BİLGİ GÜVENLİĞİ POLİTİKASI

AMAÇ

Bu politikanın amacı, Otokoç Otomotiv'in sahip olduğu Bilgi Sistemleri ile bu sistemlerde işlenen verilerin gizliliğini, belirlenen standartlara uygun şekilde korumaktadır. Otokoç Otomotiv'e ait tüm veri ve bilgilere yalnızca yetkili kişilerin, yetki seviyeleri doğrultusunda erişmesini sağlamak ve kamuya açıklanması durumunda şirket çıkarlarını zedeleyebilecek bilgilerin asgari standartlarda korunmasına yönelik güvenlik politikaları ile ilgili standartları tanımlamaktadır.

Bu doküman, organizasyon içindeki bilgiyi kullanan, bilgi güvenliğini sağlayan ve bilginin sürekliliğini temin eden kişilerin kullanımı için bilgi güvenliği yönetimi ile ilgili politika ve standartları kapsamaktadır. Bu doküman; organizasyon içindeki güvenlik standartları ve etkili güvenlik yönetimi uygulamaları geliştirmek amacıyla yaygın bir temel oluşturmak ve iş ilişkilerinde güven sağlama amacı taşımaktadır.

KAPSAM

Bu politika, kurumdaki tüm çalışanları, üçüncü taraf olarak bilgi sistemlerine erişen kullanıcıları, bilgi sistemlerine destek sağlamakta olan hizmet, yazılım veya donanım sağlayıcılarını ve ziyaretçileri kapsamaktadır.

UYGULAMA

- Otokoç Otomotiv (Kurum); amaçları, değerleri ve stratejik hedefleri doğrultusunda bilgi güvenliğine birinci derecede önem vermektedir.
- Kurum yönetimi;
  - Kurumun güvenilirliğini ve imajını korumayı,
  - Yapılan sözleşmelerin, bilgi güvenliği gerekliliklerini yerine getirdiğinden emin olmayı ve kurumun temel destekleyici faaliyetlerinin en az kesinti ile devam etmesini sağlamayı hedeflemektedir.
- Kurum, bu kapsamda bilgi varlıklarının gizliliğini, bütünlüğünü, erişilebilirliğini sağlamak ve korumak için gerekli tedbirleri almayı taahhüt etmektedir.
- Bilgi güvenliği risklerinin tanımlanması, değerlendirilmesi ve işlenmesi, kurumun risk yönetimi kapsamında ele alınmaktadır. Siber Güvenlik ve Bilgi Güvenliği Risklerinin yönetiminden Siber Güvenlik personeli sorumludur.
- Kuruma ait bilgi teknolojileri altyapısını kullanan ve bilgi kaynaklarına erişen herkes:
  - Kişisel veya elektronik iletişimde, üçüncü taraflarla yapılan bilgi alışverişlerinde kuruma ait bilginin gizliliğini sağlamalı,
  - Kritiklik düzeylerine göre işlediği bilgiyi yedeklemeli,
  - Risk düzeylerine göre belirlenen güvenlik önlemlerini almalı,
  - Bilgi güvenliği ihlalleri hakkında bilgi sahibi olmalı, ihlal olacak davranışlarda bulunmamalı ve gözlemledikleri bilgi güvenliği ihlal olaylarını kurumun belirlediği ve duyurduğu kanallar üzerinden raporlamalı,
  - Kurum içi bilgi kaynaklarını yetkisiz kişilerle paylaşmamalı,
  - T.C. yasalarına ve yönetmeliklerine aykırı faaliyetler amacıyla kullanmamalıdır.
- Kurumun çalışanları, üçüncü taraf, tedarikçi vb. tüm paydaşlar, bu politikaya ve bu politikanın uygulanmasını sağlayan diğer politika, prosedür ve talimatlara uymakla yükümlüdür.
- Siber Güvenlik Ekibi, bilgi güvenliği altyapısını desteklemek ve işleyişini devam ettirmek ile sorumludur.
- Kurum, bilgi güvenliği farkındalığını sağlamak amacıyla tüm çalışanlara "Bilgi Güvenliği Farkındalık Eğitimleri" vermeyi, bilgi güvenliğini sürekli iyileştirmeyi, yasal mevzuat ve düzenlemeler ile ilgili tarafların uygulanabilir beklentilerini karşılamayı taahhüt etmektedir.
- Bilgi güvenliği politika, prosedür ve talimatlarına uyulmaması halinde, kurum personel yönetmeliği gereğince uyarma, kınama, sözleşme feshi gibi yaptırımlar uygulayabilir.
- Kurumun üst yönetimi, Otokoç Otomotiv Bilgi Güvenliği Politikası'nda belirtilen kurallar çerçevesinde bilgi varlıklarının korunması, bilgi güvenliği farkındalığının yaratılması, ortak bir kurum kültürü oluşturulması, risklerin tespit edilmesi, zayıflıkların kapatılması için gerekli aksiyonların alınması ve güvenlik ihlallerinde gerekli yaptırımın icra edilmesi konularında her türlü desteği vermekle yükümlüdür.
- Kurum, bilgi güvenliği gerekliliklerine uyumunu; iç ve dış denetimler, denetim sonuçlarının yönetime sunulması ve bu sonuçlara dayalı aksiyonların alınması ile sağlamaktadır. Uygulanabilir bilgi güvenliği kontrolleri de ilgili taraflarla birlikte belirlenerek yönetilmektedir.
- Bu politika, Siber Güvenlik Ekibi tarafından yılda en az bir kez gözden geçirilir ve kurumun üst yönetimi tarafından onaylanıp duyurulur. Bilgi güvenliği süreçlerine büyük etkisi olan değişikliklerde de politikanın yeniden gözden geçirilmesi gerekir.