CİNER GRUBU ŞİRKETLERİ ÜÇÜNCÜ TARAF YÖNETİM POLİTİKASI

Doküman Kodu	POL.28
İlk Yayın Tarihi	24.05.2022
Revizyon Tarihi	20.11.2025
Revizyon No	02
Gözden Geçirme Tarihi	20.11.2025
Sayfa Sayısı	1 / 3

1.AMAÇ

Ciner grubu şirketleri, tüm satıcılar için BT ve bilgi güvenliği ile ilgili riskleri ve kontrolleri yöneten kurallar oluşturur.

2.KAPSAM

Bu politika;

- *Hizmet alınan tüm dış firmaları,*
- *Ürün veya hizmet sağlayan tedarikçileri,*
- *Kurum adına hizmet gerçekleştiren taşeronları,*
- *Bu kuruluşlarda çalışan tüm personeli kapsar*

3.TANIMLAR

Üçüncü Taraf: Kurum dışından, sözleşme veya hizmet anlaşması ile çalışan tüm kişi ve kuruluşlardır.
Tedarikçi: *Kuruma ürün veya hizmet sağlayan kişi veya kuruluş*
Taşeron: *Kurum adına belirli bir hizmeti yerine getiren dış kişi veya kuruluş.*
Erişim Yetkisi: *Üçüncü taraflara kurum sistemleri veya verilerine iş gerekliliklerine göre verilen erişim izni.*

4.SORUMLULAR

Üçüncü taraflar bu politikalara uymakla yükümlüdür. Gerektiğinde BT Direktörlüğü ve İç Denetim birimi tarafından denetlemeler yapılabilir.

5. ÜÇÜNCÜ TARAF RİSK DEĞERLENDİRMESİ

*Her üçüncü taraf ile çalışmaya başlanmadan önce; veri güvenliği, erişim gereksinimleri ve diğer bilgi güvenliği risklerine ilişkin **ön risk değerlendirmesi** yapılır*. Daha sonra, *devam eden süreçte Tedarikçi tarafından uygulanan kontroller ve Ciner Grubu bilgi güvenliği kontrolleri* ışığında bu riskleri değerlendirmek ilgili departman yöneticisinin ve BT Direktörünün sorumluluğundadır. BT Direktörü, tedarikçi katılımı boyunca etkinliklerini değerlendirmek için bu kontrollerin durumunu düzenli olarak gözden geçirmelidir; gözden geçirme sıklığı, riskin boyutuna ve doğasına bağlı olarak BT Direktörünün ve ilgili departman yöneticisinin takdirine bağlı olarak belirlenecektir.

HAZIRLAYAN	**ONAYLAYAN**
YÖNETİM TEMSİLCİSİ	**YÖNETİM KURULU ÜYESİ**

6.SÖZLEŞME YÜKÜMLÜLÜKLERİ

Üçüncü taraf sözleşmelerine gerekli görüldüğünde aşağıdaki hükümler eklenmelidir:

- *Gizlilik anlaşmaları (NDA)*
- *BT güvenlik kontrollerine uyum şartları*
- *Veri koruma ve erişim yönetimi maddeleri*
- *Olay bildirim yükümlülükleri*

Bu düzenlemelerin imzalanmasından ve tedarikçi uyumluluğunun izlenmesinden CIO ve BT Direktörü sorumludur.

İhlal durumunda uygulanabilecek yaptırımlar:

- *Maddi tazminat*
- *Erişim yetkilerinin kaldırılması*
- *Sözleşmenin feshi*

7.ERİŞİM KOTROLLERİ

Üçüncü taraf erişimleri aşağıdaki prensiplere uygun olmalıdır:

- *Sadece iş gereklilikleri doğrultusunda verilmelidir.*
- *Sınırlı süreli olmalıdır.*
- *Güvenli ve izlenebilir yöntemlerle sağlanmalıdır.*
- *Gerektiğinde derhal sonlandırılmalıdır.*

Tedarikçilere sistem erişimi verilmesi halinde, BT Direktörü her ay erişim loglarını inceleyerek tedarikçi faaliyetlerinin uygunluğunu kontrol eder.

8.DEVAM EDEN DEĞERLENDİRMELER

Altı aydan uzun süren çalışmalarda şirket, BT risklerini ve kontrol ortamının uygunluğunu üçer aylık dönemlerde yeniden değerlendirecek, bu, BT Direktörü ve ilgili departman yöneticisi tarafından gerçekleştirilecektir. *Yeni riskler veya* gerekli kontrol *iyileştirmeleri* BT Direktörü tarafından *raporlanır ve Tedarikçinin aksiyon alınması gerektiren durumda bildirim yapılır.*

HAZIRLAYAN	ONAYLAYAN
YÖNETİM TEMSİLCİSİ	YÖNETİM KURULU ÜYESİ

9. SÖZLEŞMENİN SONLANDIRILMASI VE SONRASI

Sözleşme veya çalışma süreci sona erdiğinde üçüncü taraf aşağıdaki yükümlülükleri yerine getirmelidir:

Kuruma ait tüm belge, veri, yazılım ve ekipmanları iade etmek.
Dijital ortamda tutulan kurum verilerini geri döndürülemez şekilde silmek.
Kurum talep ettiğinde erişim loglarını BT birimine teslim etmek.

Bu yükümlülüklerin doğrulanmasından ilgili BT birimi sorumludur.

10.İLGİLİ DOKÜMANLAR

BT Üçüncü Taraf Tedarik Süreci
FR- 14 Üçüncü Taraf Gizlilik Sözleşmesi Formu
POL-20-Üçüncü Taraf Güvenlik Politikası

HAZIRLAYAN	ONAYLAYAN
YÖNETİM TEMSİLCİSİ	YÖNETİM KURULU ÜYESİ