KARSAN OTOMOTİV SANAYİİ VE TİCARET A.Ş.
BİLGİ GÜVENLİĞİ POLİTİKASI

İÇİNDEKİLER:

1. AMAÇ

KARSAN OTOMOTİV SANAYİİ VE TİCARET A.Ş. (KARSAN) bünyesinde çalışanlar ve ilgili tarafların uyması gereken bilgi güvenliği şartlarının çerçevesini çizmek ve yazılı kuralları belirlemek.

Bilgi Güvenliği'nin ve bu politikanın amacı, KARSAN'a ait bilgi varlıklarının yetkili kişilerde kalmasının ve "**Bilgi Varlıklarının Gizlilik, Bütünlük ve Erişilebilirlik"** mevcudiyetinin sağlanmasıdır.

2. KAPSAM

Bilgi Güvenliği Yönetim Sistemi; Şirketin faliyetleri sırasında bilgi varlıklarının güvenliğinin sağlanmasına yönelik gerekli güvenlik önlemlerini, özellikle gümrük ve dış ticaret işlemlerini ve bu işlemlere ilişkin lojistik, depolama, muhasebe, finans ve bilgi işlem faaliyetlerinin bilgi varlıkları ile bu varlıkları korumak amacıyla kullandığı güvenlik önlemlerini kapsar.

Fiili olarak tüm Bilgi Güvenliği Yönetim Sistemi işletme genelinde uygulanacaktır. Gümrük işlemlerinin kolaylaştırılması amacını taşıyan Yetkilendirilmiş Yükümlü Statüsü Sertifikası gereklilikleri uyarınca kurulan Bilgi Güvenliği Yönetim Sistemi çerçevesinde ithalat, ihracat, fiktif depo ve ilgili gümrükleme işlemleri dışındaki diğer tüm süreç ve departmanlar ISO denetim kapsamı dışı olmakla birlikte, bu süreçlerin da denetim kapsamına alınması için gerekli adımlar atılacaktır.

3. REVİZYON BİLGİSİ

Yürürlüğe giren ikinci sürümdür.

4. TANIMLAR

KARSAN kurumsal ve kişisel bilgiyi son derece değerli bir varlık olarak kabul eder. Bu nedenle bilgi varlıkları ve iş sistemleri, işimiz açısından kritik önem taşır ve uygun şekilde korunur.

Bilgi güvenliği, bu politikada aşağıdaki bilgi niteliklerinin korunması olarak tanımlanır:

Gizlilik: Bilginin sadece erişim yetkisi verilmiş kişilere erişilebilir olduğunu garanti etmek,

Bütünlük: Bilginin ve işleme yöntemlerinin doğruluğunu ve yetkisiz değiştirilememesini temin etmek,

Erişilebilirlik: Yetkili kullanıcıların, gerek duyulduğunda bilgiye ve ilişkili kaynaklara en hızlı şekilde erişebileceklerini garanti etmek. Bilgi güvenliği politikası dokümanı, yukardaki korumaları ve gereksinimleri sağlayabilmek için oluşturulmuş denetimlerin uygulanması sırasında kullanılacak en üst seviyedeki prensiplerin belirtildiği dokümandır.

5. İLGİLİ DÖKÜMANLAR

6. İLGİLİ BİRİMLER

Konumları veya görevleri ne olursa olsun tüm KARSAN personeli, Çalışan El Kitabı'nda ve İş Sözleşmelerinde değinilen bilgi varlıklarının korunması ilkelerine uymak zorundadır.

KARSAN bilgilerine erişimi olan üçüncü taraf paydaşlar ile bunların bağlı destek personellerinin, Bilgi Güvenliği Politikası'nın genel ilkelerine ve uymak zorunda oldukları diğer güvenlik kurallarına ve yükümlülüklerine bağlı kalması şarttır.

