BİLGİ GÜVENLİĞİ POLİTİKASI

1. Açıklama

Bilgi Güvenliği Politikasının amacı, TürkTraktör'ün işlettiği sistem, bilgi ve varlıkların gizlilik, bütünlük ve erişilebilirliği için ihtiyaç duyduğu gereksinimleri tanımlamaktadır.

Bilgi Güvenliği Politikası, halka açık şirketler için Sermaye Piyasası Kurulu tarafından yürürlüğe konan VII-128.9 Bilgi Sistemleri Yönetimi Tebliği (Tebliğ) ve konuyla ilgili Kişisel Verilerin Korunması Kanunu ve diğer düzenlemeler dikkate alınarak hazırlanmıştır.

1.1. Bilgi Güvenlik Yönetim Sistemi (BGYS)

Bilgi varlıklarının siber saldırılardan korunmasına yönelik politika, prosedür, organizasyon vb. güvenlik kontrollerini sağlamak için "Bilgi Güvenliği Yönetimi Sistemi" tasarlanmıştır.

Bilgi Güvenlik Yönetim Sistemi; güvenlik stratejisinin belirlenmesi, güvenlik politikalarının oluşturulması ve uygulanması, güvenlik sistemlerinin kurulumu, yönetimi ve izlenmesi süreç ve operasyonlarını içerir.

1.2 Üst Yönetimin Katılımı

Sahip olunan bilgi varlıkları; bilgiyi üretme, işleme ve sunma imkânları ile birlikte TürkTraktör'ün en önemli değerleridir.TürkTraktör, kurumsal işlevlerini yerine getirmek için birçok bilgiye ve bilgi varlıklarına gereksinim duymaktadır.

TürkTraktör Bilgi Güvenliği Politikasının ana ilkesi:

TürkTraktör'ün ihtiyaç duyduğu her türlü bilginin "GÜVENLİ, ERİŞİLEBİLİR, SÜREKLİ ve DOĞRU olmasını sağlamak"tır.

Ana ilkemize ulaşmak için:

- Bilgiye kontrolsüz erişimin engellenmesi, kişisel ve kurumsal iletişim ile üçüncü taraflarla yapılan bilgi alışverişlerinde kuruma ait bilginin gizliliğinin sağlanması,

- Sürekli ve düzenli gözden geçirme ile sistemlerin erişilebilirliğinin, bütünlüğünün ve devamlılığının kontrol edilmesi ve iyileştirilmesi,
- İş süreçlerine ve bilgi varlıklarına yönelik risklerin tespit edilmesi, gerekli iyileştirme faaliyetlerinin yapılması ve bunların düzenli olarak gözden geçirilmesinin sağlanması,
- Çalışanlarımızın bilgi güvenliği konusunda farkındalık eğitimleri ile bilinçlendirilmesinin sağlanması,
- Bilgi Teknolojileri alt yapı ve uygulamalarında iş sürekliliğini destekleyecek hizmetlerin oluşturulması ve devamlılığının sağlanması,
- İç ve dış (Bayi, Servis, Tedarikçi) müşteriye sunulan hizmetlerin kalitesinin en yüksekte tutulmasının sağlanması,
- Bilgi güvenliği ihlal olaylarının raporlanması, ihlalleri engelleyecek önlemlerin alınarak kurumsal öğrenmenin sağlanması,
- Yasalar ve regülasyonlar çerçevesinde bilginin üretilmesi ve erişiminin sağlanması,

hedefimizdir.

