KVKK_P1

BİLGİ GÜVENLİĞİ VE KİŞİSEL VERİLER ÇERÇEVE POLİTİKASI

AED

ARES
ECZA DEPOSU

ARES ECZA DEPOSU TİCARET LİMİTED ŞİRKETİ

BİLGİ GÜVENLİĞİ VE KİŞİSEL VERİLER ÇERÇEVE POLİTİKASI

1. GİRİŞ VE AMAÇ

1.1. İşbu belge künyesi aşağıda detaylı olarak verilen ARES Ecza Deposu Ticaret Limited Şirketi'nin Bilgi Güvenliği Ve Kişisel Veriler Çerçeve Politikası (bundan böyle Çerçeve Politika olarak anılacaktır) ortaya koymak amacıyla kaleme alınmıştır.

Veri Sorumlusu : ARES ECZA DEPOSU TİCARET LİMİTED ŞİRKETİ
Adres : OSTİM OSB MAH. 243.CAD NO:7 Yenimahalle/Ankara, Türkiye
Telefon : +90 312 222 30 31
Mail : kvkk@aresecza.com.tr
WEB Sitesi : http://www.aresecza.com.tr/main
Faaliyet Alanı : Eczacılıkla ilgili ürünlerin bir ücret veya sözleşmeye dayalı olarak toptan satışı

Çerçeve, Şirketimizin Bilgi Güvenliği ve Kişisel Verilerin Mahremiyeti hususunda geçerli olan Politikalar, Yönetmelikler, Aydınlatma Metinleri ve kılavuz ilkelerin genel bir değerlendirmesini içermekte olup aynı zamanda Şirketin zikredilen alanlarda eğitim ve farkındalık artırma iradesini ortaya koymayı amaçlamaktadır.

1.2. İşbu Çerçeve Politika Şirketimizin elde ettiği tüm bilgi ve verilerin hukuka uygun, güvenli, etkin ve verimli bir şekilde işlenebilmesi için gerekli ve geçerli olacak koşulları bir araya getirmeyi amaçlamaktadır. Bilgi ve veri işleme Şirketimizin gündelik faaliyetlerinin yürütülmesi ve idaresinin sağlanması açısından hayati bir öneme sahiptir. Şirketin sunduğu hizmetlerin kalitesi, planlanması, performans ölçümü, iş güvenliği, sigorta ve mali yönetimi büyük oranda doğru ve güvenilir bilgi toplama ve işleme süreçlerine bağlıdır. Sağlıklı ve güvenilir bilgi yönetişimi ise açık ve etkili bir yönetim ve hesap verebilirlik, yönetişim süreçleri, belgelenmiş politikalar ve prosedürler, eğitimli personel ve yeterli kaynakların varlığını gerektirmektedir. Bu doğrultuda işbu Çerçeve Politika ile bilgi kaynaklarının yönetimi ve mahremiyeti alanında geçerli olacak şartlar, standartlar ve en iyi uygulamalar ortaya konulacaktır.

1.3. Bilgi Güvenliği Ve Kişisel Verilerin Mahremiyeti Şirketimizin her bir çalışanı için önem arz eden bir sorumluluktur. Her bir çalışan, Şirketin çalışma pratiklerinin uygulanması ve politika ve çalışma kurallarının içselleştirilmesi noktasında görevlidir. Bu nedenle her bir çalışanımızın işbu Çerçeve belgesinde belirtilen hususlar konusunda bilgi sahibi olması elzemdir. İşbu çerçeve belgede vazedilen esaslara Şirket verilerini kullanan üçüncü tarafların da uygun hareket etmesi beklenmektedir.

1.4. İşbu Çerçeve Politikanın amacı şirketimize aşağıda sıralanan sorumluluklarını yerine getirme noktasında yardımcı olmaktır:

- Hukuki, idari ve sözleşmelerden kaynaklanan yükümlülüklere riayet edilmesi;
- Sağlıklı bir kurumsal yönetişimin temin edilmesi;
- Hizmetlerin yüksek kalitede sunulması;
- Şirketin mali kaynaklarının korunması;
- Uygun iş sürekliliği süreçlerinin planlanması;
- Şirketin kontrolünde olan verilerin işlem güvenliğinin devamlılığının sağlanması ve geliştirilmesi.

1.5. Şirket hizmet sunumu, ticari ilişkiler ve taahhütlerin devamlılığının sağlanması ve çalışanların iş güvenliğinin temini için gerekli olan geniş çapta standart ve özel nitelikli kişisel veri toplama ve işleme faaliyetlerini gündelik olarak icra etmektedir.

