olası teklif sahiplerine resmi Bilgi Talebi'nde (RFI) bulunur.

5.2 Çalışanlara Duyurulması

Kurum tarafından alınacak hizmetin etkileyeceği çalışanlara, dış kaynak kullanım gerekçelerini ve Operasyonel yaklaşımları bildirir.

Yönetim, çalışanlarına, üçüncü partilerle ilişkilerin nasıl sürdürülmesi gerektiğini duyurur. Bu durum, Kurum çalışanları ile üçüncü taraflar arasında bir köprü oluşması ve tamamlayıcı rollerin anlaşılması açısından oldukça önemlidir.

5.3 Tedarikçi Seçme Prosedürü

5.3.1 Teklif Daveti

Bilgi İşlem Yöneticisi/Bilgi Güvenliği Yöneticisi ve ilgili süreç sahibinden gerekli onayın alınmasının ardından, dış kaynağın kullanılacağı faaliyet için tedarikçi seçim süreci başlatılır. Teklif için alınabildiği durumlarda en az üç adet sağlayıcı davet edilir. Ürün veya hizmet tedariki sürecinde, standartlarda belirtilen, ana (çerçeve) sözleşmesi olan ya da tercih edilen tedarikçiler listesinde bulunan tedarikçiler için çoklu teklif gerekli değildir. Tercih edilen tedarikçi listesindeki tedarikçiler, Bilgi İşlem Yöneticisi/Bilgi Güvenliği Yöneticisi ve ilgili süreç sahibi tarafından belirlenir ve her sene listedeki tedarikçiler üzerinde değerlendirmeler gerçekleştirilerek, gerekirse bu liste güncellenir.

İstisnai durumlar dokümante edilerek Bilgi İşlem Yöneticisi/Bilgi Güvenliği Yöneticisi ve ilgili süreç sahibi tarafından onaylanır. Teklifte bulunacak taraflara uygun bir cevap dönüş tarihi ile resmi bir Teklif Talebi (RFP) geçilir.

5.3.2 Tedarikçi Analizi ve Değerlendirmesi

Ürün veya hizmetin dokümantasyonunu sağlayacak, verilecek hizmetlerin işlevselliğini veya detaylarını sunacak ve resmi tekliflerde bulunacak muhtemel tedarikçiler belirlenir. Ayrıca, referanslar ve daha önce yapılan işler de dâhil tüm tedarikçi bilgisi kontrol edilir. İstenen kalite, kabul görececek performans ve kriter, sözleşme hükümleri, ödeme seçenekleri ve bunların verilecek hizmetlerle doğrudan bağlantısını detaylı şekilde gösteren bir sözleşme hazırlanır.

Tedarikçi analizi, minimumda, tedarikçi seçim kriterinde bahsi geçen uygun parametreleri içerir.

Hazırlayan		Onaylayan



Tedarikçi Yönetimi Prosedürü

Doküman No	PR.07
İlk Yayın Tarihi	20.02.2018
Revizyon No	0
Revizyon Tarihi	
Sayfa No	

Kurum, gerektiğinde üçüncü partilerin tayin edeceği personelin yetkinliğini sorgular ve analiz eder.

5.3.3 Tedarikçi Seçimi

Analiz ve değerlendirme kriterine bağlı olarak, ilgili süreç sahipleri Kurum gereksinimlerini en iyi karşılayan tedarikçiyi seçer. İlgili süreç sahipleri tedarikçiden kaynaklanacak olası risk etkenlerini belirlemek için yazılı olarak emniyet müdürlüğünden tedarikçi hakkında bilgi alır ve Elektronik Kamu Alımları Platformu (EKAP) üzerinden yasaklı olup olmadığını sorgular. Sunulan değerlere göre en son kararı verecek olan ilgili süreç sahipleridir.

