3. TARAF BİLGİ GÜVENLİĞİ POLİTİKASI

Bu politikanın amacı Rakun Mobilite' nin bilgi varlıklarının ve bilgi işleme tesislerine üçüncü taraflar tarafından ulaşılması durumunda güvenliğinin sağlamaktır. Bu politikanın uygulanmasından BT Ekibi ve üst yönetim sorumludur.
Kurum çalışanı olmayıp bilgi sistemleri kaynaklarına erişim sağlayan her türlü kişi 3. Taraf olarak kabul edilir. 3. Tarafların uyması gereken kurallar ve yönetim şekli BGYS kapsamlı dokümanlarda 3. Taraf olarak ayrıca belirtilmiştir. 3. Taraf tanımına uyan her türlü kişi ya da kurumla yapılacak geçici ya da sürekli çalışma sözleşmelerin imzalanması güncel olarak takip edilir. Sözleşme imzalanmadan önce kararlaştırılmış ve onaylanmış güvenlik anlaşmaları hazırlanıp kurumlarla kurumsal gizlilik sözleşmesi 3. Taraf çalışanlarıyla bireysel gizlilik sözleşmesi yapılır. Gerektiği takdirde üçüncü taraf çalışanlarının politikaya uyması için süre tahsis edilir. Bilgi Güvenliği 3. Taraf politikasında yapılacak güncellemeler Yönetim Gözden Geçirme toplantılarında belirlenir ve BGYS Yöneticisi tarafından dokümana yansıtılır. Her güncellemede doküman Üst Yönetim tarafından onaylanır.

Rakun Mobilite bilgi işlem altyapısını kullanan ve bilgi kaynaklarına erişen 3. Taraf herkes:

Üçüncü taraf personele Rakun Mobilite bilgi sistemlerine erişim izni verilmeden önce yapılan risk değerlendirmesi dikkate alınır ve değerlendirilir. Aşağıdaki kriterler erişim izni verilmesi noktasında dikkat edilecek hususları tanımlamaktadır.

Kişisel ve elektronik iletişimde ve üçüncü taraflarla yapılan bilgi alışverişlerinde kuruma ait bilginin gizliliğini sağlamalı,
Kurum dışından gelen bakım ve tamir çalışanları, diğer tedarikçilerde de olduğu gibi, kurum içinde olduğu süre boyunca bir gizlilik anlaşması imzalamalı ve anlaşmaya uygun hareket etmekle yükümlü.
Bilgi Güvenliği Politikasını bilmek ve uymak,
BGYS kapsamında belirlenen uyulması gereken davranışlara riayet etmek,
Taahhüt ettiği Gizlilik Sözleşmelerine riayet etmek, 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.
BGYS'nin sağlıklı işlemesi için gerekli görülen önerileri ve ihlal olaylarını ilgili kişiye iletmek
Firma tarafından sağlanan bilgi işlem sistemleri ve uygulamalar iş amaçlı olarak kullanmak. İş süreçlerini engellemeyecek düzeyde ve Bilgi Güvenliği Politikası'nı ve BGYS prosedürlerini ihlal etmeyen kişisel kullanımlar kabul edilebilir kapsamda değerlendirilir.
Üçüncü taraf çalışanı veya firma temsilcisi erişmek istediği bilgi işlem sistemlerini bildirir.
• Erişim şekli (fiziksel erişim, mantıksal erişim, erişimin Rakun Mobilite içinden veya dışından sağlanması gibi) Fiziksel Güvenlik Politikası ve Erişim Kontrol Politikası'nda öngörüldüğü şekilde kararlaştırmak. Erişilecek bilginin hassasiyeti ve değeri Sistem /Varlık Sahibi tarafından belirlenmelidir.
• Üçüncü taraf personelin Rakun Mobilite bilgi sistemleri erişimi ile ilgili kaydedilecek denetim takibi bilgilerinin (audit log) seviyesi BT Sistem Yöneticisi ve BT İş Uygulamaları Yöneticisi tarafından belirlenmelidir. Rakun Mobilite harici tarafların erişimine açık olmayan bilgilerin korunması için gerekli kontroller Erişim Kontrol Politikası referans alınarak uygulanır.
• Rakun Mobilite dışındaki taraflara ilişkin hukuki ve yasal şartlar ve bunların sözleşmeden doğan yükümlülükleri dikkate alınmalıdır.
Eğer üçüncü taraf Rakun Mobilite ağına bir sistem bağlamayı talep ediyorsa, o zaman Rakun Mobilite güvenlik politikalarına uygun hareket etmesi şarttır. Bu konu kötü yazılımlara karşı koruma sağlanmasını ve bunun devam ettirilmesini sağlamak için gereklidir.
Rakun Mobilite bilgi sistemlerine erişim yetkisi bulunan üçüncü taraf şirketler güvenlik meseleleri ile ilgili konularda görüşülmek üzere bir irtibat kişisi sunmalıdır.
Üçüncü taraf personelin Rakun Mobilite ağı ve sistemlerine erişimi, hizmet sözleşmelerinde tanımlanan görevleri ile sınırlı olmalıdır. Üçüncü taraf personelin görevi gereği Rakun Mobilite sistemlerine / uygulamalarına erişmesi gerekiyorsa, Erişim Kontrol Politikası'na 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.
Başarı ile geçmeyen ürün veya hizmetle ilgili olarak sözleşmede yer alan hukuki süreç işletilir. Gerekli durumlarda tazminat talebinde bulunulur.
Rakun Mobilite Üçüncü Taraf Anlaşmalarda Güvenlik Konusunun Ele Alınması Güvenlik gereksinimlerinin yerine getirilmesi için aşağıdaki şartların anlaşmaya dâhil edilmesine dikkat edilir. (Rakun Mobilite Bilgi Güvenliği Politikası'na atıfta bulunulması. - Varlıkların korunmasına yönelik kontroller-Gerekli fiziksel güvenlik kontrolleri ve mekanizmaları- Kötü amaçlı yazılımlara ilişkin güvenlik kontrolleri - Varlıklar üzerinde herhangi bir tehlikenin mevcut olup olmadığını anlamaya yönelik prosedürler / Politikalar (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,- Gerekirse personel transferi ile ilgili hükümler.)
Gerekli durumlarda üçüncü taraf personelin Rakun Mobilite bilgi sistemlerine erişimi ile ilgili ayrıntılar sözleşmelere ek madde olarak eklenir. (Üçüncü taraf personel, fiziksel güvenlik de dâhil olmak üzere Rakun mobilite güvenlik politikalarına, standartlarına ve ilgili mevzuata uygun hareket etmelidir, - Üçüncü tarafların üzerine düşen güvenlik yükümlülükleri açıkça tanımlanmış olmalıdır, - Rakun Mobilite, üçüncü tarafların Rakun Mobilite 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, - Rakun Mobilite bilgi varlıkları anlaşma feshedildikten sonra geri alınmalıdır veya imha edilmelidir, - Rakun Mobilite bilgi varlıklarına erişim hakkı anlaşma feshedildikten sonra iptal edilmelidir.)
Üçüncü taraflar, Rakun Mobilite' ye sağlanan hizmetlerle ilgili herhangi bir alt yüklenici kullanma kararı almadan önce Rakun Mobilite' ye 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.
Rakun Mobilite Kuruluş içinde kullanılan telefon rehberleri üçüncü tarafların eline geçmemelidir.
Bu politikaya uygun olarak çalışmayan tüm personel hakkında Çalışan Disiplin İç Yönergesi hükümleri uygulanır.