7. Roller ve Sorumluluklar

7.1 BİLGİ GÜVENLİĞİ ORGANİZASYONU

- Bilgi Güvenliği ile ilgili faaliyetlerin sürdürülmesinden ve geliştirilmesinden Bilgi Güvenliği Yönetim Sistemi (BGYS) Yönetim Temsilcisi sorumludur.
- Bilgi Güvenliği Yönetim Sistemi'nin kurulması ve işletilmesinden BGYS Yöneticisi sorumludur.
- BGYS Yönetim Temsilcisi ve BGYS Yöneticisi, Üst Yönetim tarafından atanmıştır.
- Kapsam dahilindeki birimlerde BGYS Sorumluları belirlenmiştir.
- BGYS Sorumluları kendi birimlerindeki Bilgi Güvenliği Yönetim Sistemi çalışmalarını takip etmek ve koordine etmekle yükümlüdürler.
- BGYS'nin işletilmesi, sürdürülmesi gözden geçirilmesi, eylem planı oluşturulması, karar alınması ve uygulanması faaliyetleri bir komite ile yürütülmektedir. Bu anlamda BGYS Yürütme ve Yönetim Komitesi oluşturulmuştur. BGYS Yürütme ve Yönetim Komitesi, BGYS Üst Yönetim Temsilcisi, BGYS Yöneticisi, İlgili Müdürler ve ilgili birimlerden seçilen BGYS Sorumluları'ndan oluşur. BGYS Yürütme ve Yönetim Komitesi İş sürekliliği tatbikat raporlarının değerlendirmesi veya önemli bir güvenlik ihlal olayı olması durumunda da toplanabilir.

KIRAÇA Bilgi Sistemleri Direktörlüğü, Bilgi Sistemleri faaliyetlerini tarifleyen politika ve prosedürlerin işlevsel olarak sahibidir ve bunların KARSAN bünyesinde uygulanmasından sorumludur.

Tüm KARSAN personeli, Bilgi Güvenliği Politikası'na uyumun sağlanması için gerekli tedbirleri alması ve sistemi gözetlemekten birinci derece sorumludur.

7.2 RİSK YÖNETİMİ

Firmanın ISO 27001 risk yönetim çerçevesi; Bilgi Güvenliği ve Hizmet Yönetimi risklerinin tanımlanmasını, değerlendirilmesini ve işlenmesini kapsar. Risk Analizi ve Risk İşleme Planı Bilgi Güvenliği ve Hizmet Yönetimi risklerinin nasıl kontrol edildiğini tanımlar. Risk İşleme Planının yönetiminden ve gerçekleştirilmesinden BGYS Yürütme ve Yönetim Komitesi sorumludur.

7.3 YÖNETİM SORUMLULUĞU

Yönetim Taahhüdü

KARSAN belirlediği hedef ve politikalarını gerçekleştirmek için Bilgi Güvenliği Yönetim Sistemini ISO/IEC 27001'de belirtilen gereksinimleri yerine getirecek şekilde kurarak yürütür.

KARSAN Genel Müdürlüğü Yönetimi, tanımlanmış, yürürlüğe konmuş ve uygulanmakta olan Bilgi Güvenliği Yönetim Sistemine uyacağını ve sistemin verimli şekilde çalışması için gerekli olan kaynakları tahsis edeceğini, etkinliğini, sürekli iyileştireceğini ve bunun tüm çalışanlar tarafından anlaşılmasını sağlayacağını taahhüt eder. Bu taahhüdün sonucu olarak, firma genelinde bilgi güvenliği farkındalık programları düzenler ve alt yapı yatırımlarını sürdürür.

BGYS kurulurken üst yönetim tarafından BGYS Yönetim Temsilcisi ve BGYS Yöneticisi, atama yazısı ile atanır. BGYS Yönetim Temsilcisi ve BGYS Yöneticisi değiştiğinde, işten ayrıldığında üst yönetim

tarafından doküman revize edilerek atama tekrar yapılır. BGYS Yöneticisini belirlemek ve değiştirmek üst yönetimin yetkisindedir.

Yönetim kademelerindeki yöneticiler güvenlik konusunda alt kademelerde bulunan personele sorumluluk verme ve örnek olma açısından yardımcı olurlar. Üst kademelerden başlayan ve uygulanan bir güvenlik anlayışıyla, firmanın en alt kademe personeline kadar inilmesi zorunludur. Bu yüzden firmadaki yöneticilerin, gerek yazılı gerekse sözlü olarak güvenlik prosedürlerine uymaları, güvenlik konusundaki çalışmalara katılmaları konusunda güvenlik ile ilgili çalışmalarda bulunan personele destek olurlar.