2. KAPSAM

2.1. İşbu Çerçeve Politika gerek elektronik ortamda gerekse de fiziki ortamda aşağıda örnek olarak sıralanan veriler dâhil olmak üzere Şirketimiz tarafından muhafaza edilen ve Şirket namına veri işleyen taraflarca işlenen tüm veriler için geçerlidir:

- Sabit ya da taşınabilir bilgisayarlar ve depolama araçları tarafından depolanan ve işlenen elektronik veriler;
- Ağlar üzerinden aktarılan veriler;
- Faks ve benzeri aktarım yöntemleri kullanılarak gönderilen bilgiler;
- Her türlü kâğıt ortamında tutulan kayıtlar;
- Mikrofiş ile slayt ve kapalı devre kamera sistem kayıtları dâhil olmak üzere görsel ve fotoğrafik materyaller;
- Yüz yüze iletişim, sesli mesaj ve kaydedilen görüşmeler de dâhil olmak üzere sözlü iletişim verileri.

2.2. Aşağıda sıralanan tarafların işbu Çerçeve belgede vazedilen usul ve esaslara riayet etmesi gerekir:

- Tüm Şirket çalışanları;
- Danışmanlar, hizmet tedarikçileri ve yüklenici firmalar, ziyaretçiler dâhil olmak üzere Şirket verilerine erişim yetkisi verilen tüm üçüncü taraflar.

2.3. İşbu çerçeve belge iki bölümden ibarettir. Birinci Bölümde Şirketimizin Bilgi Güvenliği ve Kişisel Verilerin Mahremiyeti hususunda stratejisi tasvir edilirken ikinci

bölümde bu hususta ilgili paydaşların üstleneceği roller ve sorumlulukları ile bu alanda uygulanacak olan politikalar ve eğitimler açıklanmaktadır.

2.4. Aşağıda Şirketin kontrolünde olan verilerin nasıl tasnif edileceğine dair bilgiler verilmektedir:

(1) 'Kişisel Veri' tanımlanmış veya tanımlanabilir bir gerçek kişiye ilişkin her türlü bilgidir ('veri sahibi'); tanımlanmış bir gerçek kişi özellikle bir isim, kimlik numarası, konum verileri, çevrim içi tanımlayıcı ya da söz konusu gerçek kişinin fiziksel, fizyolojik, genetik, ruhsal, ekonomik, kültürel veya toplumsal kimliğine özgü bir ya da daha fazla sayıda faktöre atıfta bulunularak doğrudan veya dolaylı olarak tanımlanabilen bir kişidir. Kişisel verilerin toplanması, kullanılması ve saklanmasında Şirketin kişisel Verilerin İşlenmesi ve Korunması Politikasında belirtilen usul ve esaslara uyulmalıdır;

(2) Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir. Özel nitelikli kişisel verilerin işlenmesinde güvenliğin artırılması için ek şartlar ve koruma tedbirleri Şirketin kişisel Verilerin İşlenmesi ve Korunması ve Veri Güvenliği Politikalarında belirtilmiştir.

(3) Kişisel verilerin haricinde yer alan aşağıda sıralanan veriler şirketin kurumsal verileri olarak anılacaktır:

(a) Planlama / idari veya araştırma verileri, gizlilik sözleşmeleri ve maddeleri ile korunan yasal olarak ayrıcalıklı bilgiler gibi ticari açıdan hassas olan hassas kurumsal veriler. Bahse konu veriler uygun koruma önlemleri ile korunmalıdır;

(b) Şirket ile ilgili olup kamuya açıklanmamış, özel nitelikli olmayan Bilgi Edinme Kanunu gibi yasal gereklilikler karşısında açıklanabilir olan veriler.

3. AMAÇ

3.1. Şirketimizin kurumsal stratejisinin amacı, Şirket'in müşterileri, işletmeler, ortaklar ve tedarikçilerinin verilerin değeri ve riski dikkate alınarak işlendiğine ve saklandığına dair Şirketimize güven duymalarını sağlamak ve bilgi yönetimi, bilgi güvenliği ve kişisel verilerin mahremiyeti alanında yasal sorumluluklarını yerine getirmesini sağlamaktır. Tüm ilgili tarafların verilerin doğru kullanımı, hukuka uygun olarak toplanması ve işlenmesi ve uygunsuz kullanıma karşı korumanın önemini kavramalıdır.