Amaçlar:

- Faaliyetlerinin, bu doküman ve bu dokümanda belirtilen prosedür ve talimatlar çerçevesinde yürütülmesini ve periyodik gözden geçirme ile daha iyiye götürülmesini,
- Bilgi Teknolojileri ve ilişkili süreçlere destek veren Uygulamalar, Ekipmanlar, Yazılımlar, sunulan Hizmetler ve Sistemlerin bilgi güvenliği bakış açısı altında sürekliliğinin ve sürdürülebilirliğinin sağlanmasını,
- Bünyelerinde veya faaliyetlerinde kullanılan iş süreçlerinin, Gizlilik – Bütünlük – Kullanılabilirlik değerleri göz önünde bulundurularak önem değerine tabi tutulması ve bu çerçevede yönetilmesini,
- İş Süreçlerine ve varlıklarına yönelik her türlü riskin belirlenmesi ve bu risklerin, kabul edilebilir seviyede tutulmasını,
- TürkTraktör “Entegre Yönetim Sistemi Politikası” ve kurallarına uyumluluk sağlanmasını,

- "Türkiye Cumhuriyeti Yasalarına ve buna bağlı yönetmeliklere, sözleşmelerden kaynaklanan gereksinimlere uyumluluk sağlanmasını;
- "TS.ISO.IEC.27001" e uyumluluk sağlanmasını,
- "TS.ISO.IEC.27001" sertifikasının korunmasını amaç edinmiştir.

Bu amaçların gerçekleştirilebilmesi için ortaya çıkan gereksinimleri karşılamak ve bilgi güvenliğini yönlendirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ile sürekli olarak iyileştirmek için Bilgi Güvenliği Komitesi tesis edilmiş ve Bilgi Güvenliği Yöneticisi atanmıştır.

TürkTraktör yönetimi olarak,

"Bilgi Güvenliği Politikası"nın uygulanmasının sağlanması, kontrolünün yapılması, güvenlik riskleri değerlendirilmesi ve gerekli önlemlerin alınması, devamlılığını sağlamak için gerekli kaynaklar sağlanması, sistemin sürekli gelişmesi ve güvenlik ihlallerinde gerekli yaptırımın icra edilmesi yakından takip edilmekte ve desteklenmektedir.

2. Kapsam

Bu politikanın kapsamına aşağıdakiler dahildir:

- Tüm TürkTraktör lokasyonları
- Tüm TürkTraktör çalışanları ve TürkTraktör için çalışan üçüncü taraflar
- Tüm TürkTraktör ağı ve bilişim sistemleri
- TürkTraktör tarafından işlenen, saklanan ve paylaşılan tüm kişisel veriler
- TürkTraktör'ün sahip olduğu tüm bilgi varlıkları
- Tüm TürkTraktör süreçleri
- ISO 27001 belge kapsamında tüm birimler

3. Sorumlular

Yönetim Kurulu ve Üst Yönetim:

Yönetim Kurulu etkili bir bilgi güvenliği yönetim yapısının tesis edilmesi amacıyla, bilgi güvenliği stratejisi ve yol haritasının belirlendiği Bilgi Güvenliği Politikasını onaylar ve uygulanmasını zorunlu tutar. Politika kapsamında hazırlanması gereken tüm standart, prosedür ve talimatların onaylanması için Yönetim Kurulu tarafından, CFO ve Mali İşler Direktörü'nden oluşan Üst Yönetim yetkilendirilmiştir. Üst Yönetim, Bilgi Güvenliği Yönetim Sistemi'nin kurulması ve işletilmesi için gerekli kaynak ve yetki / sorumluluk tahsislerini gerçekleştirir.

Bilgi Güvenliği Komitesi:

Bilgi Güvenliği Komitesi, Bilgi Güvenliği Politikası altında belirlenen bilgi güvenliği standartları ve stratejisi hedefinde ilgili bilgi güvenliği süreçlerini tasarlar, prosedür ve talimatları onaylar ve yayınlar. Bilgi güvenliği gereksinimlerinin yerine getirilmesi sürecini yürütür ve gerekli yatırımları yapar. Bilgi Güvenliği Komitesi, bilgi güvenliği konularında Üst Yönetime karşı sorumludur.

