BİLGİ GÜVENLİĞİ POLİTİKASI

AMAÇ

Bilgi Güvenliği Politikasının amacı, Rakun Mobilite bilgi sistemlerinin ve bilgi varlıklarının gizlilik, bütünlük ve erişilebilirliğinin sağlanması amacıyla gerekli gereksinimlerini tanımlamaktır. Şirket Bilgi Güvenliği Politikası, tüm çalışanlara, tedarikçilere, iş ortaklarına ve paydaşlara Şirket'in bilgi güvenliği ihtiyacını, kapsamını, amaçlarını, hedeflerini, ilkelerini ve esaslarını ve bilgi güvenliği ile ilgili rol ve sorumlulukları bildirmek amacıyla hazırlanmıştır.

KAPSAM

Bu politika, Şirket bünyesindeki veri ve bilgilerin; bilgi güvenliğinin kapsamını, hedeflerini, ilkelerini, yönetim desteğini, risk yönetimi çerçevesini, sürekliliğini, görev ve sorumlulukları, uyum gereksinimlerini ve ihlali durumunda uygulanacak yaptırımları kapsamaktadır.

Şirket, tabi olduğu ulusal, uluslararası ve sektörel düzenlemeler doğrultusunda; bilgi güvenliğini sağlamak, ilgili mevzuat ve standartlara uygunluğu sürdürmek ve kurumsal sorumluluklarını yerine getirmek amacıyla, bu politika kapsamında uygulanacak mevzuatlar arasında; 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK), ISO/IEC 27001:2022 ve ISO/IEC 27701:2019 standartları" konuyla ilgili Kişisel Verilerin Korunması Kanunu diğer düzenlemeler dikkate alınarak hazırlanmıştır. Rakun Mobilite özellikle aşağıda belirtilen konuların yerine getirilmesini benimsemiştir:

- Bilgi Güvenliği ile ilgili tüm yasal mevzuata uyum sağlamayı, Bilgi Güvenliği Standartlarının gerekliliklerini yerine getirmeyi,
- Bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlayacak altyapı ve kontrolleri uygulamayı,
- Bilgi Güvenliği Yönetim Sistemi'nin yaşatılması için gerekli kaynakları sağlamayı, kontrolleri tesis etmeyi, sürekli iyileştirme fırsatlarını değerlendirmeyi ve gözetim için gerekli çalışmaları gerçekleştirmeyi,
- Bilgi güvenliği farkındalığını artırmak için, teknik ve davranışsal yetkinlikleri geliştirecek şekilde eğitimler gerçekleştirmeyi, çalışanların bilgi güvenliği farkındalığını artırarak kurum kültürüne entegre etmeyi,
- Kişisel verilerin mahremiyetini koruyacak teknik ve idari tedbirleri almayı,
- Görevler ayrılığı prensibi çerçevesinde yetkilendirme ve onay mekanizmaları kurmayı,
- "Bilmesi gereken" ve "en az yetki" prensiplerine uygun erişim kontrolünü uygulamayı,
- Dış tehditlere karşı ağ güvenliğini sağlamayı,
- Geliştirme, test ve üretim ortamlarını fiziksel ve mantıksal olarak ayırmayı,
- Katmanlı güvenlik mimarisi kurarak ve sürekliliğini sağlamayı,
- Hizmetlerin doğrulanabilirliğini teknik yöntemlerle garanti altına almayı,
- Şifreleme anahtarlarının güvenliğini temin etmeyi,
- Mobil cihazlarda hassas verilerin güvenliğini sağlamayı,
- Bilgi güvenliği risklerini periyodik olarak değerlendirmeyi ve aksiyon planları oluşturmayı,
- Bilgi güvenliği faaliyetlerini entegre bir yapıda yönetmek üzere organizasyon kurmayı,
- Bilgi varlıklarını tanımlamayı, sahipliklerini belirleyip ve risklerini yönetmeyi,
- Bilgi güvenliği olaylarını tespit etmeyi, raporlar ve tekrarını önleyici tedbirler almayı,
- Fiziksel ve çevresel güvenlik önlemleriyle bilgiye erişimi kontrol altına almayı,
- Sistemlerin edinim, geliştirme ve bakım süreçlerine güvenlik gerekliliklerini dahil etmeyi,
- İş sürekliliği planları ile bilgiye kesintisiz erişimi güvence altına almayı,
- Güncel teknolojileri takip ederek güvenlik kontrollerini sürekli iyileştirmeyi,
- İç ve dış denetimlerle BGYS'nin etkinliğini izlemeyi, değerlendirmeyi ve geliştirmeyi.