3.2. İşbu stratejinin hedefi Şirketimizin aşağıda sıralanan konular için geçerli olan hukuki ve etik sorumluluklara uyum içerisinde hareket edebilmesini temin etmektir:

- Belirli veya belirlenebilir kişilere ait verilerin hukuka uygun olarak kullanılması ve güvenliğinin korunması;
- Verilerin yalnızca hukuka uygun olarak verilere erişim sağlaması gereken kişilere aktarılması;
- Bilgi yönetimi için geçerli olacak düzenleyici çerçevenin ihdas edilmesi;
- Kişisel verilerin kaydedilmesi, paylaşılması ve kullanımı için verilecek açık rızanın alınması hususunda davranış kuralları;
- Şirket tarafından kabul edilen profesyonel davranış kuralları ve uygulama direktifleri;
- Üçüncü taraflarla bilgi ve veri teatisi.

3.3. Strateji, şirketin kurumsal kimliğinden beklenen yüksek standartların yanı sıra bilgi yönetimi alanında uygun güvenlik standartlarını muhafaza etme ve Şirket genelinde kişisel veri güvenliği kültürünü tam olarak yerleştirmeyi amaçlamaktadır.

3.4. Şirketin Bilgi Güvenliği ve Kişisel Verilerin Mahremiyeti hususunda Stratejik Hedefleri aşağıda sıralandığı gibidir:

- Bilgi Yönetiminin Şirketin genel stratejisi ve altında yer alan ilgili unsurların stratejileri ve iş dönüştürme programlarını desteklemesi ve bilgi güvenliği pratiklerinin bahse konu strateji ve programların geliştirilmesi ve uygulanması süreçlerinde içkin bir rol oynaması.
- Doğru bilginin doğru kişiye doğru zamanda doğru amaçla ulaştırılması için gerekli alt yapı ve süreçlerin oluşturulması ve etik, hukuka uygun, etkili ve uygun yöntemlerle teslim edilmesi için gerekli alt yapı ve süreçlerin tespit edilmesi;
- İş süreçlerinin dönüştürülmesi göz önünde bulundurularak bilgi yönetişimi hususunda yeniliğe açık çözümlerin geliştirilmesi;
- Bilginin asli bir varlık olarak kabul edilmesi için geniş kapsamlı davranış değişikliklerinin gerçekleştirilmesi suretiyle bilgi yönetişiminin Şirketin idari işleyişinin bir parçası haline getirilmesi;
- Çalışanların yeterlilik ve iş tanımlarına bilgi yönetişimi ile ilgili spesifik koşulların yerleştirilmesi;
- Çalışanların harcanan çabaların tekrarının önlenerek kaynakların daha etkin bir şekilde kullanılabilmesi için birlikte çalışmaya teşvik edilmesi;
- Yasal, idari ve sözleşmelerden kaynaklı yükümlülükler ile ilgili politikalara uyumlu hareket edilebilmesi için geçerli standartların temin edilmesi için çalışılması;
- Şirket bünyesinde bulunan bilgi kaynaklarının tespiti ve yönetilmesi ile bilgi kaynakları için geçerli olan risk ve fırsatların dengelendiği bir bilgi risk yönetimi rejiminin inşası;

- Bilgi kaynaklarının korunması için en iyi uygulama standartlarının tatbik edilmesi için gerekli ve orantılı tedbirlerin uygulanması suretiyle tüm ilgili taraflara güven verilmesi;
- Tüm çalışanlarımız ve ana ortaklarımıza yeterli düzeyde eğitim verilmesi, farkındalık düzeyinin artırılması, Şirket nezdinde işlenen tüm veri ve bilgilerin sorumluluk ve görev bilinci içerisinde ele alınması için uygun bir kültür ortamının yaratılması.

4. ŞİRKETİMİZİN YAKLAŞIMI

4.1. Bilgi Güvenliği ve Kişisel Verilerin Mahremiyeti konusu Şirket faaliyetlerine tüm boyutlarıyla entegre edilmektedir. Bu anlamda şirket operasyonlarının dört ana unsuru göz önünde bulundurulmaktadır:

- Beşeri unsur
- Süreçler
- Bilgi
- Teknoloji

4.2. Bilgi yönetişimi, geliştirme ve koruma faaliyetlerinin bütününde yukarıda sıralanan faktörlerin stratejik hedeflerimize ulaşmamıza nasıl katkıda bulunacağı değerlendirilmektedir.

4.3. Bilgi yönetişimi alanında stratejik hedeflerimize ihdas edilecek politikalar sayesinde ulaşılması planlanmaktadır. Geliştirme Programında her bir bilgi yönetimi projesi tanımlanacak ve işbu Çerçeve belgede açıklanan yaklaşımlar ve yönetim düzenlemeleri ile uyum içerisinde uygulanarak denetlenecektir.