Veri Sorumlusu / Veri İşleyen Sorumlulukları (KVKK ve ISO/IEC 27701 Gereği)
"Rakun Mobilite, 6698 sayılı Kişisel Verilerin Korunması Kanunu uyarınca Veri Sorumlusu olarak, üçüncü taraflarla yapılan işbirliklerinde kişisel verilerin işlenmesi durumunda, tarafların Veri Sorumlusu – Veri İşleyen ilişkisi açıkça tanımlanır.
Üçüncü taraflar, kişisel verileri yalnızca sözleşmede belirtilen amaçlarla ve Rakun Mobilite'nin yazılı talimatlarına uygun olarak işleyebilir."

Alt Yüklenici Kontrolü ISO 27001 A.5.19 / 27701 7.2.7
"Üçüncü taraflar, Rakun Mobilite'nin önceden yazılı onayı olmadan hiçbir alt yükleniciyle çalışamaz.
Onaylanan alt yükleniciler, Rakun Mobilite'nin güvenlik politikalarına ve gizlilik yükümlülüklerine tam olarak uymak zorundadır."

Bilgi İhlali Bildirimi Süresi (KVKK Madde 12 ve ISO/IEC 27701 Gereği)
"Üçüncü taraflar, bilgi güvenliği veya kişisel veri ihlali tespit ettiklerinde en geç 24 saat içinde Rakun Mobilite BGYS Sorumlusuna yazılı bildirim yapmakla yükümlüdür. Gecikmeli bildirim durumunda doğacak hukuki ve mali sorumluluklar ilgili üçüncü tarafa aittir."

Veri İmha ve İade Süreci
"Hizmet ilişkisi sona erdiğinde veya sözleşme kapsamında belirtilen sürenin dolması halinde, üçüncü taraf elindeki tüm kişisel verileri, yedekler dâhil olmak üzere imha etmek veya Rakun Mobilite'ye güvenli şekilde iade etmekle yükümlüdür. İmha veya iade işlemi, yazılı bir raporla belgelendirilir."