KARSAN Genel Müdürlüğü üst yönetimi, bilgi güvenliği kapsamlı çalışmalar için gerek duyulan bütçeyi oluşturur.

YÖNETİMİN GÖZDEN GEÇİRMESİ

Yönetimin Gözden geçirme toplantıları BGYS Yürütme ve Yönetim Komitesi tarafından yapılır. Bu komite BGYS Yönetim temsilcisi katılımında yılda en az bir kez veya ihtiyaç duyulduğunda Bilgi Güvenliği Yönetim Sisteminin uygunluğunun ve etkinliğinin periyodik olarak değerlendirmesi için toplanır. Toplantılar Yönetimin Gözden Geçirmesi Prosedürü 'ne uygun olarak yapılır.

8. UYGULAMA

8.1 Genel Esaslar

1. Bu politika ile çerçevesi çizilen bilgi güvenliği gereksinimleri ve kurallarına ilişkin ayrıntılar, BGYS prosedürleri ile düzenlenir. KARSAN personeli ve 3. taraflar bu prosedürleri bilmek ve çalışmalarını bu kurallara uygun şekilde yürütmekle yükümlüdür.
2. Bu kural ve prosedürlerin, aksi belirtilmedikçe, basılı veya elektronik ortamda depolanan ve işlenen tüm bilgiler ile bütün bilgi sistemlerinin kullanımı için dikkate alınması esastır.
3. Bilgi Güvenliği Yönetim Sistemi, TS ISO/IEC 27001 "Bilgi Teknolojisi Güvenlik Teknikleri (Information Technology Security Techniques) ve Bilgi Güvenliği Yönetim Sistemleri Gereksinimler (Information Security Management Systems Requirements)" standardını temel alarak yapılandırılır ve işletilir.
4. BGYS dokümanlarının gerektiği zamanlarda güncellenmesi BGYS Yöneticisi sorumluluğundadır.
5. Firma tarafından çalışanlara veya 3. taraflara sunulan bilgi sistemleri ve altyapısı ile bu sistemler kullanılarak üretilen her türlü bilgi, belge ve ürün aksini gerektiren kanun hükümleri veya sözleşmeler bulunmadıkça firmaya aittir.
6. Kritik iş süreçlerini büyük felaketlerin ve işletim hatalarının etkilerinden korumak amacıyla iş sürekliliği yönetimi uygulanır.
7. Çalışanların bilgi güvenliği farkındalığını artıracak ve sistemin işleyişine katkıda bulunmasını sağlayacak eğitimler düzenli olarak mevcut firma çalışanlarına ve yeni işe başlayan çalışanlara verilir.
8. Bilgi güvenliğinin gerçek ya da şüpheli tüm ihlalleri rapor edilir; ihlallere sebep olan uygunsuzluklar tespit edilir, kök neden analizi yapılarak tekrar edilmesini engelleyici önlemler alınır.

8.2 Temel BGYS Prensipleri

1. Çalışanlar ve üçüncü taraflarla kurumun gizlilik ihtiyaçlarını güvence altına almayı amaçlayan gizlilik anlaşmaları yapılır.

