FORD OTOSAN

FORD OTOMOTİV SANAYİ A.Ş.
BİLGİ GÜVENLİĞİ POLİTİKASI

FORD OTOSAN

1. AMAÇ

İşbu Ford Otomotiv Sanayi A.Ş. Bilgi Güvenliği Politikası'nın (Kısaca "**Politika**") amacı, Ford Otomotiv Sanayi A.Ş.'nin (Kısaca "**Ford Otosan**") bilgi sistemlerinin kurulması, işletilmesi, yönetilmesi ve kullanılmasına ilişkin; bilginin gizliliğinin, bütünlüğünün ve gerektiğinde erişilebilir olmasının sağlanmasına yönelik bilgi güvenliği süreçlerinin işletilmesi için gerekli rollerin ve sorumlulukların tanımlanması, bilgi sistemlerine ilişkin risklerin yönetilmesine dair süreçlerin oluşturulması, kontrollerin tesis edilmesi ve gözetiminin sağlanmasıdır.

2. KAPSAM

Tüm Ford Otosan çalışanları, Ford Otosan Yetkili Servis ve Bayileri, Ford Otosan ile iş yapan tedarikçi, müteahhit, alt-işverenler ve diğer üçüncü taraflar ve bunların personelleri işbu Politika'nın kapsamındadır.

3. TANIMLAR

İşbu dokümanda bahsi geçen;

Bilgi Güvenliği Yönetim Sistemi (BGYS): Ford Otosan'ın hassas ve önemli bilgilerini yönetebilmek amacıyla benimsenen sistematik bir yaklaşımı,

Bilgi Güvenliği Forumu: Ford Otosan CFO, Bilgi Teknolojileri Direktörü, BT Denetim, Uyum ve Risk Yönetimi Yöneticisi, BT Altyapı ve İşletim Müdürü, BT Siber Güvenlik Ekip Lideri, İç Denetim Müdürü, Risk Yönetimi Yöneticisi, Toplam Kalite Müdürü, ve BGYS kapsamı içindeki bölümlerin yöneticilerinin katılımıyla oluşturulmuş**,** Ford Otomotiv Sanayi A.Ş. Bilgi Güvenliği Yönetim Sistemi Komitesi'ni,

Bilgi Sistemleri Güvenliği Sorumlusu: Tebliğ kapsamında Üst Yönetim tarafından görevlendirilen Ford Otosan BT Denetim, Uyum ve Risk Yönetimi Yöneticisi'ni

Bilgi Teknolojileri ve Bilgi Güvenliği İhlal Yönetim Ekibi: Çalışanların bilgi güvenliği ihlalerini kaydeden ve inceleyen, Bilgi Teknolojileri Denetim, Uyum ve Risk Yönetimi Ekibi, Siber Güvenlik Ekibi, Hizmet Masası Ekip Lideri ve Altyapı ve İşletim Müdürü'nden oluşan Ford Otosan ekibini,

Bilgi/Bilgi Varlıkları: Ford Otosan'a ait tüm bilgi ve bilginin kullanılması için gerekli tüm elektronik (yazılım, donanım, iletişim ve güvenlik altyapısı, arşiv sistemleri vb.) ve fiziksel (tesisler, odalar, dolaplar vb.) ortamları ve bilgiye erişen tüm çalışanları,

Bilgi Teknolojileri Direktörü: Ford Otomotiv Sanayi A.Ş. Bilgi Teknolojileri Direktörü'nü,

Çalışan(lar): Ford Otosan bünyesinde iş sözleşmesi ile çalışan tüm personeli,

Ford Otosan: Ford Otomotiv Sanayi A.Ş.'yi,

Ford Otosan KVK Komitesi: 6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamında BT Direktörü başkanlığında oluşturulan ve Bilgi Teknolojileri, Hukuk Bölümü, İç Denetim Müdürlüğü ve tüm departmanlarda atanan KVK sorumlularından oluşan komiteyi,

Üçüncü Taraflar : Ford Otosan Yetkili Servis ve Bayileri, Ford Otosan ile iş yapan tedarikçi, müteahhit, alt-işverenler, diğer üçüncü taraflar ve bunların personellerini,

Politika: Ford Otomotiv Sanayi A.Ş. Bilgi Güvenliği Politikası'nı,

Tebliğ : 05.01.2018 tarihinde yayımlanan Sermaye Piyasası Kurulu'nun Bilgi Sistemleri Tebliği (VII-128.9)'ni

Üst Yönetim: Ford Otosan Yönetim Kurulu tarafından yetkilendirilmiş Ford Otosan Genel Müdür'ü ve Bilgi Teknolojileri Direktörü'nü,

Yönetim Kurulu: Ford Otosan Yönetim Kurulu'nu,

ifade eder.

