ÜÇÜNCÜ TARAF BİLGİ GÜVENLİĞİ POLİTİKASI

Üçüncü taraf personele AROMSA bilgi sistemlerine erişim izni verilmeden önce bir risk değerlendirmesi yapılmalıdır. Aşağıdaki kriterler erişim izni verilmesi noktasında dikkat edilecek hususları tanımlamaktadır.

Üçüncü taraf çalışanı veya firma temsilcisi erişmek istediği bilgi işlem sistemlerini bildirir.

- Erişim şekli (fiziksel erişim, mantıksal erişim, erişimin AROMSA içinden veya dışından sağlanması gibi) Fiziksel Güvenlik Politikası (BGYS.POLTK.02) ve *Erişim Kontrol Prosedürü'nde (SÇP.28)* öngörüldüğü şekilde kararlaştırılmalıdır.
- Erişilecek bilginin hassasiyeti ve değeri Sistem /Varlık Sahibi tarafından belirlenmelidir.
- Üçüncü taraf personelin AROMSA bilgi sistemleri erişimi ile ilgili kaydedilecek denetim takibi bilgilerinin (audit log) seviyesi BT Sistem Yöneticisi ve BT İş Uygulamaları Yöneticisi tarafından belirlenmelidir.
- AROMSA harici tarafların erişimine açık olmayan bilgilerin korunması için gerekli kontroller Erişim Kontrol *Prosedürü (SÇP.28)* referans alınarak uygulanır.
- AROMSA dışındaki taraflara ilişkin hukuki ve yasal şartlar ve bunların sözleşmeden doğan yükümlülükleri dikkate alınmalıdır.

Mevcut bilgi güvenliği politika ve *prosedürlerinin* (Bilgi Güvenliği Yönetim Sistemi Politika Dökümanı- BGYS.POLTK, Erişim Kontrol *Prosedürü (SÇP.28)*, Fiziksel Güvenlik Politikası- BGYS.POLTK.02, İnsan Kaynakları Güvenliği Politikası- BGYS.POLTK.03, Ağ Güvenliği Politikası- BGYS.POLTK.06, Bilgi Değişim Politikası- BGYS.POLTK.08, Kayıt Yönetim Politikası- BGYS.POLTK.09), prosedürlerinin (Bilgi Güvenliği İhlal Olayı Yönetim Prosedürü- SÇP.29, Sürüm Güncelleme ve Yama Prosedürü- SÇP.32, Uyarlama ve Yazılım Geliştirme Prosedürü- SÇP.37) ve talimatlarının (ABAP Standartları Talimatı- KT.BG.003) korunması ve iyileştirilmesi de dâhil olmak üzere hizmet alımı ile ilgili değişiklikler söz konusu olduğunda üçüncü taraflara ilişkin riskler varlık sahibi ve Bilgi Güvenliği Yöneticisi tarafından gözden geçirilmelidir. Değişiklik talepleri hem AROMSA'dan hem de üçüncü taraflardan gelebilir.

Üçüncü taraf sözleşme değişikliklerinin yönetilmesi sürecinde dikkate alınması gerekenler aşağıdaki gibidir:

1.1 AROMSA tarafından yapılabilecek değişiklikler

- Hali hazırda sunulan hizmetlere yönelik iyileştirmeler,

- Yeni uygulama ve sistemlerin geliştirilmesi,

- Organizasyon politikaları ve prosedürleri üzerindeki değişiklikler veya güncellemeler,

- Bilgi güvenliği olaylarını çözmek ve güvenliği arttırmak adına uygulanan yeni kontroller.

1.2 Üçüncü taraf tarafından yapılabilecek değişiklikler;

- Ağlar üzerinde yapılan değişiklikler ve iyileştirmeler,

- Yeni teknolojilerin kullanılması,

- Yeni ürünlerin veya son sürümlerin kabul edilmesi,

- Yeni geliştirme araçları ve ortamları,

- Hizmet tesislerinin fiziksel mekânlarının değiştirilmesi,

- Üretici firma değişikliği.

Yapılan değişiklikler ek sözleşmelerle belirlenir.

Gizlilik maddeleri içeren sözleşme veya gizlilik anlaşmasına imza atmadan, üçüncü taraf personele hassas verilere erişim izni tanınmamalıdır. Bu sözleşme veya gizlilik anlaşmalarında ilgili politika ve prosedürlere atıf yapılır.

Eğer üçüncü taraf AROMSA ağına bir sistem bağlamayı talep ediyorsa, o zaman AROMSA güvenlik politikalarına uygun hareket etmesi şarttır. Bu konu kötü yazılımlara karşı koruma sağlanmasını ve bunun devam ettirilmesini sağlamak için gereklidir.

AROMSA bilgi sistemlerine erişim yetkisi bulunan üçüncü taraf şirketler güvenlik meseleleri ile ilgili konularda görüşülmek üzere bir irtibat kişisi sunmalıdır.