2. Dış kaynak kullanım durumlarında oluşabilecek güvenlik gereksinimleri analiz edilerek güvenlik şart ve kontrolleri şartname ve sözleşmelerde ifade edilir.
3. Bilgi varlıklarının envanteri bilgi güvenliği yönetim ihtiyaçları doğrultusunda oluşturulur ve varlık sahiplikleri atanır.
4. Kurumsal veriler sınıflandırılır ve her sınıftaki verilerin güvenlik ihtiyaçları ve kullanım kuralları belirlenir.
5. İşe alım, görev değişikliği ve işten ayrılma süreçlerinde uygulanacak bilgi güvenliği kontrolleri belirlenir ve uygulanır.
6. Güvenli alanlarda saklanan varlıkların ihtiyaçlarına paralel fiziksel güvenlik kontrolleri uygulanır.
7. Firmaya ait bilgi varlıkları için firma içinde ve dışında maruz kalabilecekleri fiziksel tehditlere karşı gerekli kontrol ve politikalar geliştirilir ve uygulanır.
8. Kapasite yönetimi, üçüncü taraflarla ilişkiler, yedekleme, sistem kabulü ve diğer güvenlik süreçlerine ilişkin prosedür ve talimatlar geliştirilir ve uygulanır.
9. Ağ cihazları, işletim sistemleri, sunucular ve uygulamalar için denetim kaydı üretme konfigürasyonları ilgili sistemlerin güvenlik ihtiyaçlarına paralel biçimde ayarlanır. Denetim kayıtlarının yetkisiz erişime karşı korunması sağlanır.
10. Erişim hakları ihtiyaç doğrultusunda ve onaylı Erişim Yetkilendirme talebi ile atanır. Erişim kontrolü için mümkün olan en güvenli teknoloji ve teknikler kullanılır.
11. Sistem temini ve geliştirilmesinde güvenlik gereksinimleri belirlenir, sistem kabulü veya testlerinde güvenlik gereksinimlerinin karşılanıp karşılanmadığı kontrol edilir.
12. Bilgi güvenliği ihlal olayları ve zayıflıklarının raporlanması için gerekli altyapı oluşturulur. İhlal olay kayıtları tutulur, gerekli düzeltici önleyici faaliyetler uygulanır ve düzenlenen farkındalık eğitimleri vasıtasıyla güvenlik olaylarından öğrenme sağlanır.
13. Kritik altyapı için süreklilik planları hazırlanır, bakımı ve tatbikatı yapılır.
14. Yasalara, iç politika ve prosedürlere, teknik güvenlik standartlarına uyum için gerekli süreçler tasarlanır, sürekli ve periyodik olarak yapılacak gözetim ve denetim faaliyetleri ile uyum güvencesi sağlanır.

8.3 Uyulması Gereken BGYS Kuralları

1. Uyulması Gereken Kabul Edilebilir Kullanım Kuralları, çalışanlar ve 3. taraflar için kurum iş süreçlerinde ve ilgili çalışmalarında bilgi depolama, iletim ve kullanım biçimleri ile ilgili uyulması gereken kuralları belirler.
2. Aşağıda yer alan davranışlar; aksi yönde açık ve net bir iş tanımı, talimat veya prosedür bulunmadıkça Bilgi Güvenliği Politikası'nın ihlali olarak değerlendirilir.
3. Firma tarafından sağlanan bilgi işlem sistemleri ve uygulamalar iş amaçlı olarak kullanılır. İş süreçlerini engellemeyecek düzeyde ve Bilgi Güvenliği Politikası'nı ve BGYS prosedürlerini ihlal etmeyen kişisel kullanımlar kabul edilebilir kapsamda değerlendirilir.
4. Çalışma alanlarında, "Temiz Masa ve Temiz Ekran" prensiplerine uygun olarak, Genel özellikteki bilgiler dışında bilgilerin başkalarınca görülmesine imkân verilmeyecek şekilde önlemler alınmalıdır.
5. Genel olmayan belgeler, masalarda bırakılmamalıdır.
6. Genel olmayan dosyalar üzerinde çalışılırken bilgisayar ekranları herkesin görebileceği konumda bırakılmamalıdır.