4.4. Bahse konu stratejinin hayata geçirilmesiyle aşağıda sıralanan faydaların elde edilmesi ön görülmektedir:

- Şirket bünyesinde işlenen bilgi ve verilerin tutarlı ve etkin bir şekilde yönetilmesi;
- İlgili mevzuatın daha iyi anlaşılarak ön gördüğü hususlara uyum düzeyinin artırılması;
- Bilgi güvenliği ve kişisel veri mahremiyetini etkileyen olayların yaşanma sıklığının belirgin bir şekilde azaltılması;
- Çalışanların bu konuda harcamak zorunda kaldığı zaman ve çabanın azaltılması;
- Veri kalitesinin artırılması;
- Bilgi Yönetimi ve Güvenliği hususunda üstlenilecek sorumlulukların açık bir şekilde ortaya konulması;
- Bilgi ve veri güvenliğini tehdit eden risklerin etkili bir şekilde yönetilmesi;

4.5. Şirket Genel Müdürü işbu stratejinin yürütülmesinden sorumludur. Kişisel Veri Koruma Komitesi Genel Müdürün Başkanlığında yıl boyunca Geliştirme Programının denetlenmesi ve kat edilen mesafenin raporlanmasından sorumludur. Bilgi Güvenliği ve Kişisel Verilerin Korunması stratejisi kararlaştırılan politikalar, geliştirme programları ve projeleri vasıtasıyla uygulamaya konulacaktır. Her yılın sonunda Kişisel Veri Koruma Komitesi üzerinde anlaşma sağlanan öncelikler ve mevcut kaynaklar temel alınarak müteakip yıl için ön görülen geliştirme programları üzerinde mutabakata varacaktır. Genel Müdür, Kişisel Veri Koruma Komitesi tarafından üzerinde mutabakat sağlanan geliştirme programlarını onaylayacaktır.

4.6. Tanımlar

4.6.1 BGYS: Bilgi Güvenliği Yönetim Sistemi.

4.6.2 Envanter: Firma için önemli olan her türlü bilgi varlığı

4.6.3 Üst Yönetim: Şirket Üst Yönetimidir.

4.6.4 Know-How: Bir şeyi yapabilme yetkinliğidir.

4.6.5 Gizli Bilgi: Bilgi, tüm diğer kurumsal ve ticari varlıklar gibi, bir işletme için değeri olan ve bu nedenle uygun şekilde korunması gereken bir varlıktır. Şirket içerisinde, know-how, süreç, formül, teknik ve yöntem, müşteri kayıtları, pazarlama ve satış bilgileri, personel bilgileri, ticari, sınai ve teknolojik bilgiler ve sırlar GİZLİ BİLGİ olarak kabul edilir.

4.6.6 Gizlilik: Bilginin içeriğinin görüntülenmesinin, sadece bilgiyi/veriyi görüntülemeye izin verilen kişilerin erişimi ile kısıtlanmasıdır. (Örnek: Şifreli e-posta gönderimi ile e-postanın ele geçmesi halinde dahi yetkisiz kişilerin e-postaları okuması engellenebilir - Kayıtlı elektronik posta - KEP)

4.6.7 Bütünlük: Bilginin yetkisiz veya yanlışlıkla değiştirilmesinin, silinmesinin veya eklemeler çıkarmalar yapılmasının tespit edilebilmesi ve tespit edilebilirliğin garanti altına alınmasıdır. (Örnek: Veri tabanında saklanan verilerin özet bilgileri ile birlikte saklanması - elektronik imza - mobil imza)

4.6.8 Erişilebilirlik/Kullanılabilirlik: Varlığın ihtiyaç duyulduğu her an kullanıma hazır olmasıdır. Diğer bir ifadeyle, sistemlerin sürekli hizmet verebilir halde bulunması ve sistemlerdeki bilginin kaybolmaması ve sürekli erişilebilir olmasıdır. (Örnek: Sunucuların güç hattı dalgalanmalarından ve güç kesintilerinden etkilenmemesi için kesintisiz güç kaynağı ve şaselerinde yedekli güç kaynağı kullanımı - UPS). Bu politikada “Erişilebilirlik” olarak kullanılacaktır.

4.6.9 Bilgi Varlığı: Şirket'in sahip olduğu, faaliyetlerini aksatmadan yürütebilmesi için önemli olan varlıklardır. Bu politikaya konu olan süreçler kapsamında bilgi varlıkları şunlardır:

- Kâğıt, elektronik, görsel veya işitsel ortamda sunulan her türlü bilgi ve veri,
- Bilgiye erişmek ve bilgiyi değiştirmek için kullanılan her türlü yazılım ve donanım,
- Bilginin transfer edilmesini sağlayan ağlar,
- Tesisler ve özel alanlar,
- Bölümler, birimler, ekipler ve çalışanlar,
- Çözüm ortakları,
- Üçüncü taraflardan sağlanan servis, hizmet veya ürünlerdir.

