Fikri mülkiyet haklarına Türkiye'nin sahip olduğu, küresel ölçekte rekabet edecek bir otomobil markası yaratma hedefiyle çıktığımız yolda elektrikli ve bağlantılı yeni nesil otomobiller geliştiriyor ve bu otomobiller etrafında bir mobilite ekosistemi oluşturuyoruz. Bu ekosistem sayesinde geniş kitlelerin hayatını kolaylaştırıp, zararlı emisyonları sıfırlayarak temiz bir geleceğe katkıda bulunmayı hedefliyoruz.

Togg'a ait teknolojiyi, bilgi birikimini ve şirket itibarını koruyabilmek ve ayrıca iş faaliyetlerimizi sürdürebilmek açısından bilgi güvenliği 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 'gerektiği kadar bilme' prensibine uygun bir biçimde erişim kontrolleri verilir ve gelişen teknolojiye uygun güvenlik önlemleri alınır. Bilgi güvenliği tehditleri göz önünde bulundurularak kuruluş bilgi varlıkları ve hizmetleri açısından riskler ve önlemler arasında uygun bir denge sağlayan Bilgi Güvenliği Yönetimi Sistemi uygulanır.

Bilgi Güvenliği Politikası İlkeleri

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

- Togg bilgi güvenliğinin uluslararası standartlarda yönetilmesi ve sağlanmasında, ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi çerçevesindeki bilgi güvenliği prensipleri ile KVKK (Kişisel Verilerin Korunması Kanunu), GDPR (General Data Protection Regulation) ve Payment Card Industry (PCI) Veri Güvenliği Standartları başta olmak üzere ilgili otoriteler tarafından çıkarılan yasal düzenlemelere uyum sağlanır.
- Togg mülkiyetinde olan her türlü bilgi veya bilgi varlığını hedef alan bilgi güvenliği 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 Togg bilgi ve bilgi varlıkları, bu varlıkların gizlilik, bütünlük ve erişilebilirlik kayıpları ve bu kayıpların Togg'a etkisi dikkate alınır. Bilgi ve 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.
- Togg bünyesinde üretilen, işlenen, saklanan veya üçüncü taraflar tarafından iletilen her türlü bilgi Togg 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.
- Togg 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 Kokpit ile paylaşılır.
- Togg 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 Kokpit'e raporlanır. Kokpit tarafından onaylanan aksiyon planında yer alan önlemlerin takibi gerçekleştirilir.
- Üçüncü taraflarla yapılacak çalışmalarda üçüncü taraflar, Togg tarafından hazırlanan gizlilik taahhütnamesinde belirtilen hususları içerecek şekilde Togg bilgi güvenliği kuralları ve prensipleri konusunda bilgilendirilir.
- Togg 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.
- Togg 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.