Rakun Mobilite, Bilgi Güvenliği Yönetim Sistemi süreçlerinin işletilmesi ve sürekliliğinin sağlanması için gereken kontrollerin tesis edilmesini ve gözetimini bu politikaya bağlı alt politikalar, prosedürler ve talimatlar vasıtasıyla sağlayarak, Bilgi Güvenliği Politikaları ister tam zamanlı, ister yarı zamanlı, daimi ya da sözleşmeli olsun, tüm bilgileri veya iş sistemlerini kullanan tüm personel için, coğrafi konumdan veya iş biriminden bağımsız olarak geçerli ve zorunludur.

Bu sınıflandırmalara girmeyen ve Rakun Mobilite bilgilerine erişim gereği olan üçüncü şahıs hizmet sağlayıcıları ve bunların bağlı destek personeli gibi tüm kişilerin, bu politikanın genel ilkelerine ve uymak zorunda oldukları diğer güvenlik sorumluluklarına ve yükümlülüklerine bağlı kalması şarttır.

BİLGİ GÜVENLİĞİ HEDEFLERİ VE AMAÇLARI

Rakun Mobilite Bilgi Güvenliği, Rakun Mobilite'nin itibarının, güvenilirliğinin, bilgi varlıklarının korunması, temel ve destekleyici iş faaliyetlerinin mümkün olan en az kesinti ile devam etmesi amacıyla,

- Bilgi sistemlerinin sürekliliğini tam olarak sağlamayı,
- Çalışanların bilinç, farkındalık ve güvenlik gereksinimlerine uyum düzeylerini en üst seviyeye çıkarmayı,
- Üçüncü taraflar ile yapılan sözleşmelere uygunluğun tam olarak tesis edilmesini sağlamayı,
- Bilgi güvenliği ihlal olaylarını en aza indirmeyi ve bunları öğrenme fırsatına çevirmeyi,
- Bilginin yasalara tam uyumlu üretilmesini, erişim sağlanmasını ve saklanmasını,
- En güncel ve etkin teknik güvenlik kontrolleri uygulamayı hedefler. Tüm çalışanlar bu hedeflere katkı sağlamaktan sorumludur.

"Bilgi güvenliği hedefleri ve performans göstergeleri yıllık olarak gözden geçirilecek, olay sayısı, farkındalık oranı ve risk azaltma başarıları gibi ölçümlerle sürekli iyileştirme sağlanacaktır." Bilgi Güvenliği Politikası, şirket çalışanlarına, tedarikçilerine, temsilcilerine, iş ortaklarına ve paydaşlarına şirketin güvenlik gereksinimlerine uygun şekilde hareket etmesi konusunda yol göstermek, bilinç ve farkındalık

seviyelerini artırmak ve bu şekilde şirkette oluşabilecek riskleri minimuma indirmek, şirketin güvenilirliğini ve imajını korumak, üçüncü taraflarla yapılan sözleşmelerde belirlenmiş uygunluğu sağlamak, teknik güvenlik kontrollerini uygulamak, şirketin temel ve destekleyici iş faaliyetlerinin minimum kesinti ile devam etmesini sağlamak amacıyla şirketin tüm işleyişini etkileyen fiziksel ve elektronik bilgi varlıklarını iç ve dış kasıtlı veya kasıtsız tehditlere karşı korumayı hedefler.