7. Genel olmayan dokümanlar diğer kişilerce görülmesini engellemek amacıyla, kullanılmadığı zamanlarda masa üstlerinden kaldırılıp gerekli korumaları alınmış çekmece ve dolaplarda saklanmalıdır.
8. Genel olmayan belgeler dışında doğrudan işle ilgili olarak kendisine ulaştırılmayan ya da teslim edilmeyen firma belgelerini incelememeli, değiştirmemeli, saklamamalı, kopyalamamalı, silmemeli ve paylaşmamalıdır.
9. Firma tarafından açıkça belirtilen durum ve yöntemler dışında 3. taraflar ile kurum bilgilerini paylaşmamalı, satmamalı, aktarmamalı, yayınlamamalı ve internet ortamında paylaşmamalıdır.
10. Birim çalışanları çalıştıkları ortamdaki masa ve dolap çekmecelerini kilitli tutmalı ve anahtarları sorumlu kişiler haricinde kimseyle paylaşmamalıdır.
11. Bilgisayarlar, aktif kullanım dışında iken şifreli ekran koruyucular devreye alınmalıdır. Mesai zamanları dışında bilgisayar sistemleri kapalı tutulmalıdır.
12. Çalışanlar, kendilerine verilmiş olan kullanıcı adı ve şifreleri sadece kendileri kullanmalıdır.
13. Çalışanlar, kendilerine verilmiş olan kullanıcı adı ve parola bilgilerini yetkilendirilmemiş kişilerin ele geçirmesine imkan verecek şekilde söylememeli, yazmamalı, kaydetmemeli ve elektronik ortamda depolamamalıdır.
14. Firmanın, bilgi ve haberleşme sistemleri ve donanımları (İnternet, e-posta, telefon, çağrı cihazları, faks, bilgisayarlar, mobil cihazlar ve cep telefonları vb.) firma işlerinin yürütülmesi için kullanılmalıdır. Bu sistemler yasadışı, firmanın diğer politika, standart ve rehberlerine aykırı veya firmaya zarar verecek herhangi bir şekilde kullanılmamalıdır.
15. Firmaya ait bilgi sistemleri üzerindeki kaynaklara erişecek tüm bilgisayarlar etki alanına dahil edilerek kullanılmalıdır.
16. Gerekmedikçe bilgisayar kaynaklarını paylaşıma açılmamalıdır. Kaynakların paylaşıma açılması halinde sadece ilgili kişilere yetki verilmelidir.
17. Gizli ve hassas bilgiler elektronik ortamda firma içine ve özellikle firma dışına gönderilmeden önce şifrelenmelidir.
18. Gizlilik dereceli bilgiler içeren belgeleri, elektronik ortamları ve bilgi işlem sistemlerini korumak için gerekli fiziksel önlemleri "Fiziksel Güvenlik Prosedürü"ne uygun şekilde yerine getirmemelidir.
19. Firmaya ait bilgi işlem sistemlerini, veri tabanlarını, dosyaları, ağ topolojilerini, cihaz konfigürasyonlarını ve benzeri kaynakları, firma tarafından açıkça yetkilendirilmedikçe 3.taraflar ile paylaşmamalıdır.
20. Firma çalışanları, çalıştıkları sürece veya firmadan ayrılmaları (emeklilik, istifa, vs.) durumunda firma bilgilerini gizlilik prensibine uygun olarak korumaktan sorumludur.
21. Taşınabilir sistemlerin kullanıcıları, bu sistemlerin güvenliğini sağlamak üzere "Taşınabilir Ortam Kullanımı Prosedürü" ne uymalıdırlar.
22. Başta kullanıcı bilgisayarları ve sunucular olmak üzere mümkün olan tüm sistemler, zararlı yazılımlara karşı korunması için "Virüslü ve Zararlı Yazılımdan Korunma Prosedürü "ne uygun şekilde kullanılmalıdır.
23. Gizlilik dereceli bilgiler elektronik ortamda işlenirken, depolanırken, aktarılırken "Bilgi İşleme Prosedürü "ne uygun şekilde davranılmalıdır.
24. Gizlilik dereceli bilgilerin ve bilgi içeren ortamlarının imhasında "Teçhizatın Elden Çıkarma Prosedürü "ne uygun şekilde davranılmalıdır.