Bilgi Güvenliği Yöneticisi:

TürkTraktör'ün bilgi güvenliği süreçlerini Bilgi Güvenliği Politikasına uygun olarak tasarlar ve yönetir. Bilgi Güvenliği Yönetim Sistemi için gerekli faaliyetleri ve dokümantasyonu yapar veya iş sorumlularından yapılmasını talep eder. Bilgi Güvenliği denetimleri gerçekleştirir veya dış kaynak firmalarının gerçekleştirmesini sağlar. BT Güvenlik Kurulu'nun karar verebilmesi için gerekli girdileri sağlar (Bilgi Güvenliği Denetim Raporları, Bildirilen Vakalar, Risk Analizi Raporları, Sızma Testi Raporları, vb.).
Tüm Çalışanlar:

Bilgi Güvenliği Yönetim Sistemi kategorisinde yayınlanmış tüm politika ve prosedürlere uymakla ve Bilgi Güvenliği Komitesi tarafından talep edilen tüm faaliyetleri gerçekleştirmekle yükümlüdür.

3.1 Bilgi Güvenliği Komitesi

Bilgi Güvenliği Komitesi, Üst Yönetim tarafından belirlenen bir başkan ve Bilgi Teknolojileri, Bilgi Güvenliği, Hukuk, İnsan Kaynakları ve diğer birim sorumlularının bulunduğu üyelerden oluşur. Komite üyeleri e-posta yolu ile tüm kullanıcılara bildirilir. Bilgi Güvenliği Komitesi Başkanı aynı zamanda KVK Komitesi üyesidir.

Bilgi Güvenliği Komitesi'nin rol ve sorumlulukları aşağıdaki gibidir:

- Bilgi Güvenliği Yönetim Sistemi kapsamında korunan ve kullanılan bilgilerin güvenliğini kontrol etmek.
- Bilgi Güvenliği Yönetim Sistemi faaliyetlerini geliştirmek için gerekli kaynakları ayırmak, rol ve sorumlulukların atamasını yapmak.
- Bilgi Güvenliği Yönetim Sistemi kapsamındaki süreçleri şekillendiren ve bilgi güvenliği yönetim sisteminin verimli şekilde çalışmasını sağlayan uygulanabilir politika ve süreçlerin kurallarını oluşturmak, var olanların revizyonu ve bunların dokümante edilmesi için alt gruplarını oluşturmak.
- 6698 sayılı Kişisel Verilerin Korunması Kanunu ve bilgi güvenliği yönetim sisteminin bilgi ve veri güvenliği ile ilgili mevzuata uyumlu bir şekilde yönetilmesini ve uyumluluğunun sürdürülmesini sağlamak.
- Bilgi Güvenliği Yönetim Sistemi kapsamındaki tüm faaliyetleri ve bilgiyi tehlikeye atacak, şirket imajını zedeleyecek her türlü davranışın, şirket içi uygun disiplin kuralları ile kontrol etmek.
- TürkTraktör'de acil durumlarda ve önemli güvenlik ihlallerinde, güvenlik tedbiri belirlemek ve tekrarlanmaması için gerekli önlemleri almak ve alınan önlemleri gözden geçirmek.
- Bilgi güvenliği ile alakalı oluşacak adli olaylarda ilgili kamu kuruluşları ile olan ilşkileri (endüstri casusluğu, sistem kırma faaliyetleri, bilgi sızdırma, bilgi koruma akdine uymama vb.) Bilgi Güvenliği Komitesi ile şirket avukatı tarafından koordineli olarak yürütmek.
- Gündemin yeterliliğine veya gündemin acilliğine göre yılda en az bir kez olacak şekilde düzenli toplanmak, gözden geçirme yapmak. Politika, yasalar, süreçlerdeki aksak noktalar ve dokümanları tekrar gözden geçirmek ve

gerekiyor ise ilgili politika, prosedür, talimat vb. dokümanlara değişiklikleri yansıtmak, süreçlerin güncelliğini takip etmek, iyileştirmeleri uyarlamak ve önerileri değerlendirmek.