4. GENEL PRENSİPLER

İşbu Bilgi Güvenliği Politikası;

a) Tebliğ ile halka açık şirketler için getirilen yükümlülükler dahil konuyla ilgili her türlü yasal mevzuata, Ford Motor Company ve Koç Topluluğu politikalarına uyum sağlanmasını,

b) Bilgi ve Bilgi Varlıkları'nın gizlilik, bütünlük ve erişilebilirlik özelliklerinin korunmasını,

c) Bilgi ve Bilgi Varlıkları'na olan kontrolsüz ve yetkisiz erişimlerin engellenmesini,

d) Bilgi ve Bilgi Varlıkları'na yönelik risklerin tespiti, gerekli iyileştirme faaliyetlerinin düzenli ve sürekli olarak yapılmasının sağlanmasını,

e) Bilgi teknolojileri altyapı ve uygulamalarında iş sürekliliğini destekleyecek hizmetlerin oluşturulması ve devamlılığının sağlanmasını,

f) Bilgi güvenliği ihlallerini engelleyecek önlemlerin alınarak, kurumsal öğrenmenin sağlanmasını,

g) Çalışanlar'a ve 3. taraflara bilgi güvenliği konusunda farkındalık eğitimleri verilmesi ve bilinçlendirilmesinin sağlanmasını, ve

h) Bilgi Güvenliği Yönetim Sistemi'nin sürekli iyileştirilmesini,

taahhüt eder.

5. SORUMLULUKLAR

5.1. Yönetim Kurulu

a) Bilgi Güvenliği Politikası'nın onaylanması,

b) Politika kapsamında bilgi sistemleri üzerinde etkin ve yeterli kontrollerin tesis edilmesi,

c) Bilgi güvenliği politikasının uygulanmasından sorumlu Üst Yönetim'in belirlenmesi,

d) Bilgi sistemlerinin geliştirme, değişiklik veya edinimi faaliyeti boyunca, işin gelişimini takip edebilmek için hazırlanan proje gelişim raporlarının onaylanması,

Yönetim Kurulu'nun sorumluluğundadır.

5.2. Üst Yönetim

5.2.1. Yönetim Kurulu, Ford Otosan Genel Müdürü'nü ve Bilgi Teknolojileri Direktörü'nü işbu Politika kapsamında Üst Yönetim olarak belirlemiştir.

5.2.2. Üst Yönetim;

a) Yönetim Kurulu tarafından onaylanacak Bilgi Güvenliği Politikası'nı hazırlamak,

b) Politika'nın uygulanmasını gözetmek,

c) Yeni bilgi sistemlerinin kullanıma alınmasına ilişkin kritik projelerin gözden geçirilmesi ve bunlara ilişkin risklerin yönetilebilirliği göz önünde bulundurularak onaylanması,

d) Bilgi güvenliği önlemlerinin uygun düzeye getirilmesi hususunda gereken kararlılığı göstermek ve bu amaçla yürütülecek faaliyetlere yönelik olarak yeterli kaynağı tahsis etmek,

e) Asgari olarak aşağıdaki faaliyetlerin yerine getirilmesini temin edecek mekanizmaları kurmak:

i. Bilgi güvenliği politikalarının ve tüm sorumlulukların her yıl gözden geçirilmesi ve onaylanması,

ii. Bilgi sistemlerine ve süreçlerine ilişkin potansiyel risklerin etkileriyle birlikte tespit edilmesi ve bu çerçevede söz konusu risklerin azaltılmasına yönelik faaliyetlerin tanımlanmasını içeren risk yönetiminin gerçekleştirilmesi,

iii. Bilgi güvenliği ihlallerine ilişkin olayların izlenmesi ve her yıl değerlendirilmesi,

iv. Tüm çalışanların bilgi güvenliği farkındalığını artırmaya yönelik çalışmaların yapılması ve eğitimlerin verilmesi.

