FORD OTOSAN

FORD OTOSAN
BİLGİ GÜVENLİĞİ POLİTİKASI

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;

Ayrıcalıklı Kullanıcı / Ayrıcalıklı Hesap (Privileged Account): Sistem ve güvenlik ayarlarında değişiklik yapma, kritik işlemleri yürütme gibi yüksek ayrıcalık gerektiren faaliyetlerin gerçekleştirilmesine izin veren kullanıcı hesaplarını,

Asgari Yetki Prensibi: Kullanıcılara görevlerini yerine getirebilmeleri için gerekli en düşük erişim seviyelerinin verilmesini amaçlayan yetkilendirme yaklaşımını,

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

Bilgi Güvenliği Forumu: Dijital Ürünler ve Servisler Lideri, DPS Güvenlik ve Risk Lideri, Altyapı ve İşletim Lideri, İç denetim Lideri, Kurumsal Risk Yönetimi Lideri, Kalite Platform Alanı Lideri ve BGYS kapsamı içindeki bölümlerin liderlerinin 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 Bilgi Sistemleri Güvenliği Sorumlusu,

Bilgi Teknolojileri ve Bilgi Güvenliği İhlal Yönetim Ekibi: Çalışanların bilgi güvenliği ihlallerini kaydeden ve inceleyen DPS Güvenlik ve Risk Ekibi, Çözüm Merkezi Ürün Sahibi, Altyapı ve İşletim Lideri'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,

Dijital Ürünler ve Servisler Lideri: Ford Otomotiv Sanayi A.Ş. Dijital Ürünler ve Servisler Lideri'ni

Coğrafi Ayrışma: Birincil ve ikincil sistemlerin aynı fiziksel risklere eşzamanlı maruz kalmaması için farklı lokasyonlarda konumlandırılmasını,

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

Erken Uyarı Mekanizmaları: Yetkisiz erişim, olağandışı faaliyetler veya güvenlik tehditlerinin hızlı şekilde tespit edilmesine yönelik olarak kullanılan izleme ve alarm sistemlerini,

Felaket Kurtarma Testi (DR Testi): Felaket durumlarında bilgi sistemlerinin yedek ortamlarda çalışabilirliğini doğrulamak üzere gerçekleştirilen planlı test faaliyetlerini,

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

Ford Otosan KVK Komitesi: 6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamında Dijital Ürünler ve Servisler Lideri başkanlığında oluşturulan ve Dijital Ürünler ve Servisler Liderliği, Hukuk ve Uyum Liderliği, İç Denetim Liderliği ve tüm departmanlarda atanan KVK sorumlularından oluşan komiteyi,

Hizmet Envanteri: Bilgi sistemleri kapsamında sunulan tüm hizmetlerin kapsamı, bileşenleri, sahipliği ve güvenlik sınıflandırması ile kayıt altına alındığı envanteri,

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,

Süreç Envanteri: Bilgi sistemleri kapsamındaki iş süreçlerinin tanımlanarak dokümante edildiği, sınıflandırıldığı ve güncel tutulduğu envanteri,

Tebliğ : 05.01.2018 tarihinde yayımlanan VII-128.9 sayılı tebliğ ve 13.03.2025 tarihinde yürürlüğe giren VII-128.10 sayılı değişiklikler dâhil olmak üzere Sermaye Piyasası Kurulu'nun Bilgi Sistemleri Yönetimine ilişkin ilgili tebliğ ve düzenlemelerini

Üst Yönetim: Ford Otosan Yönetim Kurulu tarafından yetkilendirilmiş *Ford Otosan Lideri* ve *Dijital Ürünler ve Servisler Liderini,*

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,(ayrıca bkz. Madde 9)

c) Bilgi ve Bilgi Varlıkları'na olan kontrolsüz ve yetkisiz erişimlerin engellenmesini, (ayrıca bkz. Madde 8)

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, (ayrıca bkz. Madde 11)

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 Lideri ve Dijital Ürünler ve Servisler Lideri'ni* 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 kaynaklı hizmetlere ilişkin gözetim mekanizmasını (bkz. Madde 10) işletmek üzere 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 Bilgi Sistemleri Güvenliği Sorumlusu bilgi sistemleri iç kontrolü, denetimi, yönetişimi veya güvenliği alanlarında teknik bilgiye ve en az 5 yıl tecrübeye sahip olmalıdır. Bilgi sistemleri yönetimine ilişkin gerekliliklerin yerine getirilmesinde herhangi bir operasyonel görevi olmamalı ve doğrudan üst yönetime bağlı olarak çalışmalıdır.

5.4.2. *Ford Otosan Bilgi Sistemleri 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 Liderliği ve İnsan Kaynakları ve Dönüşüm Liderliği'ne* iletmekten,

sorumludur.