- Bilgi güvenliği risk değerlendirme ve sızma testi raporlarını, aksiyon planlarını, güvenlik kontrollerini gözden geçirmek ve bilgi güvenliği risk yönetimi faaliyetleri ve artık risklerin kabulünü gerçekleştirmek.
- Bilgi güvenliği ve ISO 27001'e uyumu kontrol edebilmek amacı ile en az yılda bir kez iç ve dış denetim yaptırmak ve denetim sonuçlarına göre verilecek kararları sistemlere ve süreçlere uygulamak.
- Kişisel Verilerin Korunması Kurulu ile istişarede bulunmak ve Kurul'un aldığı kararlar doğrultusunda Bilgi Güvenliği Politika, Prosedür ve Uygulamalarında gerekli güncelleme ve değişiklikleri yapmak.
- Üst Yönetimi Bilgi Güvenliği Yönetim Sisteminde gerçekleştirilen faaliyetler ve önemli güvenlik konuları hakkında bilgilendirmek.
- Bilgi güvenliğinin kurumsal olarak yaygınlaşmasını sağlamak için gerekli görev ve sorumlulukları delege etmek.

3.2 Bilgi Güvenliği Yöneticisi

TürkTraktör Bilgi Güvenliği Yöneticisinin sorumlulukları aşağıdaki gibidir:

- Bilgi güvenliği farkındalık eğitimlerinin etkinliğini ölçmek ve sonuçlarını değerlendirmek.
- TürkTraktör Bilgi Güvenliği Politikası, Standartları ve Prosedürlerini gözden geçirmek ve gerekli değişiklikler için önerilerde bulunmak.
- Bilgi güvenliği ihlal olaylarını raporlamak, ihlalleri engelleyecek önlemleri alarak kurumsal öğrenmeyi sağlamak.
- Belirlenen kritik kontrollerin uygulanmasını sağlamak
- İlgili otorite ve çalışma grupları ile iletişim ve koordinasyonun sağlamak.
- Dış taraflara karşı kurumu temsil etmek ve ilgili faaliyetlerde koordinasyonu sağlamak.
- Bilgi Güvenliği Komitesi'ne katılım sağlayarak çalışmalar hakkında kurulu bilgilendirmek.

- Bilgi Güvenliği Politika ve Prosedürlerini, Bilgi Güvenliği Komitesi'ne gözden geçirilmesi ve onaylanması için sunmak.
- KVK Komite üyesi olmak.

3.3. TürkTraktör Çalışanları

TürkTraktör çalışanlarının rol ve sorumlulukları aşağıdaki gibidir:

- Kendilerine duyurulan Bilgi Güvenliği Politikasına ve Prosedürlerine uymak.
- Kendi süreç ve sistemlerinin yönetimleri için oluşturacakları süreç, akış, talimat, kılavuz, form gibi dokümanlarda Bilgi Güvenliği dokümanlarına uyumu sağlamak.
- Bilgi Güvenliği Politikalarına ve/veya Prosedürlerine uyumun sağlanmadığı veya bilgi güvenliği ihlal olaylarını bilgiguvenligi@turktraktor.com.tr adresine bildirmek
- TürkTraktör bilgi sistemlerinin çalışmasını olumsuz etkileyebilecek veya bilgi güvenliğini tehlikeye atacak faaliyetlerde bulunmamak.
- Bilgi Güvenliği dokümanları ile ilgili güncelleme/iyileştirme taleplerini Bilgi Güvenliği Yöneticisine bildirmek.
- Bilgi ve kurumsal kaynaklarına iş ihtiyaçları ölçüsünde erişim talebinde bulunmak.