BİLGİ GÜVENLİĞİ ORGANİZASYONU Şirket yönetimi bilgi güvenliği organizasyonunu şirket bünyesinde oluşturur. Bu kapsamda şirkette güvenlik politikalarının bütünsel bir yaklaşım oluşturulması, sürdürülmesi ve yönetilmesine ilişkin çalışmalar Bilgi Güvenliği Yönetim Süreci kapsamında yürütülür. Şirketin güvenlik kontrol süreçlerini koordine edecek, yönetecek rol ve sorumluluklar Görev Tanımları kapsamında belirlenir. "Bilgi Güvenliği Yönetim Sistemi'nin uygulanması, sürdürülmesi ve sürekli iyileştirilmesinden BGYS Sorumlusu (Lideri) yetkili ve sorumludur. Tüm bölüm yöneticileri, kendi sorumluluk alanlarında bilgi güvenliği gerekliliklerine uyumdan sorumludur. Çalışanlar, bilgi güvenliği politikalarına ve prosedürlerine uymakla yükümlüdür."

"Çalışanlar, görevi sırasında öğrendikleri gizli bilgileri üçüncü kişilerle paylaşamaz. Rakun Mobilite'nin fikri mülkiyet haklarını korumak tüm personelin sorumluluğundadır."

Bilgi Güvenliği Yönetim Sistemi kategorisinde yayınlanmış tüm politika ve prosedürlere uymakla, gerçekleşmiş ya da olası güvenlik ihlallerini ve zafiyetlerini bildirmek ve Bilgi Güvenliği Ekibi tarafından talep edilen tüm faaliyetleri gerçekleştirmekle yükümlüdür. Bilgi Güvenliği'nin ve bu politikanın amacı, bilgilerin ve tüm destek iş sistemlerinin, süreçlerinin ve uygulamalarının gizliliğini, bütünlüğünü ve kullanılabilirliğini korumak, sürdürmek ve yönetmektir. Bunun anlamı; bilgilerin yetkili ellerde kalması; bilgilerin eksiksiz, doğru ve kullanılabilir durumda olmasının sağlanması; ve bilgilerin, sistemlerin gerektiğinde kullanıma hazır olmasının sağlanmasıdır.

Bu nedenle tüm Rakun Mobilite ve dış kaynaklı personeller ile stajyerleri, bayi kullanıcıları ve yansanayi personeli konumları veya görevleri ne olursa olsun işlerini, bilgilerin Rakun Mobilite bünyesinde korunmasını gözetecek biçimde yapmaktan sorumludur. Bu bağlamda Varlık ve Süreç Sahipleri;

