

Tedarikçi Yönetiminde Bilgi Güvenliği Prosedürü

AMAÇ

Bu prosedürün amacı, kurum tarafından hizmet alınan tüm tedarikçi, yüklenici, danışman, taşeron ve üçüncü tarafların bilgi güvenliği gerekliliklerine uyumunu sağlamak, tedarikçi kaynaklı bilgi güvenliği risklerini azaltmak, kurum verilerinin gizlilik, bütünlük ve erişilebilirliğini korumaktır.

KAPSAM

Bu prosedür Mal/hizmet tedarik eden tüm firmaları, Yazılım, donanım, bakım-destek sağlayıcılarını, Bulut hizmeti, veri depolama, ağ/donanım sağlayıcılarını, Uzaktan erişim ile hizmet veren tedarikçilerini, KVKK kapsamında veri işleyen konumundaki tedarikçileri, Tedarikçi personellerini, Tedarikçilerle yapılan tüm bilgi alışverişleri, erişimler, sözleşmeler ve teslim süreçleri bu kapsamda değerlendirilir.

UYGULAMA

Tedarikçi Güvenlik Gereksinimlerinin Tanımlanması

Her tedarikçi için aşağıdaki güvenlik kriterleri değerlendirilir:

- Hizmet kritiklik seviyesi
- İş sürekliliğine etkisi
- Veriye erişim durumu (erişiyor/erişmiyor)
- Kişisel veri işleyip işlemediği
- Dış sistemlere bağlantı gerekip gerekmediği
- Bulut altyapısı kullanıp kullanmadığı
- Geçmiş güvenlik ihlalleri veya riskleri

Tedarikçi riskleri BGYS risk analizine dahil edilir.

Tedarikçi Sözleşmelerinde Güvenlik Hükümleri

Tüm sözleşmelerde: Gizlilik yükümlülüğü (NDA), KVKK veri işleyen yükümlülükleri, Erişim kontrolü ve yetkilendirme, Uzak bağlantı kurallarına uyum, Loglama ve kayıt yükümlülüğü, Güvenlik ihlali bildirim süresi (en fazla 24 saat), Yetkisiz personelin erişimini engelleme, Alt yüklenicilerin kurallara uyması, Hizmet sona erdiğinde tüm verilerin imhası/teslimi zorunludur.

Tedarikçi Erişim Yönetimi

Erişim Talepleri: Her tedarikçi için "Tedarikçi Erişim Talep Formu" oluşturulur. Form ilgili birim yöneticisi + BGYS + Bilgi İşlem tarafından onaylanmadan erişim açılmaz.

Yetki Sınırlaması: Asgari yetki prensibi uygulanır. Tedarikçinin erişebileceği sistemler tanımlanır. Erişim süreli ve kapsamı kısıtlı olmalıdır (örn. 2 saatlik destek erişimi).

Uzak Bağlantı: Tüm tedarikçi bağlantıları VPN + MFA ile yapılır. Varsayılan parola veya paylaşılmış hesap kullanılmaz. Uzak bağlantılar her zaman loglanır ve izlenir.

Tedarikçi Güvenlik İzleme ve Denetimi: Periyodik Denetimler, Kritik tedarikçiler yılda en az 1 kez denetlenir. Bulut hizmet sağlayıcıları için SOC2/ISO 27001 gibi sertifikalar talep edilir.

Tedarikçi Yönetiminde Bilgi Güvenliği Prosedürü

Log Kayıtları: Tedarikçilerin sistemlere erişimi sırasında oluşan loglar en az 2 yıl saklanır. Şüpheli girişimler derhal incelenir.

Performans ve Uyum Kontrolleri: SLA, bakım sözleşmeleri ve güvenlik gerekliliklerine uyum takip edilir. Kritik hizmetlerde aylık/çeyreklik raporlama zorunludur.

Güvenlik İhlali ve Bildirim Süreci: Tedarikçi kaynaklı bir olay yaşanırsa: Tedarikçi en geç 24 saat içinde kuruma ihlali bildirmek zorundadır. İhlal türü (erişim, veri sızıntısı, hizmet kesintisi vb.) kayıt altına alınır. Etki analizi yapılır. Gerekirse KVKK veri ihlal bildirimi yapılır. Tedarikçi ile düzeltici faaliyet süreci başlatılır.

Hizmet Sonlandırma ve Erişimlerin Kapatılması: Hizmet sona erdiğinde veya tedarikçi personeli değiştiğinde: Tüm erişimler 24 saat içinde kapatılır. Verilerin iadesi, imhası veya anonimleştirilmesi sağlanır. Tedarikçi tarafındaki tüm kopyalar imha belgesiyle doğrulanır. Varsa yedekler silinir. Fiziksel anahtar, kart, cihaz teslimleri alınır.

Bulut Hizmeti Tedarikçilerinin Yönetimi, bulut hizmeti alınan tedarikçiler için: Veriler hangi ülkede saklanıyor? Şifreleme mekanizması var mı? Yedekleme nasıl yapılıyor? Erişim kayıtları tutuluyor mu? Tedarikçi SOC2 / ISO27001 belgesine sahip mi?

Soruları mutlaka değerlendirilir.

İhlaller, Bu prosedüre uyulmaması halinde: Sözleşme feshi, Tedarikçi kara listeye alınması, KVKK kapsamında idari yaptırımlar, Disiplin süreçleri uygulanabilir.

Şirketimiz ile iş ilişkisi içindeki tedarikçiler (veri işleyen) her yıl en az 1 kez bilgi güvenliği ve 6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamında ve ISO/IEC 27001-2022 BGYS Standardı bağlamında bilgilendirilir ve denetlenir. Denetim kayıtları saklanır.