4.7. İşbu Çerçeve belgenin ekinde yer alan idari teşkilatlanma şemasında Şirket nezdinde bilgi yönetişimi konusunda rol alacak aktörler ve görevleri belirtilmiştir.

4.7.1 Yönetim Sorumluluğu

- Şirket Yönetimi, tanımlanmış, yürürlüğe konmuş ve uygulanmakta olan Bilgi Güvenliği ve Kişisel Veri Mahremiyeti Sistemine uyacağını ve sistemin verimli şekilde çalışması için gerekli kaynakları tahsis edeceğini, sistemin tüm çalışanlar tarafından anlaşılmasının sağlayacağını taahhüt eder. Genel Müdür bilgi güvenliğine ilişkin risklerinin değerlendirilmesini ve azaltılmasını sağlamaktan genel olarak sorumlu olup Şirket nezdinde bilmesi gereken herkese ilgili politika ve farkındalığın yayılmasını sağlayacaktır. Bilgi ve veri güvenliği riskleri, mali, yasal ve kurumsal itibara ilişkin diğer risk faktörleri ile benzer şekilde ele alınacaktır.

- Bilgi Güvenliği ve Kişisel Veri Mahremiyeti Sistemine kurulumu sırasında Veri İrtibat Sorumlusu atama yazısı ile atanır. Gerekli olduğu durumlarda üst yönetim tarafından doküman revize edilerek atama tekrar yapılır.

- Yönetim kademesindeki yöneticiler güvenlik konusunda alt kademelerde bulunan personele sorumluluk verme ve örnek olma açısından yardımcı olurlar. Üst kademelerden başlayan ve uygulanan anlayış, firmanın en alt kademe personeline kadar inilmesi zorunludur. Bu yüzden tüm yöneticiler yazılı ya da sözlü olarak güvenlik talimatlarına uymaları, güvenlik konularındaki çalışmalara katılmaları yönünde çalışanlarına destek olurlar.

- Üst Yönetim, Bilgi güvenliği kapsamlı çalışmalar için gerek duyulan bütçeyi oluşturur.

İlgili paydaşlarla veri paylaşma ve işleme anlaşma ve ek protokollerinin imzalanması ile Şirketin faaliyetleri kapsamında ihtiyaç duyduğu veriye erişim ve veri aktarma konularında geçerli olacak diğer sözleşme ve protokollerin hazırlanmasından Veri İrtibat Sorumlusu sıfatıyla görevlendiren Sorumlu Üst Yönetime karşı sorumludur.

4.7.2. Veri İrtibat Sorumlusu

Veri İrtibat Sorumlusu, Şirketin sahip olduğu bilgi varlıkları ve sistemlerinin korunması içi gerekli kurumsal vizyon, strateji ve programların hazırlanması ve uygulanmasından sorumludur. Bu kapsamda yürüteceği görevler aşağıda sıralanmıştır:

- Bilgi Güvenliği ve Kişisel Veri Mahremiyeti Sisteminin planlanması, kabul edilebilir risk seviyesinin belirlenmesi, risk değerlendirme metodolojisinin belirlenmesi,

- Bilgi Güvenliği ve Kişisel Veri Mahremiyeti Sisteminin kurulumunda destekleyici ve tamamlayıcı faaliyetler için gerekli kaynakların sağlanması, kullanıcı kabiliyetlerinin sağlanması/iyileştirilmesi ve farkındalığın oluşması, eğitimlerin yapılması, iletişimin sağlanması, dokümantasyon gereksinimlerinin sağlanması,

- Bilgi Güvenliği ve Kişisel Veri Mahremiyeti Sistemi uygulamalarının yürütülmesi ve yönetilmesi, değerlendirmelerin, iyileştirmelerin ve risk değerlendirmelerinin sürekliliğinin sağlanması,

- İç denetimler, hedeflerin ve yönetim gözden geçirme toplantıları ile Bilgi Güvenliği ve Kişisel Veri Mahremiyeti Sistemi ve kontrollerin değerlendirilmesi,

- Bilgi Güvenliği ve Kişisel Veri Mahremiyeti Sistemin ‘de mevcut yapının sürdürülmesi ve sürekli iyileştirmelerin sağlanması.

4.7.3 Departman Şefleri

- Bölümleri ile ilgili varlık envanteri ve risk analiz çalışmalarının yapılması,

- Sorumluluğu altında bulunan bilgi varlıklarında bilgi güvenliği risklerini etkileyecek bir değişiklik olduğunda, risk değerlendirmesi yapılması için Yönetim Temsilcisini bilgilendirmesi,

- Departman çalışanlarının politika ve prosedürlere uygun çalışmasını sağlanması,

- Bölümleri ile ilgili BGYS kapsamında farkındalığın oluşması, iletişimin sağlanması, dokümantasyon gereksinimlerinin sağlanması,

- BGYS' de mevcut yapının sürdürülmesi ve sürekli iyileştirmelerin sağlanmasından sorumludur.