5.4 Sözleşmeler, Hizmet Seviyesi Anlaşması (SLA) ve Gizlilik Anlaşması (NDA)

Tedarikçi seçildikten sonra, hizmet sağlayıcıyla resmi bir sözleşme imzalanır. Sözleşme, Kurum'un ve tedarikçinin uymak zorunda olduğu tüm yasaları içerir. Sözleşme, belirlenen seviyede kesintisiz ve etkili ve Kurum operasyonlarını aksatmayan bir hizmet alınması için güçlü bir Hizmet Seviyesi Anlaşması (SLA) ile bağlanır. Bu anlaşmadaki hizmet seviyeleri, iki taraf için de adil, eşit, açık ve eksiksiz olacak şekilde hazırlanır. Ayrıca, SLA, çıkış maddelerini açık olarak içerir. Sözleşme ve SLA' da olması gereken çeşitli maddeler için bkz. Tedarikçi Yönetimi Standardı.

Kurum şunları sağlamakla yükümlüdür:

- Tedarikçi performansının yönetilmesi ve ölçülmesi için ölçülebilir parametrelerle SLA kullanımı
- Sözleşmenin yenilenmesinden önce geçmiş performansın gözden geçirilmesi için uygun zaman aralığı

5.4.1 Diğer Bölümlerle Yapılan Servis Seviyesi Anlaşmaları

Üçüncü taraflar dışında, Kurum ilgili bölümlerle de (Kurumlarla) SLA imzalar. Bu SLA, Kurum diğer bölümlerin tüm sorumluluklarını ve iki taraftan da beklenen servis seviyelerini açık bir şekilde tanımlar.

Baş koordinatörler ve raporlama prosedürleri gibi diğer hususlar da SLA şeklinde tanımlanır ve düzenlenir.

5.5 Tedarikçi İlişkileri Yönetimi

Teknolojik planlamalar doğrultusunda, Operasyonel yönetim ve kapsamlı ilişki yönetimini göz önünde bulundurulur.

Kurum ve tedarikçiden birer kişi Operasyonel konuların yönetimi için tek irtibat noktası olarak seçilir. Her bir tedarikçi için, dış kaynak kullanımı ile ilgili çözümlenmemiş konuların çözülmesi amacıyla uygun bir raporlama hiyerarşisi kurulur. Bilgi İşlem Yöneticisi/Bilgi

Hazırlayan		Onaylayan



Tedarikçi Yönetimi Prosedürü

Doküman No	PR.07
İlk Yayın Tarihi	20.02.2018
Revizyon No	0
Revizyon Tarihi	
Sayfa No	

Güvenliği Yöneticisi ve ilgili süreç sorumluları, kuruluşun karşılaştığı Operasyonel hususlar ile ilgili konuları düzenli olarak takip eder.

5.6 Tedarikçi Değerlendirmesi

Kurum, mevcut tedarikçilerin değerlendirilmesi, sınıflandırılması ve tedarikçiye daha iyi hizmet vermesi için yapıcı geri bildirimlerde bulunulması amacıyla, bir tedarikçi geliştirme programı hazırlanır. Tedarikçinin verdiği hizmetin kalitesini ölçmek için tedarikçi değerlendirme formu oluşturulur.

Değerlendirmenin bir parçası olarak sağlanan hizmetin ya da verinin kritikliğine bağlı olarak, Kurum kendisine ait herhangi gizli / hizmete özel / kurum içi bilginin güvenli bir şekilde sürdürüldüğünü kontrol etmek için hizmet sağlayıcının iç kontrol yapısını gözden geçirebilir ya da gözden geçirilmesini talep edebilir.

Tedarikçiye, tedarikçi değerlendirme matrisinde yer alan kısımlardan geçerli olanlar için bir not verilir.

Tedarikçinin SLA maddelerini sağlayamaması durumu, tedarikçi değerlendirme sürecini hükümsüz kılar. Kurum, bu durumda, sözleşmede yer alan hükümlere göre gerekli aksiyonları alır.