25. Herkese açık sistemler (örn. Genel internet sayfaları) hariç tüm bilişim sistemlerine erişim parola korumalı olmalıdır. Parolalar “Şifre Politikası’’na uygun şekilde tanımlanmalı ve kullanılmalıdır.
26. Gizlilik dereceli bilgilerin posta, faks, telefon, e-posta ve benzeri elektronik yöntemlerle iletiminde “Bilgi İşleme Prosedürü“ne uygun davranılmalıdır.
27. Herkese açık bilgiler dışındaki bilgileri internet üzerinde, haber gruplarında, posta listelerinde ve forumlarda paylaşmamalıdır.
28. Yeni bilgi sistemlerinin devreye alınması ve geliştirilmesi “Yeni Bilgi Sistemleri ve Yapılan Geliştirme Prosedürü “ne uygun yapılmalıdır.
29. Çalışanlara ve gerekli görülen durumlarda 3. taraflara tahsis edilen e-posta hesapları, “E-posta Prosedürü“ne uygun şekilde kullanılmalıdır.
30. Bilgi işlem sistemlerinin teknik güvenlik gereksinimlerine uygun durumda bulunup bulunmadığı, “Teknik Açıklıklarının Kontrolü Prosedürü “ne uygun şekilde kontrol edilmelidir.
31. Firmaya ait bilgi işlem sistemleri izinsiz olarak kullanım dışı bırakılmamalı, yeri değiştirilmemeli ve firma dışına çıkartılmamalıdır.
32. Kullanım gerekliliği firma tarafından yazılı olarak belirtilen güvenlik yazılımları (örn. Anti virüs, kişisel güvenlik duvarı, vb.) bilgi işlem sistemlerinden kaldırılmamalı veya devre dışı bırakılmamalıdır.
33. İstemciden istemciye dosya paylaşım programları (P2P) kurum bilgisayarlarına yüklenmemeli ve kullanılmamalıdır.
34. Firmaya ait bilgisayarlara, firmanın yasakladığı yazılımlar yüklenmemeli ve çalıştırılmamalıdır. Firma tarafından lisanslanmış yazılımlar çoğaltılmamalı, paylaşıma açılmamalı ve firma dışına çıkarımamalıdır.
35. Etki alanına dahil olmayan sistemler ile etki alanına dahil olan sistemler arasında bilgi aktarımı yapılmamalıdır.
36. Taraflar ile gizlilik sözleşmesi imzalanmadan ve yetkili firma çalışanınca nezaret edilmeden kurum bilgi işlem sistemlerine ve donanımlarına bağlanmamalı ve çalışmalarına izin verilmemelidir.
37. Sunucu sistemleri üzerinde, kişisel bilgisayar uygulamalarını (örn; e-posta programları, ofis uygulamaları, yazılım geliştirme araçları, network test araçları, vb.) kurulmamalı ve kullanılmamalıdır.
38. İş süreçleri için gerekmeyen ve kullanılmasına izin verilmeyen sunucu hizmetlerini (örn; HTTP, Telnet, SSH, vb.) bilgi işlem sistemleri üzerinde çalıştırılmamalıdır. Firma tarafından sağlanan ve kullanım amaç ve biçimleri yazılı olarak bildirilen kurum ağ bağlantı yöntemleri dışında bir yöntemle (örn; ADSL modem, 3G modem, GPRS, vb.) internete veya başka ağlara bağlanmak için kullanılmamalıdır.
39. Çalışanlar, firma içi ya da firma dışı bilgi sistemlerine yetkisi olmadığı halde zorla girmeye çalışmamalıdır.
40. Firmaya ait bilgi işlem sistemlerine şifreleme ve parola mekanizmalarını kırmaya yönelik program ve araçlarını yüklenmemeli ve kullanılmamalıdır.
41. Firmaya ait bilgi sistemleri üzerinde, firmanın bilgisi ve izni olmadan değişiklik, yükseltme, genişletme yapılmamalıdır.

42. İşle ilgili olmayan veya telif hakları ile korunan dosyaları (örn. Müzik, film, kitap dosyaları, vb.) firma bilgisayarlarına ve bilgi sistemlerine indirilmemeli, depolanmamalı, çoğaltılmamalı ve paylaşıma açılmamalıdır.
43. Firma bilgi işlem sistemlerini iş dışında, eğlence amaçlı (oyun vb.) kullanılmamalıdır.
44. Firma e-posta hesabı ile zincirleme e-posta gönderilmemelidir.
45. Firma bilgi işlem sistemlerinde veya süreçlerinde gözlenen güvenlik zafiyetlerini, açıklarını veya oluşmuş saldırıları Bilgi Güvenliği İhlal Olayı Yönetim Prosedürü'nde belirtilen "bildirme" yöntemi ve muhatapları dışında ilgili olmayan kişilere iletilmemeli, açıklanmamalı, yayınlanmamalı veya bu zafiyetleri yetkisi dışındaki sistem ve bilgilere erişmek için veya kendi yetkilerini arttırmak için kullanılmamalıdır.

8.4 Yaptırım

Bilgi Güvenliği Politikası ilkeleri, Çalışan El Kitabı'na paralel uygulanır. Bilgi Güvenliği Politikası ihlalleri aynı zamanda etik kural ihlalidir ve disiplin cezası sonucunu doğurabilir. Gerek gözetim, gerek denetim, gerekse ihbar sonucu tespit edilen Bilgi Güvenliği Politikası ihlalleri iş akdine son verilmesine kadar gidebilecek disiplin cezaları ile sonuçlanabilir.

9. KAYITLAR

10. DAĞITIM VE DOSYALAMA