- Departman Şefleri yönettikleri departmanın çalışma süreçleri ve paydaşlarla ortaklaşa yürütülen faaliyetlerde bilgi yönetimini ilgilendiren hususların değerlendirilmesinden sorumludurlar. Bilgi güvenliği ile ilgili yüklenilecek spesifik sorumluluklarla ilgili olarak Bilgi Güvenliği Politikasını inceleyiniz.

4.7.4 Tüm Çalışanların Sorumluluğu

- Çalışmalarını bilgi güvenliği hedeflerine, politikalarına ve bilgi güvenliği yönetim sistemi dokümanlarına uygun olarak yürütmekten,

- Kendi birimi ile ilgili bilgi güvenliği hedeflerinin takibini yapar ve hedeflere ulaşılmasını sağlar.

- Sistemler veya hizmetlerde gözlenen veya şüphelenilen herhangi bir bilgi güvenliği açıklığına dikkat etmek ve raporlamaktan,

- Üçüncü taraflar ile yapılan ve Satın alma sorumluluğunda olmayan hizmet sözleşmelerine (danışmanlık vb.) ilave olarak gizlilik sözleşmesi yapmak ve bilgi güvenliği gereksinimlerini sağlamaktan sorumludur.

- Tüm şirket çalışanları ve şirketin bilgi varlıklarına erişim izni verilen üçüncü taraflar bilgi yönetimi için kişisel sorumluluklarının farkında olarak yasalara ve kurallara riayet etmelidir. Tüm çalışanlar Şirketin ihdas ettiği politikalarına, prosedürlerine ve rehberliğine uymalı ve bilgi yönetimiyle ilgili olarak düzenlenecek eğitim ve etkinliklere katılmalıdır.

5. BİLGİ GÜVENLİĞİ GENEL ESASLARI

5.1. Bu politika ile çerçevesi çizilen bilgi güvenliği gereksinimleri ve kurallarına ilişkin ayrıntılar, Şirket çalışanları ve 3. taraflar bu politika ve prosedürleri bilmek ve çalışmalarını bu kurallara uygun şekilde yürütmekle yükümlüdür.

5.2. Bu kural ve politikalar, aksi belirtilmedikçe, basılı veya elektronik ortamda depolanan ve işlenen tüm bilgiler ile bütün bilgi sistemlerinin kullanımı için dikkate alınması esastır.

5.3. Bilgi Güvenliği ve Kişisel Veri Mahremiyeti Sistemi, KVKK, GDPR, 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.

5.4. Bilgi Güvenliği ve Kişisel Veri Mahremiyeti Sisteminin hayata geçirilmesi, işletilmesi ve iyileştirilmesi çalışmalarını, ilgili tarafların katkısıyla yürütür. İlgili dokümanların gerektiği zamanlarda güncellenmesi Veri İrtibat Sorumlusu sorumluluğundadır.

5.5. Şirket 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 şirkete aittir.

5.6. Çalışanlar, danışmanlık, hizmet alımı (Güvenlik, servis, yemek, temizlik firması vb.), Tedarikçi ve Stajyer ile gizlilik anlaşmaları yapılır.

5.7. İşe alım, görev değişikliği ve işten ayrılma süreçlerinde uygulanacak bilgi güvenliği kontrolleri belirlenir ve uygulanır.

5.8. Çalışanların bilgi güvenliği farkındalığını artıracak ve sistemin işleyişine katkıda bulunmasını sağlayacak eğitimler düzenli olarak mevcut şirket çalışanlarına ve yeni işe başlayan çalışanlara verilir.

5.9. Bilgi güvenliğinin gerçek ya da şüpheli tüm ihlalleri rapor edilir; ihlallere sebep olan uygunsuzluklar tespit edilir, ana sebepleri bulunarak tekrar edilmesini engelleyici önlemler alınır.

5.10. Bilgi varlıklarının envanteri bilgi güvenliği yönetim ihtiyaçları doğrultusunda oluşturulur ve varlık sahiplikleri atanır.

5.11. Kişisel ve Kurumsal veriler sınıflandırılır ve her sınıftaki verilerin güvenlik ihtiyaçları ve kullanım kuralları belirlenir.

5.12. Güvenli alanlarda saklanan varlıkların ihtiyaçlarına paralel fiziksel güvenlik kontrolleri uygulanır.

5.13. Firmaya ait bilgi varlıkları için firma içinde ve dışında maruz kalabilecekleri fiziksel tehditlere karşı gerekli kontrol ve politikalar geliştirilir ve uygulanır.

