

Bilgi Güvenliđi Politikası

Trugo olarak,

Türkiye çapında tüm elektrikli araç kullanıcılarına dilediđi yere seyahat etme özgürlüğü sunmak ve kullanıcı odaklı akıllı enerji sistemleriyle kullanıcılarının şarj deneyimlerini benzersiz kılmak hedefiyle çıktığımız yolda sistemlerin sürekli geliştirilerek uygulanması ile sağlanacağına inanıyoruz.

Trugo'ya ait teknolojiyi, bilgi birikimini ve şirket itibarını koruyabilmek ve ayrıca iş faaliyetlerimizi sürdürebilmek açısından bilgi güvenliđi bizim için hem stratejik hem de operasyonel olarak kritik derecede önem taşıyor. Şirketimize ait veya şirketimiz tarafından kullanılan bilgi varlıkları iş faaliyetlerimizin, ürün ve hizmetlerimizin oluşturulması ve iyileştirilmesi için gerekli temel bir unsurdur. Bu bağlamda şirketimizde yasal uyumluluklar çerçevesinde 'gerektiđi kadar bilme' prensibine uygun bir biçimde erişim kontrolleri verilir ve gelişen teknolojiye uygun güvenlik önlemleri alınır. Bilgi güvenliđi tehditleri göz önünde bulundurularak kuruluş bilgi varlıkları ve hizmetleri açısından riskler ve önlemler arasında uygun bir denge sağlayan Bilgi Güvenliđi Yönetimi Sistemi uygulanır.

Bilgi Güvenliđi Politikası İlkeleri

Bu Politika; ilgili düzenlemeler uyarınca Trugo için belirlenen görev ve sorumlulukların kesintisiz sürdürülmesini, Trugo'nun stratejik planlarının desteklenmesini, vizyon ve misyon hedeflerine ulaşılması ile Trugo'nun, çalışanların, müşterilerin ve iş ortaklarının bilgilerinin korunması amacıyla iş süreçlerinin BGYS çerçevesinde yürütülmesinin sağlanmasını amaçlar.

- Trugo bilgi güvenliđinin uluslararası standartlarda yönetilmesi ve sağlanmasında, ISO/IEC 27001 Bilgi Güvenliđi Yönetim Sistemi çerçevesindeki bilgi güvenliđi prensipleri ile KVKK (Kişisel Verilerin Korunması Kanunu ve GDPR (General Data Protection Regulation) başta olmak üzere ilgili otoriteler tarafından çıkarılan yasal düzenlemelere uyum sağlanır.
- Trugo mülkiyetinde olan her türlü bilgi veya bilgi varlığını hedef alan bilgi güvenliđi tehditlerine karşı gerekli tespit ve engelleme yöntemleri ve mekanizmaları hayata geçirilir. Söz konusu yöntem ve mekanizmaların güncel tehditlere karşı etkin koruma sağlamasını teminen gerekli güncelleme faaliyetleri yürütülür. Bu kapsamda gerekli yatırım, proje ve insan kaynağı ihtiyaçları planlanarak hayata geçirilir.
- BGYS'nin yürütülmesinde ISO 27001 standardına uygun risk yönetimi yaklaşımı uygulanır. Risk yönetimi yaklaşımında Trugo bilgi ve bilgi varlıkları, bu varlıkların gizlilik, bütünlük ve erişilebilirlik kayıpları ve bu kayıpların Trugo'ya etkisi dikkate alınır. Bilgi

varlıklarının taşıdığı bilgi güvenliği risklerinin tamamen yok edilmesinin mümkün olmadığı ve her durumda “artık risk” olacağı bilinci ile mevcut risklerin yönetilmesi, söz konusu artık riski asgariye düşürecek düzeltici ve önleyici tedbirlerin etkin şekilde uygulanması esastır.