5.7 Tedarikçi Yönetimi Standardı

5.7.1 Sözleşme Hususları

Yasal hususların dışında, Kurum tedarikçiyle yapılan sözleşmede aşağıda yer alan bilgi güvenliği ile ilgili maddeleri de göz önünde bulundurur.

- Bilgi Güvenliği hakkında genel politika
- Varlıkların korunması ile ilgili prosedürler
- Alınacak hizmetlerin her biri için açıklama
- Gerekli olduğunda personel sağlanması
- Sözleşme gereği tarafların yükümlülükleri
- Belirli erişim kontrolü prosedürleri
- Problem çözümü için eskalasyon sürecinin oluşturulması – gerekli olduğu noktalarda acil durum düzenlemelerinin de uygulanabileceği
- Donanım ve yazılım kurulumu ve bakımı ile ilgili sorumluluklar
- Belirli bir değişiklik yönetimi süreci
- Üçüncü partinin taşeronlarla olan ilişkisi
- Bilgi güvenliği ile yasal yükümlülüklerin nasıl yerine getirildiği
- Taşeronlar dâhil tüm dış kaynaklarda, güvenlik sorumlulukları ile ilgili farkındalık yaratılması için yapılan düzenlemeler
- Kuruluşun işletme varlıklarının bütünlüğü ve gizliliğinin nasıl korunacağı ve test edileceği
- Kuruluşun hassas işletme bilgisine erişimin yalnızca yetkili kullanıcılarla olması için uygulanacak fiziksel ve mantıksal kontroller

Hazırlayan		Onaylayan



Tedarikçi Yönetimi Prosedürü

Doküman No	PR.07
İlk Yayın Tarihi	20.02.2018
Revizyon No	0
Revizyon Tarihi	
Sayfa No	

- Olağanüstü bir durum olduğunda (deprem, sel vb.) hizmetlerin erişilebilirliğinin nasıl korunacağı
- Dış kaynak kullanımı yoluna gidilen donanım için hangi seviyede fiziksel güvenlik sağlanacağı
- Süreçleri ve güvenlik kontrollerini gözden geçirme ve denetleme hakkı
- Kurum konuda tedarikçiden talep edeceği güvenlik hükümlerini yazılı olarak hazırlar.

5.7.2 SLA Hususları

Taraflar	
Kurum	Kurum bilgileri (lokasyon, iletişim bilgileri ve bağlantıya geçilecek kişilerin isimlerini içerecek şekilde)
Tedarikçi	Tedarikçi bilgileri (İsimler, unvanlar, lokasyonlar, iletişim numaraları ve adresini içerecek şekilde)
Anlaşma	
Hizmetler	“Hizmet koşulları” üzerinde anlaşma; aşağıda
Personel Yetkinliği	Tedarikçinin sağlayacağı personelin yetkinlikleri
Personelin Erişilebilirliği	Seçilen tedarikçi personelinin minimum ne kadar süre ile hizmet vereceğinin bilgisi.
Değişiklikler	“Hizmet değişiklik prosedürlerinde” anlaşma; aşağıda
Acil Durum Planı	“Acil Durum planlama prosedürlerinde” anlaşma; aşağıda
Sonlandırma	Sözleşme sonlandırma koşulları üzerinde anlaşma
	Hizmet Koşulları
Kurum Gereksinimi	Kurum gereksiniminin genel tanımı ve dış kaynak kullanımı nedenleri
Sağlanacak Hizmetlerin Beyanı	Sağlanacak her bir hizmetin tanımı; son kullanıcıları, performans kriteri (Servis Seviyesi) ve performans değerlerini içerecek şekilde
Kaynaklar	Tedarikçinin, sağlayacağı hizmetler için kullanacağı kaynakların tanımı
Güvenlik	Kurum’un uygulamalarını ve verisini korumak için kullanılacak güvenlik yöntemlerinin tanımı
Destek	Kurum’a sağlanacak desteğin, Servis Seviyeleri’ni ve performans kriterini de içeren tanımı
Kısıtlamalar	Hizmetlerin sağlanmasındaki, operasyon saatleri, servis seviyeleri gibi kısıtlamaların tanımı
Raporlama	Sağlanacak servis seviyeleri ve performans değerlerine ait istatistiklerin detaylarını içerecek şekilde standart raporlama sürecinin tanımı
	Tedarikçinin talebi üzerine Kurum’un gerekli bilgiyi sağlamada takip