3.4 TürkTraktör Yöneticileri

TürkTraktör Yöneticileri rol ve sorumlulukları aşağıdaki gibidir:

- Bilgi Güvenliği politika ve prosedürlerine uymak ve ekibi içerisinde uyumu sağlamak üzere gerekli aksiyonların koordinasyonunu ve takibini gerçekleştirmek.
- Kendilerine bağlı çalışanlarının sistem ve uygulama yetkilerini 6 ayda bir gözden geçirmek ve iş ihtiyacı dışında olan yetkilerin iptalini sağlamak.
- Kişisel Verilere erişimleri, Birim Sorumluları ile birlikte düzenli olarak kontrol etmek ve/veya edilmesini sağlamak

- Kendilerine bağlı çalışanların nakil, terfi ve ayrılmalarında bilgi erişim yetkilerini gözden geçirmek ve ihtiyaç kalmayan yetkilerin iptal edilmesini sağlamak.

3.5 Varlık Sahipleri ve Süreç Sahipleri

Varlık Sahiplerinin ve Süreç Sahiplerinin rol ve sorumlulukları aşağıdaki gibidir:

- Sahibi olunan varlığın ve Kişisel Verilerin, erişim haklarını ve kimlerin yönetici ve kullanıcı bazında hangi ayrıcalıkla erişilebileceğini tayin etmek.
- Varlık envanterini gözlemlemek ve güncelliğini sağlamak.
- Sahibi olunan varlıkların ve/veya Kişisel Verilerin gizlilik sınıflarını KVK Komitesi ve Birim Sorumluları ile birlikte tayin etmek, gizlilik sınıfı değişen varlıkları güncellemek ve KVK Komitesine'nin onayına sunmak.

3.6 Üçüncü Partiler

Şirket'e mal ve hizmet sağlayan üçüncü kişilerin ve çalışanlarının uyması gereken bilgi güvenliğine ilişkin düzenlemeler ilgili sözleşmeler ve güvenlik protokolleri ile belirlenir. Bunlar asgari aşağıdaki hususları kapsar:

- Sözleşmeler veya protokoller ile bildirilen bilgi güvenliği kuralları başta olmak üzere üçüncü taraflarla ilişkileri düzenleyen TürkTraktör Politika ve Prosedürleri'ne uygun hareket etmek.
- TürkTraktör'e ait bilgi ve varlıkları TürkTraktör'ün onayı ve izni olmadan başkaları ile paylaşmamak.
- TürkTraktör tarafından kendilerine verilen kimlikleri mukavelelere ve talimatlara uygun şekilde kullanmak.
- Üçüncü partinin TürkTraktör'de çalışmakta olan çalışanlarının kendi firmasından ayrılması/görev değiştirmesi söz konusu ise, bu durumu aynı gün içerisinde TürkTraktör'e bildirmek ve yetkilerinin iptal olmasını sağlamak.

- TürkTraktör'ün onay ve izni olmadan, TürkTraktör'e ait cihazlardaki her türlü veri ve yazılımı kopyalamak, ortamın resmini/videosunu çekmek.
- TürkTraktör'ün veri güvenliğini veya imajını tehlikeye atabilecek paylaşımlarda/hareketlerde bulunmamak.
- TürkTraktör lokasyonunda yapılacak sistem erişimlerini Bilgi Teknolojileri ekibi gözetiminde gerçekleştirmek.

4. Standartlar

Aşağıda yer alan maddeler TürkTraktör'ün Bilgi Güvenliği hususundaki üst seviye politikaları olup, bu maddeleri desteklemesi amacı ile oluşturulan diğer bütün bilgi güvenliği politikalarına ve prosedürlere de ilgili taraflarca uyulması gerekmektedir.

4.1. Erişim Kontrolü

4.1.1. Her türlü bilgi, Kişisel Veri ve kurumsal kaynaklara erişim/bağlantı yetkileri, "gerekli olan en az yetki" prensibine göre verilir.

4.1.2. Erişim/bağlantı yetkileri ve sorumluluklar, "görevler ayrılığı ilkesine" göre verilir.

4.1.3. Erişim/bağlantı yetkileri belirlenirken, Kişisel Veri Envanteri ile belirlenen veri işleme amaçları dahilinde Kişisel Veri Saklama ve İmha Politikası'na ve Erişim Kontrol Prosedürüne uygun olarak ilgili kullanıcıların ilgili verilere erişmesi amaçlanır.