5.14. Kapasite yönetimi, üçüncü taraflarla ilişkiler, yedekleme, sistem kabulü ve diğer güvenlik süreçlerine ilişkin prosedür ve talimatlar geliştirilir ve uygulanır.

5.15. 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.

5.16. Erişim hakları ihtiyaç nispetinde atanır. Erişim kontrolü için mümkün olan en güvenli teknoloji ve teknikler kullanılır.

5.17. Sistem temini ve geliştirilmesinde güvenlik gereksinimleri belirlenir, sistem kabulü veya testlerinde güvenlik gereksinimlerinin karşılanıp karşılanmadığı kontrol edilir.

5.18. Kritik altyapı için süreklilik planları hazırlanır, bakımı ve tatbikatı yapılır.

5.19. 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.

6. BİLGİ GÜVENLİĞİ VE KİŞİSEL VERİLER ÇERÇEVE POLİTİKASI KAPSAMINDA İHDAS EDİLECEK POLİTİKALAR

6.1. Bilgi Güvenliği Ve Kişisel Veriler Çerçeve Politikası kapsamında ihdas edilmesi ön görülen politika ve davranış kurallarını belirleyen yönetmelikler aşağıdaki gibidir:

BELGENİN TÜRÜ	REFERANS NUMARASI	BAŞLIĞI
POLİTİKA	KVKK_P1	BİLGİ GÜVENLİĞİ VE KİŞİSEL VERİLER ÇERÇEVE POLİTİKASI
POLİTİKA	KVKK_P2	KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ POLİTİKASI
POLİTİKA	KVKK_P3	KİŞİSEL VERİLERİ SAKLAMA VE İMHA POLİTİKASI
POLİTİKA	KVKK_P4	PERSONEL İÇİN GEÇERLİ KİŞİSEL VERİLERİN KORUNMASI POLİTİKASI
POLİTİKA	KVKK_P5	BİLGİ GÜVENLİĞİ POLİTİKASI
POLİTİKA	KVKK_P6	BİLGİ VE İLETİŞİM TEKNOLOJİLERİNİN KULLANIMI POLİTİKASI
POLİTİKA	KVKK_P7	ERİŞİM KONTROL POLİTİKASI
POLİTİKA	KVKK_P8	KAPALI KAMERA SİSTEMLERİ POLİTİKASI
POLİTİKA	KVKK_9	İNTERNET VE ELEKTRONİK İLETİŞİM ARAÇLARININ KABUL EDİLEBİLİR KULLANIMI HAKKINDA USUL VE ESASLARA İLİŞKİN POLİTİKA VE YÖNETMELİK
YÖNETMELİK	KVKK_Y1	VERİ SAHİBİ İLGİLİ KİŞİLERİN TALEPLERİNE VERİLECEK CEVAPLARIN USUL VE ESASLARI HAKKINDA YÖNETMELİK
YÖNETMELİK	KVKK_Y2	VERİ İHLALİ MÜDAHALE PLAN YÖNETMELİĞİ
YÖNETMELİK	KVKK_Y3	VERİ KORUMA ETKİ DEĞERLENDİRMESİ USUL VE ESASLARI HAKKINDA YÖNETMELİK
YÖNETMELİK	KVKK_Y4	ELEKTRONİK HABERLEŞME VE ELEKTRONİK VERİLERİN DENETLENMESİ HAKKINDA YÖNETMELİK
YÖNETMELİK	KVKK_Y5	ELEKTRONİK MESAJLAŞMA KULLANIMI USUL VE ESASLARINA DAİR YÖNETMELİK
YÖNETMELİK	KVKK_Y6	KAPALI DEVRE KAMERA SİSTEMLERİNİN KULLANIM USUL VE ESASLARI

		HAKKINDA YÖNETMELİK
YÖNETMELİK	KVKK_Y7	KULLANICI ŞİFRELERİNİN BELİRLENMESİ, KULLANIMI VE KORUNMASINA İLİŞKİN USUL VE ESASLAR HAKKINDA YÖNETMELİK
YÖNETMELİK	KVKK_Y8	VERİ AKTARIM GÜVENLİĞİ USUL VE ESASLARI HAKKINDAKİ YÖNETMELİK
AYDINLATMA METNİ	KVKK_A1	ÇALIŞAN AYDINLATMA METNİ
AYDINLATMA METNİ	KVKK_A2	İNTERNET SİTESİ ÇEREZ KULLANIMI HAKKINDA AYDINLATMA METNİ
AYDINLATMA METNİ	KVKK_A3	KAPALI KARESRA SİSTEMLERİ AYDINLATMA METNİ
AYDINLATMA METNİ	KVKK_A4	VERİ SAHİBİ BAŞVURU FORMU
AYDINLATMA METNİ	KVKK_A5	KVKK AYDINLATMA METNİ
AYDINLATMA METNİ	KVKK_A6	KİŞİSEL VERİLERİN KORUNMASI HAKKINDA YÜKLENİCİ AYDINLATMA METNİ
EKLER	KVKK_E1	OLASI İHLAL SENARYOLARI
FORM	KVKK_F1	VERİ KORUMA ETKİ DEĞERLENDİRMESİ FORMU