Üçüncü taraf personelin AROMSA ağı ve sistemlerine erişimi, hizmet sözleşmelerinde tanımlanan görevleri ile sınırlı olmalıdır. Üçüncü taraf personelin görevi gereği AROMSA sistemlerine / uygulamalarına erişmesi gerekiyorsa, Erişim Kontrol *Prosedürü'ne (SÇP.28)* ve diğer ilgili bilgi güvenliği politikalarına uyması zorunludur.

Etki alanında kullanıcı eklenirken üçüncü taraf çalışanları için proje veya sözleşme süresi sorgulanır. Sözleşme süresi bitiminde kullanıcı erişimi otomatik olarak engellenir. Erişim haklarının periyodik olarak gözden geçirilmesi sırasında üçüncü taraflara verilen haklar da gözden geçirilir.

Verilmiş olan bütün üçüncü taraf erişimleri periyodik olarak gözden geçirilir ve gerek kalmadığında silinir.

Üçüncü taraf hizmet ve/veya ürün alımlarında kabul muayenelerinde hizmeti alan, hizmet veya ürünün sözleşmeye aykırı durumlar içerip içermediğini değerlendirir.

Kabul muayenesinden başarı ile geçmeyen ürün veya hizmetle ilgili olarak sözleşmede yer alan hukuki süreç işletilir. Gerekli durumlarda tazminat talebinde bulunulur.

2 Üçüncü Taraf Anlaşmalarda Güvenlik Konusunun Ele Alınması

Güvenlik gereksinimlerinin yerine getirilmesi için aşağıdaki şartların anlaşmaya dâhil edilmesine dikkat edilmelidir.

2.1 AROMSA Bilgi Güvenliği Politikası'na atıfta bulunulması.

2.2 Varlıkların korunmasına yönelik kontroller.

Örneğin,

- Bilgi, yazılım ve donanım dahil olmak üzere organizasyon varlıklarının korunmasına yönelik prosedürler,

- Gerekli fiziksel güvenlik kontrolleri ve mekanizmaları,

- Kötü amaçlı yazılımlara ilişkin güvenlik kontrolleri,

- Varlıklar üzerinde herhangi bir tehlikenin mevcut olup olmadığını anlamaya yönelik prosedürler (örneğin bilginin, yazılımın ve donanımın kaybedilmesi veya değiştirilmesi),

- Anlaşma sona erdiğinde veya anlaşma henüz yürürlükteyken kararlaştırılan bir zaman diliminde bilginin iadesini veya imha edilmesini temin etmek için yürütülecek kontroller,

- Gizlilik, bütünlük, kullanılabilirlik (erişilebilirlik) ve diğer varlık özellikleri,

- Bilginin çoğaltılması ve ifşa edilmesi ile ilgili kısıtlamalar ve gizlilik anlaşmalarının kullanılması,

- Gerekli durumlarda anlaşılır bir raporlama yapısı ve kararlaştırılan raporlama formatları,

- Gerekli durumlarda anlaşılır ve belirlenmiş bir bilgi değişim yönetimi,

- Gerekirse personel transferi ile ilgili hükümler.

2.3 Gerekli durumlarda üçüncü taraf personelin AROMSA bilgi sistemlerine erişimi ile ilgili ayrıntılar sözleşmelere ek madde olarak eklenir.

- Üçüncü taraf personel, fiziksel güvenlik de dâhil olmak üzere AROMSA güvenlik politikalarına, standartlarına ve ilgili mevzuata uygun hareket etmelidir,
- Üçüncü tarafların üzerine düşen güvenlik yükümlülükleri açıkça tanımlanmış olmalıdır,
- AROMSA, üçüncü tarafların AROMSA bilgi sistemlerine erişimini izleme ve kendi takdiri doğrultusunda bu erişimi engelleme hakkına sahiptir,
- Gizliliğin, fikri mülkiyet haklarının, telif hakkının ve ortak çaba eseri çalışmalara / ürünlere ilişkin güvenliğin garanti altına alınması için gerekli gizlilik anlaşmaları mevcut olmalıdır,
- AROMSA bilgi varlıkları anlaşma feshedildikten sonra geri alınmalıdır veya imha edilmelidir,
- AROMSA bilgi varlıklarına erişim hakkı anlaşma feshedildikten sonra iptal edilmelidir.

Üçüncü taraflar, AROMSA'ya sağlanan hizmetlerle ilgili herhangi bir alt yüklenici kullanma kararı almadan önce AROMSA'ya danışmalı, onay almadan herhangi suretle alt yüklenici çalıştırmamalıdır.

Üçüncü taraflar periyodik olarak izlenir ve gözden geçirilir. Yıllık yapılan tedarikçi denetim planına bağlı olarak, hizmet alınan üçüncü taraflar, bilgi güvenliği kapsamında denetlenebilir.