- Kendilerine duyurulan Bilgi Güvenliği Politikasına ve prosedürlerine uymak.
- Kendi süreç ve sistemlerinin yönetimleri için oluşturacakları süreç, akış, talimat, kılavuz, form gibi dokümanlarda Bilgi Güvenliği dokümanlarına uyumu sağlamak.
- Bilgi Güvenliği politikalarına ve/veya prosedürlerine uyumun sağlanmadığı veya bilgi güvenliği ihlal olaylarında **BilgiGuvenligi@rakunmobilite.com** adresine bildirmek
- Bilgi sistemlerinin çalışmasını olumsuz etkileyebilecek veya bilgi güvenliğini tehlikeye atacak faaliyetlerde bulunmamak.
- Bilgi Güvenliği dokümanları ile ilgili güncelleme/iyileştirme taleplerini Bilgi Güvenliği Yöneticine bildirmek.
- Bilgi ve kurumsal kaynaklarına iş ihtiyaçları ölçüsünde erişim talebinde bulunmak.
- Sahibi olunan varlığın ve Kişisel Verilerin, erişim haklarını ve kimlerin yönetici ve kullanıcı bazında hangi ayrıcalıkla erişilebileceğini tayin etmek.
- Varlık envanterini gözlemlemek ve güncelliğini sağlamak,
- Sahibi oldukları varlıkların Kişisel Verileri dahil olmak üzere sınıflandırmasını, güncellenmesini ve gözden geçirilmesini sağlamaktan sorumludur. Rakun Mobilite personeli, Rakun Mobilite Çalışan Disiplin İç Yönergesi Kurallarında belirtilen gizli bilgilerin korunması ve Rakun Mobilite Global İş Etiği İlkelerine de uymak zorundadır. Rakun Mobilite; Kişisel Verilerin Korunması Yasasında belirtilen önlemleri almayı ve Rakun Mobilite Kişisel Verilerin Korunması Politikasına tam uyumlu çalışmayı taahhüt eder.
- "Bilgi güvenliği ile ilgili olarak tüm çalışanlar, yöneticiler ve paydaşlar düzenli olarak bilgilendirilecek, farkındalık eğitimleri ve bilgilendirme toplantıları ile güvenlik kültürü güçlendirilecektir."

RİSK YÖNETİM ÇERÇEVESİ: Şirketin bilgi güvenliğine ilişkin risk değerlendirme yaklaşımı Bilgi Güvenliği Yönetim Sistem Sorumlusu (Lideri) tarafından belirlenir ve Bilgi Güvenliği Yönetim Süreci kapsamında tanımlanır. Bilgi güvenliği risk değerlendirme yaklaşımı ile şirketin bilgi güvenliği risklerinin hangi yöntemler ile belirleneceği, risk seviyelerinin nasıl hesaplanacağı ve risklerin nasıl değerlendirileceği belirlenir. Bilgi varlıklarıyla ilgili oluşabilecek risklerin tanımlanması, derecelendirilmesi, işlenmesi ve gözden geçirilmesi çalışmaları belirlenen risk değerlendirme yaklaşımına uygun olarak gerçekleştirilir. Risk değerlendirme çalışması sonucunda, riskleri azaltmaya yönelik aksiyonları da içeren "Bilgi Sistemleri Risk Değerlendirme Raporu" oluşturulur.

"Bilgi güvenliği yönetim sisteminin etkinliğini sağlamak amacıyla iç ve dış denetimler düzenli olarak yapılacak, denetim bulguları doğrultusunda düzeltici ve iyileştirici faaliyetler uygulanacaktır. BGYS'nin performansı yönetim tarafından izlenecek ve raporlanacaktır."

"Bilgi güvenliği ihlalleri ve kişisel veri sızıntıları zamanında tespit edilecek, kaydedilecek ve KVKK ile ISO/IEC 27701'e uygun olarak gerekli bildirimler yapılacaktır."

"Fiziksel güvenlik, veri merkezleri ve ofis alanlarında kontrollü erişim, izleme ve çevresel risklerin (yangın, su baskını, enerji kesintisi vb.) yönetimi ile sağlanacaktır."

"İş sürekliliği ve felaket senaryoları planlanacak, düzenli tatbikatlarla test edilecek ve BGYS kapsamında kritik varlıkların korunması sağlanacaktır."

ÜÇÜNCÜ PARTİLER

Rakun Mobilite'ye mal ve hizmet sağlayan üçüncü kişilerin ve bunların çalışanlarının uyması gereken bilgi güvenliğine ilişkin düzenlemeler ilgili sözleşmeler ve güvenlik protokolleri ile belirlenir. Bunlar asgari aşağıdaki hususları kapsar:

- Sözleşmeler veya protokoller ile bildirilen bilgi güvenliği kuralları başta olmak üzere üçüncü taraflarla ilişkileri düzenleyen Rakun Mobilite Politika ve Prosedürleri'ne uygun hareket etmek.
- Rakun Mobilite'ye ait bilgi ve varlıkları Rakun Mobilite onayı ve izni olmadan başkaları ile paylaşmamak.
- Rakun Mobilite tarafından kendilerine verilen kimlikleri mukavelelere ve talimatlara uygun şekilde kullanmak

• Üçüncü partinin Rakun Mobilite'yle çalışmakta olan çalışanlarının kendi firmasından ayrılması/görev değiştirmesi söz konusu ise, bu durumu aynı gün içerisinde Rakun Mobilite'ye bildirmek ve yetkilerinin iptal edilmesini sağlamak.
• Rakun Mobilite'nin onay ve izni olmadan, Rakun Mobilite'nin cihazınlarındaki hiçbir veri ve yazılımı kopyalamamak, ortamın ses kaydınını almamak, resmini, videosunu çekmemek, veri güvenliğini veya imajını tehlikeye atabilecek paylaşımlarda/hareketlerde bulunmamak. Rakun Mobilite lokasyonlarında yapılacak sistem erişimlerini Bilgi Teknolojileri ekiplerinin gerçekleştirmek. "Tedarikçiler, iş ortakları ve üçüncü taraf hizmet sağlayıcılarının bilgi güvenliği ve kişisel veri koruma gerekliliklerine uygunluğu sözleşmeler ve denetimlerle sağlanacaktır."