4.1.4. Kaynaklara erişim özellikle tahsis edilmediği sürece, yasak olarak kabul edilir.

4.1.5. Varlık Sahipleri kullanıcıların erişim haklarını düzenli aralıklarla gözden geçirir.

4.1.6. Her kullanıcı kendi kimlik doğrulama bilgilerinin korunmasından sorumludur. Erişim bilgileri kişiye özeldir ve paylaşılmaz.

4.1.7. Her erişim için kişisel bir kullanıcı hesabı yaratılması ve hesabın doğrulanması için bir parola (şifre) olması gerekir.

4.1.8. Her parola (şifre) için bir geçerlilik tarihi olması zorunludur.

4.1.9. Tüm bilgisayar ve cihazlar belirli bir süre kullanılmadığında parola ile kilitlenerek koruma altına alınır.

4.1.10. Karmaşıklığı, parola geçmişi ve şifre değiştirme gereksinimlerini karşılamak için güçlü parolalar kullanılır ve parola ilkeleri uygulanır.

4.1.11. Sistem yönetim hesaplarına (örneğin; root, etkinleştirme, NT admin, uygulama yönetim hesapları vb.) ait parolalar (şifreler) en fazla üç ayda bir değiştirilir.

4.2. Kriptografi

4.2.1. Aktarılan ve depolanan veriler üzerinde kriptografik kontrollere ihtiyaç olup olmadığı ve ihtiyacın seviyesi; şifreleme algoritmasının türü, gücü ve kalitesi risk analizi ile belirlenir.

4.2.2. Taşınabilir bilgisayar ve cihazlardaki disk şifreleme yapılır.

4.2.3. Kullanılan kriptografik anahtarların güvenli yaşam döngüsü belirlenir ve buna göre yönetilir.

4.3. Fiziksel ve Çevresel Güvenlik

4.3.1. Bilgi sistemlerini barındıran alanları korumak için; güvenlik sınırları belirlenir ve bu alanlarda taşıdığı riskle doğru orantılı olarak fiziksel güvenlik tesis edilir.

4.3.2. Güvenlik önlemleri alınırken doğal felaketler, kötü niyetli saldırılar ve kazalar göz önünde bulundurulur.

4.3.3. Basılı dokümanlar ve taşınabilir depolama ortamlarının yönetimi Fiziksel ve Çevresel Güvenlik Talimatına göre yapılır.

4.3.4. Giriş çıkış kapıları, ofis odaları ve ürün teslim alma/verme alanları (depolar, giriş kapıları vb.) güvenli konuma getirilir ve Fiziksel ve Çevresel Güvenlik Talimatına uygun hareket edilir.

4.4. İşletim Güvenliği

4.4.1. Kritik süreç ve sistemlere ait güvenli işletim konfigürasyon kuralları yazılı hale getirilir ve düzenli olarak güncellenir.

4.4.2. Bilgi güvenliğini etkileyen önemli değişiklikler gerçekleştirilmeden önce planlanır, onaylanır, test edilir ve kayıt altına alınır.

4.4.3. Zararlı kodlardan ve teknik güvenlik açıklıklarından kaynaklı veri kaybı yaşamamak için yıllık olarak ağ, uygulama ve sistem seviyelerinde zafiyet taraması ve sızma testleri gerçekleştirilir. Bununla beraber anti-virüs yazılımları kullanılır. Bu yazılımlarla düzenli olarak tarama gerçekleştirilir.

4.4.4. Veri kaybını en aza indirmek ve/veya tamamen önlemek için yedekleme mekanizmaları kullanılır ve bu yedek verilerin bütünlüğü düzenli olarak test edilir. Yedekleme ihtiyaçları iş etki analizi ile belirlenir.