- Trugo bünyesinde üretilen, işlenen, saklanan veya üçüncü taraflar tarafından iletilen her türlü bilgi Trugo tarafından korunur. Bilgi varlıklarının hassasiyetinin gerektirdiği şekilde korunması amacıyla uyulması gereken hususlar ilgili bilgi güvenliği mevzuatında belirlenir.
- Bilgi güvenliği kapsamında yürütülen faaliyetlerin hedeflenen başarıya ulaşabilmesi için çalışanların konuya bilinçli yaklaşımı ve sorumluluk alanlarına düşen görevleri yerine getirmesi esastır.
- Bilgi güvenliği konusunda bilinçli hareket etmek, bilginin güvenliğine ilişkin alınacak tedbirlerin uygulanmasına yardımcı olmak, şüpheli durumlar ile ilgili bildirimde bulunmak, BGYS kapsamında ihtiyaç duyulan iş sürekliliği faaliyetlerine destek vermek çalışanların rol ve sorumluluklarının ayrılmaz parçasıdır.
- Trugo çalışanlarının bilgi güvenliği farkındalığını arttırmak amacıyla yılda en az 1 (bir) defa olmak üzere “Bilgi Güvenliği Farkındalık Eğitimi” düzenlenir ve yıl içerisinde çeşitli farkındalık çalışmaları (duyurular, bültenler, afişler, farkındalık değerlendirmeleri vd.) ile çalışanlar desteklenir.
- BGYS faaliyetlerinin periyodik olarak üçüncü taraflarca denetlenmesi esastır. Denetim değerlendirmeleri kapsamında gerekli görülecek gözden geçirme ve değerlendirme aksiyonları BGYS Ekibi’nin belirleyeceği çerçevede gerçekleştirilir. Bilgi güvenliği faaliyetlerine ilişkin olarak gerek kurum içi gerekse kurum dışı taraflarca gerçekleştirilen her türlü denetim sonucu Üst Yönetim ile paylaşılır.
- Trugo bilgi varlıklarının iç ve dış tehditler karşısındaki güncel durumunun tespiti amacıyla konusunda uzman bir üçüncü tarafa yılda en az 1 (bir) kez sızma testi yaptırılır, sonuçları ve belirlenen aksiyon planları Üst Yönetim’e raporlanır. Üst Yönetim tarafından onaylanan aksiyon planında yer alan önlemlerin takibi gerçekleştirilir.
- Üçüncü taraflarla yapılacak çalışmalarda üçüncü taraflar, Trugo tarafından hazırlanan gizlilik taahhütnamesinde belirtilen hususları içerecek şekilde Trugo bilgi güvenliği kuralları ve prensipleri konusunda bilgilendirilir.
- Trugo mülkiyetinde olan bilgi veya bilgi varlıklarının bulunduğu fiziksel mekânlara erişimler, çalışanların rol ve sorumluluklarıyla uyumlu şekilde sınırlandırılır. Söz konusu sınırlandırma yöntemlerinde kullanılacak doğrulama ve yetkilendirme yöntem ve mekanizmalarının belirlenmesi, güncellenmesi ve denetim amaçlı iz kayıtlarının güvenli olarak saklanması amacıyla gerekli altyapılar tesis edilir.
- Trugo mülkiyetinde olan bilgi veya bilgi varlıklarını hedef alan tüm bilgi güvenliği olayları bilgi güvenliği olay yönetimi kapsamında değerlendirilir. Yapılan

değerlendirmeler neticesinde, mevcut kontrollerin güncellenmesi veya yeni kontrollerin devreye alınması faaliyetleri en kısa zamanda gerçekleştirilir.

- Çalışanlar, bilgi varlıkları üzerinde kendilerine tahsis edilen çalışan hesap bilgilerini korumakla yükümlü olup hesap bilgilerini üçüncü taraflarla paylaşamazlar. Çalışanlar, kendilerine tahsis edilen kullanıcı hesapları ile yapılan işlemlerden sorumludur.

Bu politika doğrultusunda; Bilgi Güvenliği Yönetim Sistemimizin etkinliğini değerlendirerek sürekli iyileştireceğimizi ve bu bakış açımızın tüm ilgili taraflara duyurulmasını sağlayacağımızı taahhüt ederiz.

Bu politikanın kapsamında yukarıda belirtilen taahhütleri gerçekleştirmek amacıyla gerekli eylem planlarının uygulanmasını ve ihtiyaç duyulan tüm bilgi ve kaynakları sağlayarak kararlılıkla takip edilmesini taahhüt ediyoruz.

İbrahim Halil KARACA

Head of Trugo