Üçüncü Taraf Farkındalık Eğitimi (ISO 27001 Madde 7.2 ve Ek A.6.3)
"Üçüncü taraf çalışanları, Rakun Mobilite sistemlerine erişimden önce bilgi güvenliği farkındalık eğitimi alır ve bu eğitimin tamamlandığı dokümante edilir."

Periyodik Değerlendirme / Tedarikçi Performansı (ISO/IEC 27001 A.5.19 ve A.5.20)
"Üçüncü tarafların bilgi güvenliği performansı yılda en az bir kez değerlendirilir.Denetim sonuçlarına göre uygunsuzluklar tespit edilirse düzeltici faaliyet planı hazırlanır ve izlenir."

Taşeron / Üçüncü Taraf İzleme Kayıtları (ISO 27001 A.5.22 – Tedarikçi İzleme ve Gözden Geçirme)
"Üçüncü taraf performans değerlendirmeleri, sözleşme ve BGYS gereksinimleri kapsamında izlenir, ölçülür ve kayıt altına alınır.
Gözden geçirme sonuçları, tedarikçi performans kayıtları dosyasında saklanır."

Erişim Süreçlerinin Sonlandırılması (ISO/IEC 27001 A.5.18 ve A.8.2.8.3)
"Üçüncü taraf personelin sözleşmesinin bitimi, görev değişikliği veya erişim gereksiniminin ortadan kalkması durumunda tüm erişim yetkileri derhal iptal edilir.Kullanıcı hesapları sistemden silinir ve cihazlar kurumsal varlık listesine iade edilir."

Hukuki Uyum ve Yaptırımlar (KVKK ve 27001 A.5.20)
"Üçüncü tarafların bu politika veya sözleşme hükümlerine uymaması halinde, Rakun Mobilite sözleşmeyi feshetme, tazminat talep etme ve gerekli hukuki yollara başvurma hakkını saklı tutar."

Yasal, Mevzuat ve Sözleşme Uyumu (ISO 27001 A.5.31 ve A.5.32)
"Üçüncü taraflar, bilgi güvenliğiyle ilgili tüm yasal, mevzuat ve sözleşme hükümlerine (KVKK, Fikri Mülkiyet Hakları, Elektronik Haberleşme, Siber Güvenlik vb.) uymakla yükümlüdür.
Uyumsuzluk durumunda Rakun Mobilite gerekli yasal yaptırımları uygulama hakkını saklı tutar."

Politikanın Gözden Geçirilmesi ve Onayı (ISO 27001 Madde 9.3)
"Üçüncü Taraf Bilgi Güvenliği Politikası yılda en az bir kez BGYS Yöneticisi tarafından gözden geçirilir, gerekli güncellemeler Yönetimin Gözden Geçirme toplantısında onaylanır."

Bilgi Güvenliği İhlal Yönetimi (ISO 27001 A.5.24 ve KVKK Madde 12)
"Üçüncü taraf kaynaklı bilgi güvenliği ihlali meydana geldiğinde, olay BGYS Olay Yönetimi Prosedürü'ne göre kayıt altına alınır.
Olayın etkisine göre sınıflandırma yapılır, düzeltici faaliyetler başlatılır ve sonuçlar yönetim gözden geçirmesine raporlanır."

Bilginin Sınıflandırılması ve Paylaşım Seviyesi (ISO 27001 A.5.12 – Bilgi sınıflandırma)

3. TARAF BİLGİ GÜVENLİĞİ POLİTİKASI

“Üçüncü taraflarla paylaşılacak bilgiler, Bilgi Sınıflandırma ve Etiketleme Prosedürü uyarınca sınıflandırılır.
‘Kamuya Açık’, ‘İç Kullanım’, ‘Gizli’, ‘Çok Gizli’ sınıflarından sadece gerekli olan düzeyde bilgi paylaşılır.”

Varlıkların Mülkiyeti ve İadesi (ISO 27001 A.5.9 – Varlıkların Mülkiyeti)
“Üçüncü taraflara tahsis edilen her türlü bilgi varlığı (donanım, erişim hesabı, belge, yazılım lisansı vb.) Rakun Mobilite mülkiyetindedir. Sözleşme sona erdiğinde tüm varlıklar eksiksiz iade edilir ve iade kayıtları tutulur.”

Politikanın Yayımı ve Farkındalığı (ISO 27001 Madde 7.3 – Farkındalık)
“Üçüncü Taraf Bilgi Güvenliği Politikası, ilgili taraflara elektronik ortamda erişilebilir şekilde yayımlanır.
Tüm üçüncü taraflara politika hakkında bilgilendirme yapılır ve farkındalık oluşturulması için düzenli hatırlatmalar planlanır.”

Beyan ve Taahhüt ederiz.
GENEL MÜDÜR
İsmail Hakkı SAVCI 14/07/2025 (R:00)