4.4.5. Sistemler üzerinde gerçekleştirilen önemli değişikliklerin denetlenebilmesi ve izlenebilmesi için gerekli loglar belirlenen süre ile saklanır ve bütünlüğü güvence altına alınır. Gizli veya Hassas /Kişisel Veri içeren sistemlere erişimler ve erişim kurallarında yapılan değişikliklerin fark edilmesi için gerekli altyapı ve yapılandırma tesis edilir.

4.5. Haberleşme Güvenliği

4.5.1. Kurumsal ağ üzerinde bulunan sistemler kritiklik seviyesi ve erişim ihtiyacına göre bölümlenir ve bu bölümler uygun güvenlik önlemleri ile birbirinden yalıtılır.

4.5.2. Kurumsal ağ uygun donanım ve yazılım kullanılarak koruma altına alınır ve kurumsal ağ trafiği izlenir.

4.5.3. Bilgilerin elektronik ortamda transferi esnasında gizlilik sınıfına uygun güvenlik ihtiyaçları sağlanır.

4.5.4. Halka açık mekânlarda, resmi konferanslarda sunum veya tanıtım yapılacak ya da TürkTraktör ile ilgili bir bilgi, resim vb, fotoğraf, video vb. paylaşılacak ise Kurumsal İletişim Müdürlüğü'nden onay alınır.

4.5.5. Kişisel Verilerin üçüncü taraflarla paylaşılmasında başta KVK Kanunu hükümleri olmak üzere, TürkTraktör Kişisel Verilerin Korunması ve İşlenmesi Politikasında belirlenen esaslara uygun hareket edilir.

4.6. Sistem Temini, Geliştirme ve Bakımı

4.6.1. Bilgi güvenliğini ilgilendiren bütün projelerde Bilgi Güvenliği Yöneticisinin, Bilgi Güvenliği Komitesi Başkanının ve gerekli durumlarda KVK Komitesi'nin görüşü alınır. Buna ek olarak, kritik önem arz eden projeler ise Üst Yönetim tarafından gözden geçirilir ve bunlara ilişkin risklerin yönetilebilirliği göz önünde bulundurularak onaylanır.

4.6.2. Bütün sistem geliştirme faaliyetleri Yazılım Geliştirme Prosedürü 'ne uygun olarak yapılır.

4.6.3. Geliştirme, test ve işletim ortamları iş verileri ve işletim yazılımlarına yetkisiz erişimi engellemek veya kazara değiştirme riskini azaltmak için ayrılır.

4.7. Üçüncü Parti İlişkileri

4.7.1. Tüm Üçüncü Parti'ler, TürkTraktör 'ün uymakla zorunlu olduğu yasa ve yönetmelik kurallarına uygun hizmet verirler.

4.7.2. TürkTraktör 'ün bilgi varlıklarına erişim hakkı olan üçüncü partilerin uyması gereken kurallar imzalanan sözleşme içerisinde tanımlanmıştır.

4.7.3. Kişisel Verilerin paylaşılmasında işbu politikanın 4.5.5 maddesindeki düzenlemelere uygun olarak gerekli aksiyonlar alınır.

4.7.4. TürkTraktör ağına bağlanacak tüm firmalar ile KVK Kanunu'na uyum için gerekli hükümleri de içeren maddeler üçüncü taraflarla yapılan sözleşmelere eklenmektedir.

4.8. Bilgi Güvenliği İhlal Olayı Yönetimi

4.8.1. Tüm bilgi güvenlik ihlallerini bilgiguvenligi@turktraktor.com.tr adresini kullanarak bildirilir. Bilgi Güvenliği Komitesi, bu güvenlik ihlallerinin gelecekte tekrar oluşmaması ve

kısa zamanda çözümlenmesi için gerekli tedbirleri alır veya ilgili paydaşları yönlendirerek gerekli tedbirlerin alınmasını sağlar.

4.8.2. Bilgi güvenliği ihlal olaylarına müdahale Olay Yönetimi Prosedürüne göre gerçekleştirilir.

4.8.3. Bilgi güvenliği ihlal olaylarının analizi ve çözümlemesinden kazanılan bilgi birikimi kullanılarak, gelecekteki ihlal olaylarının gerçekleşme olasılığını veya etkilerini azaltmak için gerekli aksiyonlar alınır.