5.5. Çalışanlar

Çalışanlar Bilgi Güvenliği Politika'sı, ilgili Ford Otosan prosedürleri ve mevzuatta belirtilen bilgi güvenliği kurallarına uymak, bilgi güvenliği ihlallerini *Dijital Ürünler ve Servisler* 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 **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. BİLGİ VARLIĞI, HİZMET VE SÜREÇ ENVANTERLERİ

Ford Otosan bünyesinde yer alan tüm Bilgi ve Bilgi Varlıkları'nın; tanımı, sahibi, kullanıcısı, güvenlik sınıfı, yedekleme bilgisi ve benzeri asgari unsurları kapsayacak şekilde envanteri oluşturulur ve güncel tutulur.

Bilgi sistemleri kapsamında sunulan tüm hizmetlere ilişkin hizmet envanteri ile bilgi sistemleri süreçlerine ilişkin süreç envanteri hazırlanır; söz konusu envanterler düzenli aralıklarla gözden geçirilerek güncellenir.

Bu envanterlerin oluşturulması, yönetimi ve güvenliğinin sağlanmasına yönelik yükümlülükler ilgili prosedürler çerçevesinde yerine getirilir.

8. ERİŞİM VE YETKİLENDİRME YÖNETİMİ

Ford Otosan bilgi sistemlerine erişimlerde, Tebliğ'in 11'inci maddesi uyarınca görevler ayrılığı ve asgari yetki prensipleri uygulanır. Bu kapsamda, yetki tanımlama, yetki onayı ve yetki kullanımı süreçleri ile sistem geliştirme, test ve canlı ortam faaliyetleri mümkün olduğunca farklı kişi veya birimler tarafından yürütülür ve kritik işlemlerin tek bir kişi tarafından uçtan uca gerçekleştirilmesi engellenir.

Kullanıcı yetkileri, iş gerekliliklerine uygunluğu açısından düzenli olarak gözden geçirilir ve güncellenir. Personelin görev değişikliği veya ayrılışı durumunda ilgili erişim yetkileri derhal sonlandırılır.

Ortak, varsayılan veya paylaşımlı kullanıcı hesaplarının kullanımı, zorunlu haller dışında engellenir; mecburi durumlarda bu hesapların kullanımından sorumlu kişiler açıkça belirlenir ve bu hesaplarla gerçekleştirilen tüm işlemlerin denetim izleri (log) tutulur.

Kullanıcılara lokal yönetici (admin) hakları verilmez; ancak iş gerekçesi ve Bilgi Sistemleri Güvenliği Sorumlusu'nun onayı ile geçici olarak tanınabilir. Ayrıcalıklı (privileged) işlemler için ayrı kullanıcı hesapları kullanılır ve bu hesaplara ilişkin faaliyetler kayıt altına alınır.

Bilgi sistemlerinde gerçekleşen olağandışı, beklenmeyen veya yetkisiz erişim girişimleri, erken uyarı mekanizmaları ve güvenlik kontrolleri üzerinden izlenir ve gerekli önleyici tedbirler alınır.

9. VERİ GİZLİLİĞİ VE KRİPTOGRAFİ YÖNETİMİ

Ford Otosan bilgi sistemleri kapsamında iletilen, işlenen, saklanan ve erişilen tüm verilere yönelik gizlilik, bütünlük ve erişilebilirlik ilkelerinin korunması esastır. Özellikle hassas veriler ve müşteri bilgileri, uygun kriptografik yöntemler kullanılarak korunur.

Kriptografik kontrollerin uygulanmasında güvenilirliği kanıtlanmış ve güncel şifreleme algoritmaları kullanılır; güvenliğini yitirmiş, kırılmış veya çalınmış şifreleme anahtarlarına ilişkin kullanım derhal durdurulur.

Şifreleme anahtarlarının oluşturulması, saklanması, dağıtımı, erişimi ve imhası süreçleri kontrol altına alınır; anahtar yönetimi, verinin ve ilgili operasyonun kritiklik seviyesine göre tanımlanan periyotlarda düzenli olarak güncellenir ve denetlenir.

Veri güvenliğine ilişkin sorumluluklar ilgili prosedürler çerçevesinde tanımlanır ve bu alandaki gerekliliklerin yerine getirilmesi Bilgi Sistemleri Güvenliği Sorumlusu tarafından gözetilir.

10. DIŞ KAYNAKLI BİLGİ SİSTEMİ HİZMETLERİ YÖNETİMİ

Ford Otosan, bilgi sistemleri kapsamındaki dış kaynak kullanımı süreçlerinde nihai sorumluluğun ve karar alma yetkisinin kendisinde olduğunu garanti edecek şekilde gerekli yönetsel ve teknik tedbirleri alır.

Dış hizmet alınacak kuruluşlar ile sözleşme yapılmadan önce; aday hizmet sağlayıcının teknik altyapısı, mali yeterliliği, bilgi güvenliği kontrolleri, insan kaynağı ve sektörel tecrübesi değerlendirilerek bir teknik yeterlilik raporu hazırlanır ve Üst Yönetim'in onayına sunulur.