f) Bilgi sistemlerine ilişkin risklerin yönetimi amacıyla tesis edilen süreç ve prosedürleri, Ford Otosan'ın organizasyonel ve yönetsel yapısı içerisinde fiili olarak işleyecek şekilde yerleştirmek ve işlerliğine ilişkin gözetim ve takipler gerçekleştirmek,

g) Bilgi sistemleri güvenliğine ilişkin süreç ve prosedürlerin gereklerinin yerine getirilmesinden ve takibinden sorumlu olan, bilgi sistemleri güvenliğiyle ilgili riskler ve bu risklerin yönetilmesi hususunda Üst Yönetime rapor veren ve yeterli teknik bilgi ve tecrübeye sahip bir Bilgi Sistemleri Güvenliği Sorumlusu belirlemek,

h) Risk önceliklerine göre tüm kritik iş süreçlerinin sürekliliğini sağlamak için iş sürekliliği planı hazırlamak ve planda kritik iş süreçlerine ilişkin kabul edilebilir kesinti süreleri ile kabul edilebilir azami veri kaybını belirlemek,

i) Bilgi güvenliği politikası kapsamında, bilgi sistemlerinden kaynaklanan güvenlik risklerinin yeterli düzeyde yönetildiğinden emin olmak için, bilgi sistemlerinin ve üzerinde işlenmek, iletilmek, depolanmak üzere bulunan verilerin gizlilik, bütünlük ve erişilebilirliklerini sağlayacak önlemlere ilişkin kontrollerin geliştirilmesini, işletilmesini, güncelliğini sağlamak ve gerekli yönetsel sorumlulukları tanımlamak,

j) Bilgi sistemleri kapsamında dış kaynak yoluyla alınacak hizmetlerin doğuracağı risklerin yeterli düzeyde değerlendirilmesine, yönetilmesine ve dış kaynak yoluyla alınan hizmeti sağlayan kuruluşlarla ilişkilerin etkin bir şekilde yürütülebilmesine olanak sağlayacak bir gözetim mekanizması tesis etmek, ve

k) Dış kaynak yoluyla gerçekleştirilen hizmetler için hizmetin erişilebilirliğini, performansını, kalitesini, bu hizmet kapsamında gerçekleşen güvenlik ihlali olayları ile dış kaynak yoluyla hizmet sağlayan kuruluşun güvenlik kontrollerini, finansal koşullarını ve sözleşmeye uygunluğunu yakından takip etmek için yeterli bilgi ve tecrübeye sahip sorumluları belirlemek,

hususunda sorumludur.

5.3. Bilgi Güvenliği Forumu

Bilgi Güvenliği Forumu, Üst Yönetim liderliğinde;

- **a)** İşbu Bilgi Güvenliği Politikası kapsamındaki uygulama esaslarının belirlenmesi amacıyla alt politikalar ile destekleyici diğer standart ve süreçleri gözden geçirmek ve onaylamaktan,
- **b)** Bilgi güvenliği gereksinimlerinin yerine getirilmesini takip etmekten,
- **c)** Şirket içi güvenlik ihlallerini tanımlamak ve bunların uygun disiplin kuralları ile kontrol edilmesini sağlamaktan,
- **d)** Bilgi varlıklarına yönelik risklerin kabul ediledilir seviyede tutulması için gerekli çalışmaları planlayıp hayata geçirmekten,

sorumludur.

5.4.Bilgi Sistemleri Güvenliği Sorumlusu

5.4.1. Ford Otosan "BT Denetim, Uyum ve Risk Yönetimi Yöneticisi", Üst Yönetim tarafından Bilgi Sistemleri Güvenliği Sorumlusu olarak görevlendirilmiştir.

5.4.2. Bilgi Sistemleri Güvenliği Güvenliği Sorumlusu;

- **a)** Bilgi güvenliği ile ilgili prosedür ve talimatları oluşturmak, onaya sunmak ve yayınlamaktan,
- **b)** Bilgi sistemleri güvenliğine ilişkin süreç ve prosedürlerin gereklerinin yerine getirilmesinden ve takibinden,
- **c)** bilgi sistemleri güvenliğiyle ilgili riskler ve bu risklerin yönetilmesi hususunda Üst Yönetim'e 2 ayda bir rapor vermekten,
- **d)** Bilgi güvenliğine ilişkin süreçleri denetlemekten ve tespit edilen ihlalleri gerektiğinde İç Denetim Müdürlüğü ve İnsan Kaynakları Direktörlüğü'ne iletmekten,

sorumludur.