6.2. Politikaların Belirlenmesi

6.2.1. Kişisel Veriler Komitesi tüm bilgi güvenliği yönetimi politikalarını gözden geçirerek gerekli gördüğü takdirde değişiklik yapılması yönünde tavsiyelerini Üst Yönetime bildirir. İhdas edilen tüm politikalar ve bunlarla ilgili güncellemeler Şirket portalı ya da internet üzerinden çalışanlara tebliğ edilir.

6.2.2. Politikalar yıllık olarak gözden geçirilerek gerekli görüldüğü takdirde güncellenirler ve aksaklıkların giderilmesi için yeni politikalar ihdas edilebilir. Uygun olduğu takdirde bahse konu politikaların çalışan iş akdi ile birlikte değerlendirilmesi yoluna gidilir.

6.2.3. İşbu Çerçeve Politika kapsamında ihdas edilecek Politikalar kapsam ve amacın ana hatlarını belirler ve personel ve diğer ilgili tarafların sorumluluklarını belirleyen bir bilgi güvenliği yönetimi çerçevesi sunar. Şirket istihdam ettiği personel ve kendisi ile iş ilişkisi içerisinde olan tarafların Şirketin amaçları ve bu amaçlara ulaşılması için ilgili paydaşlardan beklenen sorumluluklar hakkında bilgi sahibi olması için gerekli tedbirleri almayı taahhüt eder. Bu meyanda ihdas edilen Politika ve Yönetmelikler çalışanlar ve iş ortaklarına kendilerinden beklenen yükümlülüklerin bildirilmesi açısından anahtar bir role sahiptir.

6.3. Eğitim ve Geliştirme

6.3.1. Bilgi güvenliği yönetimi konusunda verilecek eğitimi ve geliştirme programları Şirket genelinde bilgi güvenliği yönetimi ile ilgili personel bilgi ve becerilerinin geliştirilmesi ve iyileştirilmesi için elzemdir.

6.3.2. Bilgi güvenliği yönetimi hususunda verilecek eğitimi, en iyi uygulamaları geliştirmek ve takip etmek için temel gizlilik ve güvenlik bilinci haricindeki konuları da içermelidir. Personel, bilginin değerini ve veri kalitesi, bilgi güvenliği, kayıt yönetimi, gizlilik vb. dâhil olmak üzere sorumluluklarını anlamalıdır.

7. ÇERÇEVE POLİTİKAYA UYUMUN TAKİBİ

7.1. Kişisel Veriler Komitesi işbu Çerçeve Politikaya riayet edilmesi ve ilgili her bir politikanın gözden geçirilerek güncellenmesinden sorumludur.

7.2. Politika ve prosedürler en az yılda bir kez gözden geçirilmelidir. Bunun dışında sistem yapısını veya risk değerlendirmesini etkileyecek herhangi bir değişiklikten sonra da gözden geçirilmeli ve herhangi bir değişiklik gerekiyorsa üst yönetime onaylatılarak yeni versiyon olarak kayıt altına alınmalıdır. Her revizyon tüm kullanıcıların erişebileceği şekilde yayınlanmalıdır.

7.3. Yönetim gözden geçirme toplantıları Veri İrtibat Sorumlusu tarafından Organize edilerek, Üst Yönetim ve Bölüm yöneticileri katılımı ile gerçekleştirilir. Bilgi Güvenliği Yönetim Sisteminin uygunluğunun ve etkinliğinin değerlendirildiği bu toplantılar en az yılda bir kez gerçekleştirilir.

8. POLİTİKANIN İHLALİ VE YAPTIRIMLAR

Bilgi Güvenliği ve Kişisel Veriler Çerçeve Politikasına ve Standartlarına uyulmadığının tespit edilmesi durumunda, bu ihlalden sorumlu olan çalışanlar için Disiplin Yönergesi ve Prosedürü ’ne göre Üçüncü Taraflar için de geçerli olan sözleşmelerde geçen ilgili maddelerinde belirlenen yaptırımlar uygulanır.