Hazırlayan		Onaylayan



Tedarikçi Yönetimi Prosedürü

Doküman No	PR.07
İlk Yayın Tarihi	20.02.2018
Revizyon No	0
Revizyon Tarihi	
Sayfa No	

Eğitim	edeceği süreçlerin tanımı Kurum'un Servis Seviyeleri'nin belirlenmesi için kullanılan istatistik ve performans değerlerinin raporlamasını takip etmek için kullandığı süreçlerin tanımı
Performans Ölçümü	Kurum'un alabileceği eğitimlerin tanımı (hizmetlere yönelik eğitimler ve diğer uygun eğitimler)
Hizmet Değişikliği Prosedürleri	Müşteri memnuniyetinin ölçüleceği yöntemlerin tanımı (Servis seviyeleri, performans değerleri vs.)
Talep Edilen Değişiklikler	Kurum'un değişiklik talebi için kullanacağı sürecin tanımı
Beklenen Gelişim	Kurum tarafından, hizmetlerin geliştirilmesine imkan vermek için kullanılan süreç ve yöntemlerin tanımı (Servis Seviyeleri'ndeki gerekli değişiklikleri de içerecek şekilde)
Acil Durum Planlama Prosedürleri	
Kesintiler	Kurum'a planlanmış kesintileri bildirmedeki Servis Seviyeleri ve sürecin tanımı
Hata Düzeltimi	Hizmet hataları ve aksaklıkları için kullanılacak sürecin, Kurum tarafından alınan/planlanan aksiyonların izlenebilmesini sağlayacak yöntemleri de içerecek şekilde tanımı
Eskalasyon	Tedarikçi tarafından hataların ve aksaklıkların düzeltilmesi için kullanılacak raporlama prosedürlerinin, iletişim noktaları, raporlama yöntemleri, hataların tanımlanması için gerekli bilgi, hata öncelikleri ve olası etkileri de içerecek şekilde tanımı
Güvenlik Gereksinimleri	
Politika	Bilgi Güvenliği genel politikası
Varlık Korunumu	Kuruluş varlıklarını (bilgi ve yazılımı) korumaya yönelik prosedürler Varlıkların tehlikeyle (verinin kaybı ya da değiştirilmesi gibi) karşı karşıya olup olmadığını belirlemek için kullanılacak prosedürler Bilgi ve varlıkların sözleşme sonunda veya kararlaştırılmış bir zamanda iade edilmesi veya imha edilmesi, Bütünlük ve erişilebilirlik Bilginin kopyalanmasının ve açıklanmasının kısıtlanması
Yükümlülükler	Tarafların sözleşmeyle ilgili yükümlülükleri
Tazminat	Kurum'un verilen yetersiz hizmetten ötürü maruz kalacağı kayıpların karşılanması için gerekli düzenlemeler

Hazırlayan		Onaylayan



Tedarikçi Yönetimi Prosedürü

Doküman No	PR.07
İlk Yayın Tarihi	20.02.2018
Revizyon No	0
Revizyon Tarihi	
Sayfa No	

Bildirim

Güvenlik olayları ve güvenlik ihlallerinin incelenmesi, bildirim ve raporlanması için gerekli düzenlemeler

6. İLGİLİ DOKÜMAN

- Tedarikçi Yönetimi Politikası
- Kabul Edilebilir Kullanım Politikası
- Varlık Yönetimi Politikası

Hazırlayan		Onaylayan