Üst Yönetim, dış kaynaklı kritik hizmetlerin performansını, güvenilirliğini, güvenlik seviyesini ve iş sürekliliğini izlemek üzere yeterli bilgi ve tecrübeye sahip sorumlular görevlendirir. Bu sorumlular yılda en az bir kez değerlendirme raporu hazırlayarak Üst Yönetim'e raporlama yapar.

Dış kaynak hizmet sözleşmeleri asgari olarak Tebliğ'in 19/3 maddesinde belirtilen unsurları içerecek şekilde düzenlenir.

Dış kaynaklı hizmetlerin konusuna göre veri mahremiyeti, mevzuat uyumu ve iş sürekliliği gereksinimleri göz önünde bulundurularak gerekli güvenlik kontrolleri sağlanır.

11. İŞ SÜREKLİLİĞİ VE FELAKET KURTARMA YÖNETİMİ

Ford Otosan; bilgi sistemlerinin kesintisiz ve güvenli şekilde hizmet vermesini sağlamak üzere iş sürekliliği ve felaket kurtarma planları oluşturur, güncel tutar ve uygulanmasını temin eder.

Birincil ve ikincil bilgi sistemleri altyapıları, doğal afetler ve çevresel felaketler başta olmak üzere aynı risklere eşzamanlı maruz kalmayacak şekilde konumlandırılır ve gerekli coğrafi ayrışma sağlanır.

Kritik bilgi sistemlerinin felaket durumlarında yedek altyapı üzerinden çalıştırılabilirliğini doğrulamak üzere yılda en az bir kez (gerektiğinde daha sık) Felaket Kurtarma Testleri yapılır. Testlere ilişkin:

- Test tarihi ve kapsamı
- Katılımcılar
- Uygulama sonuçları

- Tespit edilen iyileştirme alanları

kayıt altına alınır ve Üst Yönetim'e raporlanır.

Test sonuçları doğrultusunda iş sürekliliği ve felaket kurtarma planları gerek görüldüğünde revize edilir ve yeni riskler doğrultusunda sürekli iyileştirilir.

12. VERİ MERKEZİ VE SİSTEM BARINDIRMA YÖNETİMİ

Ford Otosan bünyesinde kullanılan bilgi sistemlerinin birincil ve ikincil altyapıları, iş sürekliliği ve bilgi güvenliği gereklilikleri dikkate alınarak konumlandırılır; bilgi sistemleri sürekliliğine ilişkin planlama ve uygulamalar Tebliğ'in 6 ve 27'nci maddeleri kapsamında yürütülür.

VII-128.10 sayılı Sermaye Piyasası Kurulu Bilgi Sistemleri Yönetimine İlişkin Usul ve Esaslar Tebliğ uyarınca, halka açık ortaklıklar için bilgi sistemlerinin Türkiye Cumhuriyeti sınırları içerisinde barındırılması zorunluluğu bulunmamaktadır. Bu kapsamda Ford Otosan, operasyonel ihtiyaçları doğrultusunda yurt içi veya yurt dışı veri merkezi, co-location veya bulut hizmeti kullanımına yetkilidir.

Veri işleme ve depolama faaliyetlerinde; erişilebilirlik, güvenlik, uyum, kararlılık, veri bütünlüğü ve kişisel verilerin korunması gereklilikleri esas alınır. Yurt dışında hizmet alınan durumlarda; veri güvenliği, uyum, iş sürekliliği ve felaket kurtarma tedbirleri ilgili prosedürler doğrultusunda tesis edilir ve düzenli olarak gözetilir.

13. STANDARTLAR

Ford Otosan Bilgi ve Siber Güvenliği Kontrol Standartları dokümanı, bilgi güvenliği süreç, politika, prosedür ve standartları kapsamaktadır.

14. 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** ile Tebliğ'in 18. Maddesinin üçüncü fıkrası uyarınca 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.

15. DENETİM

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

16. POLİTİKA'NIN GÜNCELLENMESİ VE DUYURULMASI

İşbu Politika'nın değişen ihtiyaç ve mevzuata göre güncellenmesinden *Dijital Ürünler ve Servisler Liderliği* sorumludur. Politika yılda en az bir kere gözden geçirilir ve gerekli hallerde güncellenir. Politika'nın güncel versiyonu çalışanlara ilan edilir. Şirket portalında ve Şirket kurumsal web sitesinde erişime açık hale getirilir.

17. YÜRÜRLÜK

İlk olarak 11.09.2013 tarihinde yürürlüğe giren işbu Bilgi Güvenliği Politikası, değişen ihtiyaçlar ve mevzuat doğrultusunda revize edilerek 22.03.2021 tarihinde Yönetim Kurulu tarafından onaylanmış ve güncellenmiştir.

Politika, son olarak 30.12.2025 tarihli ve 2025/33 sayılı Yönetim Kurulu kararı ile yeniden güncellenmiş olup, bu tarih itibarıyla yürürlüğe girerek önceki tüm versiyonların yerine geçmiştir.

Revizyon	**Tarih**	**Açıklama**
1	22.03.2021	Güncelleme
2	30.12.2025	Güncelleme