5.5. Çalışanlar

Çalışanlar Bilgi Güvenliği Politika'sı, ilgili Ford Otosanprosedürleri ve mevzuatta belirtilen bilgi güvenliği kurallarına uymak, bilgi güvenliği ihlallerini Bilgi Teknolojileri ve Bilgi Güvenliği İhlal Yönetim Ekibi'ne alert@ford.com.tr mail adresi kanalı ile en kısa sürede bildirmek ile sorumludur.

5.6. Üçüncü Taraflar

Ford Otosan ile olan iş ilişkileri sırasında Ford Otosan!a ait her türlü Bilgi ve Bilgi Varlıkları'nı Ford Otosan tarafından belirlenen kriterlere uygun şekilde korumak ve talep edilen tedbirleri almakla, karşılaştıkları bilgi güvenliği eksik ve ihlallerini alert@ford.com.tr mail adresi üzerinden Ford Otosan'a en kısa sürede bildirmek ile sorumludur.

6. RİSK YÖNETİMİ

Ford Otosan bünyesinde bilgi güvenliği risklerini belirlemek, sınıflandırmak, gerekli risk azaltıcı tedbirleri almak ve bu faaliyetleri takip etmek amacı ile, Kurumsal Risk Yönetimi Süreci ile de

uyumlu olacak şekilde bir **GPRBT-062 nolu Ford Otosan BGYS Risk Yönetimi Prosedürü** uygulanmaktadır.

Bilgi ve Bilgi Varlıkları, kritiklikleri de göz önüne alınarak, tehditlerin etkileri ve bu tehditlerin gerçekleşme olasılıkları ile birlikte risk değerlendirmesi kapsamında ele alınır ve risk haritaları oluşturulur.

Risk haritaları, Kurumsal Risk Yönetimi Süreci çerçevesinde düzenli olarak gözden geçirilir ve Kurumsal Risk Yönetim Komitesi içinde ele alınır.

7. STANDARTLAR

BT-PM Kodlu Ford OtosanBilgi Güvenliği Kontrol Standartları dokümanı, bilgi güvenliği süreç, politika, prosedür ve standartları kapsamaktadır.

8. KİŞİSEL VERİLERİN KORUNMASI

İşbu Politika ve ilgili Ford Otosan prosedürlerinin **6698 Sayılı Kişisel Verilerin Korunması Kanunu** hükümlerine, **Ford Otosan Kişisel Verilerin Korunması Politikası** ve **Ford Otosan KVK Komite Çalışma Esasları Talimatı**'na uygun şekilde yürütülmesi esastır. Kişisel verilerin güvenliği için alınması gereken teknik tedbirler konusunda Üst Yönetim ve Bilgi Sistemleri Güvenliği Sorumlusu, Ford Otosan KVK Komitesi ile birlikte çalışır.

9. DENETİM

Ford Otosan'ın yaptığı denetlemeler veya bildirimler sonucunda bilgi güvenliği ihlaline ilişkin tespit edilen şüpheli olay ve bulgular Ford Otosan İç Denetim Müdürlüğü ve Bilgi Sistemleri Güvenliği Sorumlusu ile birlikte değerlendirilir ve ihlal tespit edilmesi halinde vaka Ford Otosan İnsan Kaynakları Direktörlüğü'ne ilgili disiplin prosedürün işletilmesi amacıyla Bilgi Sistemleri Güvenliği Sorumlusu tarafından uygun şekilde iletilir.

10. POLİTİKA'NIN GÜNCELLENMESİ VE DUYURULMASI

İşbu Politika'nın değişen ihtiyaç ve mevzuata göre güncellenmesinden Bilgi Teknolojleri Direktörlüğü sorumludur. Politika ayrıca **GTYBT-006 Kodlu Bilgi Güvenliği Forumu Talimatı**'nda belirlenen sürelerde gözden geçirilir. Politika'nın güncel versiyonu Şirket portalında ve Şirket kurumsal web sitesinde erişime açık hale getirilir. Ayrıca duyuru yoluyla çalışanlara ilan edilir.

11. YÜRÜRLÜK

11.09.2013 tarihinde yürürlüğe giren işbu Politika güncellenmiş ve 22.03.2021 tarihinde Yönetim Kurulu tarafından onaylanarak yürürlüğe girmiştir.