POLİTİKANIN İHLALİ VE YAPTIRIMLAR- (**Denetleme ve Politikalara Uyulması ve Uyulmama Durumlarının Çözümlenmesi/ Politika Sahipliği ve Bilgi Güvenliğinde Rehberlik Sağlanması)**
"Bu politika ve bağlı prosedürlere uyulmaması-ihlali halinde, uygunsuzlukların niteliğine göre uyarma, kınama, yasal otoriterelere bildirim ve sözleşme feshi yaptırımlarından biri ya da birden fazlası ilgili Çalışan /Disiplin iç yönergesi uygulanır. Bilgi güvenliği ihlalleri, gerekirse yasal mercilere bildirilebilir.
Her birim yöneticisi Bilgi Güvenliği Politikasına uyumun sağlanması için gerekli tedbirleri almak ve sistemi gözetlemekten birinci derecede sorumludur. BT Güvenlik Yöneticiliği başta Bilgi Güvenliği Politikası olmak üzere yayınlanmış olan tüm politika ve prosedürler ile ilgili standartlara uyumun periyodik olarak denetiminden ve ilgililere raporlanmasından sorumludur.
Bilgi Güvenliği Politikası ihlalleri, Rakun Mobilitenin risklere karşı ihtiyaç duyulan kontrollerin uygulanmaması neticesinde zarar görmesine, ayrıca yeni Türk Ceza Kanuna göre de cezai sorumluluk doğurmasına ve maddi zararların tazmini sorumluluğuna sebep olabilecektir. Dolayısıyla söz konusu ihlal aynı zamanda Rakun Mobilite Çalışan Disiplin İç Yönergesi ihlali olup disiplin cezası sonucunu doğurabilir. Gerek gözetim, gerek denetim gerekse ihbar sonucu tespit edilen Bilgi Güvenliği Politikası ihlalleri şirket içi disiplin cezalarının uygulanması, istihdama son verilmesi hatta Adli ve Cezai yasal işlemler başlatılması sonuçlanabilecektir. Bu politikanın uygulanması konusunda hep birlikte çalışılması, bilgilerimizin ve itibarımızın sürekli olarak korunmasına ve işimizin başarısının devamlılığının sağlanmasına yardımcı olacaktır.
Bu politikanın ve tüm standartların ve diğer destekleyici belgelerin ve eğitim faaliyetlerinin işlevsel sahipliği BT Güvenlik Yöneticiliği tarafından yürütülecek ve bu yöneticilik, aynı zamanda politikanın tüm Rakun Mobilite bünyesinde uygulanmasıyla ilgili olarak tavsiye kaynağı ve rehber olacaktır.
BT Güvenlik Yöneticiliği tüm çalışanların, Bilgi Güvenliği konularıyla ilgili uygun bilinçlenme düzeyinin oluşmasını sağlayacak uygun eğitimleri almalarını temin edecek ve genel olarak bilgi güvenliği olaylarının ele alınmasında rehberlik edecektir. Gerekli olduğunda bu politikanın ayrıntılı standartlar, prosedürler ve süreçlerle desteklenmesini ve bunların gerek doğdukça kullanıma hazır olmasını sağlayacaktır. Ayrıca bu politika gereklerinin tüm çalışanlara (daimi veya dönemsel) ve tüm yüklenici personeline aktarılmasını sağlamaktan sorumlu olacaktır.
Üst Yönetim, Bilgi Güvenliği ile ilgili genel yönetim çerçevesinin oluşturulmasından, sürekliliğinin sağlanmasından, bu politikanın, güncel olarak yaşamasını ve Rakun Mobilite ve iştiraklerinin işle ilgili gerekliliklerini veya bilgilerinin ve bilgi sistemlerinin karşı karşıya olduğu risk ortamındaki ya da tehditlerdeki değişimleri yansıtmaya devam etmesini temin edecek şekilde devamlı gözden geçirilmesinden sorumlu olacaktır.
Bilgi Güvenliği politikaları Rakun Mobilite bilgi varlıklarının karşı karşıya olduğu güncel riskleri yansıtması amacıyla yapılan varlık ve risk güncellemelerine paralel olarak **yılda en az bir defa** gözden geçirilirler. Yeni riskleri ve risklerde meydana gelen değişiklikleri kontrol altında tutmak için Bilgi Güvenliği Politikaları gerekli eklemeler yapılarak güncellenir. Ayrıca herhangi bir Rakun Mobilite çalışanı Bilgi Güvenliği Politikaların gelişmesi ve Rakun Mobilite'nin ihtiyaç duyduğu kontrolleri daha iyi yansıtması amacıyla politikaların değiştirilmesi konusunda BT Güvenlik Yöneticiliğine talepte bulunabilir. Yapılan talepler BT Güvenlik Yöneticiliği tarafından ele alınır ve değerlendirilir.
GÖZDEN GEÇİRME, YAYINLAMA VE DENETİM, RAPORLAMA Yönetmeliklerde veya bilgi güvenliği uygulama süreçlerindeki değişiklikler politikanın gözden geçirilmesini gerektirir. "Politikanın gözden geçirilmesinden BGYS Sorumlusu sorumludur.
Gözden geçirme sonuçları Yönetimin Gözden Geçirme (YGG) toplantılarında ele alınır.
" Bilgi Güvenliği Politikası yılda en az bir kez üst yönetim tarafından gözden geçirilecek, güncel gereksinimler ve teknolojik gelişmeler doğrultusunda revize edilecektir. "Gözden geçirilen ve güncellenen politika Genel Müdür tarafından onaylanır. Onaylanan politika kurumun tüm çalışanlarının eriştiği ortak dosya sunucusu üzerinde yer alan "BGYS" klasöründe yayınlanır.
"Bu politika, yürürlüğe alındığı tarih itibarıyla elektronik ortamda intranet üzerinden erişilebilir olacak şekilde tüm Rakun Mobilite çalışanlarına, taşeronlarına ve iş ortaklarına duyurulmuştur. Politikanın kontrolü, dağıtımı ve güncelliğinin sağlanmasından BGYS Sorumlusu/Lideri sorumludur."Bu prosedür, güvenlik anlayışı ile hizmet sunulması faaliyetleri kapsamında Bilgi Güvenliği Yönetim Sistemleri sorumluğunda yılda en az (1) bir defa denetlenir.

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