4.8.4. Bilgi güvenliği ihlal olaylarının yönetimi için güvenlik olayları ve açıklıkları üzerindeki bağlantısını içeren, tutarlı ve etkili bir yaklaşımın sağlanması amacı ile yönetim sorumlulukları ve prosedürler belirlenir.

4.8.5. bilgiguvenligi@turktraktor.com.tr adresine iletilen Kişisel Veri güvenlik ihlal olayları derhal KVK Komitesi'ne iletilir.

4.9. Uyum

4.9.1. Yasal, meşru, düzenleyici veya sözleşmeye tabi yükümlülüklere ve her türlü güvenlik gereksinimlerine ilişkin ihlalleri önlemek adına gerekli özel kontroller ve bireysel sorumlulukları karşılayan gereksinimler yazılı olarak saklanır ve güncelliği takip edilir.

4.9.2. Kişisel Veri güvenliğine ilişkin alınacak her türlü teknik ve idari tedbirler hususunda, KVK Kanunu'nun ilgili hükümleri ve bu kapsamda yayımlanan ikincil düzenlemelere uygun hareket edilir.

4.9.3. Fikri mülkiyet hakları ve tescilli yazılım ürünlerinin kullanımı üzerindeki yasal, düzenleyici ve anlaşmalardan doğan gereksinimlere uyum sağlamak için TürkTraktör Bilgi Güvenliği Komitesinin onaylamadığı ve/veya lisanssız yazılımlar kullanılmaz.

4.9.4. T.C. Devleti kanunlarının tanımladığı tüm yasal hükümler bu politikanın üzerindedir ve yasal hükümler ile çelişen herhangi bir madde olduğunda yasal hükümler geçerlidir ve uyum zorunludur.

4.10. Kişisel Verilerin Korunması

Bilgi Güvenliği Politika ve Prosedürlerinin Kişisel Verilerin Korunması ve İşlenmesi 'ne ilişkin tüm teknik ve idari tedbirleri KVK Kanunu Hükümlerine ve Kişisel Verilerin Korunması ve İşlenmesi Politikasına uygun olarak yürütülür, KVK Komitesi ile birlikte çalışılır.

5. Bilgi Güvenliği Dokümanlarına Erişim

Bilgi güvenliğini oluşturan politika ve prosedürlerin güncel ve geçerli sürümleri, Doküman Yönetim Sistemi uygulaması üzerinde erişilebilir haldedir.

Herhangi bir kaydedilmiş / basılı hale getirilmiş belgenin güncelliğinden emin olunmadığı durumlarda, Doküman Yönetim Sistemi uygulaması üzerindeki bilgilere başvurulmalıdır.

6. Denetim

Bilgi Güvenliği Yöneticisi, bilgi güvenliğine ve Kişisel Verilerin korunmasına ilişkin süreçleri denetleme hak ve sorumluluğuna sahiptir. Denetleme veya bildirimler sonucunda tespit edilen olay ve bulgular değerlendirilir.

TürkTraktör çalışanlarının bu politikaya aykırı kasti ve kasıtsız davranışları, yol açtığı olumsuz sonuç ile birlikte değerlendirilir ve sorumluluğu saptananlar Personel Yönetmeliği çerçevesinde uygun görüldüğü şekilde disiplin süreçlerine tabii tutulur.

7. Yaptırım

Diğer Bilgi Güvenlik Yönetim Sistemi dokümanları bu politika ile tutarlı olmalıdır. Aksi durumlarda bu politika geçerli olacaktır. Bilgi Güvenliği Politikasının ve diğer Bilgi Güvenliği Yönetim Sistemi dokümanlarının içerisindeki yöntemlerin ihlal edildiği hallerde, Etik Davranış Kuralları ve Disiplin Hükümleri çerçevesinde gerekli işlemler yürütülür.