BİLGİ GÜVENLİĞİ POLİTİKASI

1. Amaç

Bu politikanın amacı, yasal, düzenleyici veya sözleşmeye tabi yükümlülüklere uymak, her türlü güvenlik gereksinimlerine ilişkin ihlalleri önlemek ve bunlara ilişkin olarak Şirket yönetiminin yaklaşımını, hedeflerini tanımlamak ve tüm çalışanlara ve ilgili taraflara bu hedefleri bildirmektir.

2. Kapsam

Bu politika Şirket bünyesinde yapılan ticari faaliyetlere ve bu işlemlere ilişkin lojistik, depolama, muhasebe, finans, satın alma, insan kaynakları, hukuk, satış, pazarlama, iç denetim ve bilgi işlem faaliyetlerinden elde edilen bilgi varlıkların korunması, şirket bünyesinde tutulan kişisel verilerin kanun kapsamında işlenmesi, saklanması, korunması, gizliliğinin ve bütünlüğünün bozulmaması için sağlanan bilgi güvenliği süreçlerini kapsar.

3. Tanımlar

3.1. **Bilgi Güvenliği:** Bilginin yetki dışı bir başka kişiye aktarılması, değiştirilmesi, tahrif edilmesi, kurcalanması ya da açığa vurulması tehlikelerine karşı korunmasını, bilginin kime ait olduğunun belirlenmesi, bütünlüğünün korunması ve kullanılabilirliğinin sağlanması aşamalarıdır.

3.2. **Gizlilik:** Bilginin yetkisiz kişiler, varlıklar ya da süreçler tarafından erişilememesini, kullanılamamasını, değiştirilmemesini, depolanmamasını, başka bir ortama kaydedilmemesini veya ifşa edilmemesini ifade eder.

3.3. **Bütünlük:** Varlıkların doğruluğunu ve tamlığını koruma özelliğini ifade eder.

3.4. **Erişilebilirlik/Kullanılabilirlik:** Yetkili bir varlık tarafından talep edildiğinde erişilebilir ve kullanılabilir olma özelliğini ifade eder.

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

3.5.1. Kağıt, elektronik, görsel veya işitsel ortamda sunulan her türlü bilgi ve veri,

3.5.2. Bilgiye erişmek ve bilgiyi değiştirmek için kullanılan her türlü yazılım ve donanım,

3.5.3. Bilginin transfer edilmesini sağlayan ağlar,

3.5.4. Tesisler ve özel alanlar,

3.5.5. Bölümler, birimler, ekipler ve çalışanlar,

3.5.6. Çözüm ortakları,

3.5.7. Üçüncü taraflardan sağlanan servis, hizmet veya ürünlerdir.

4. Sorumluluklar

Çalışanların nitelik ve yeterliliklerine göre yetki ve sorumlulukları görev tanımlarında belirlenmiştir.. Bilgi güvenliği ile ilgili faaliyetlerin sürdürülmesinden ve geliştirilmesinden Bilgi Güvenliği Yetkilisi sorumludur.

4.1. Yönetim Sorumluluğu

4.1.1. Şirket Yönetimi, tanımlanmış, yürürlüğe konmuş ve uygulanmakta olan bilgi güvenliğine ilişkin her türlü kurala uyacağını ve sistemin verimli şekilde çalışması için gerekli kaynakları tahsis edeceğini, sistemin tüm çalışanlar tarafından anlaşılmasının sağlayacağını taahhüt eder.

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

4.1.3. Üst Yönetim, bilgi güvenliği kapsamlı çalışmalar için gerek duyulan bütçeyi oluşturur.

4.2. Bilgi Güvenliği Yetkilisi Sorumluluğu

4.2.1. Bilgi güvenliğinin planlanması, kabul edilebilir risk seviyesinin belirlenmesi, risk değerlendirme metodolojisinin belirlenmesini,

4.2.2. Bilgi güvenliğinin sağlanmasında destekleyici ve tamamlayıcı faaliyetler için gerekli kaynakların sağlanması, kullanıcı kabiliyetlerinin sağlanması/iyileştirilmesi ve farkındalığın oluşması, eğitimlerin yapılması, iletişimin sağlanması, dokümantasyon gereksinimlerinin sağlanması,

4.2.3. Bilgi güvenliği uygulamalarının yürütülmesi ve yönetilmesi; değerlendirmelerin, iyileştirmelerin ve risk değerlendirmelerinin sürekliliğinin sağlanması,

4.2.4. İç denetimler, hedeflerin ve yönetim gözden geçirme toplantıları ile bilgi güvenliği ve kontrollerin değerlendirilmesi,

4.2.5. Bilgi güvenliğine ilişkin mevcut yapının sürdürülmesi ve sürekli iyileştirmelerin sağlanmasından sorumludur.

4.3. Birim Yöneticilerinin Sorumluluğu

4.3.1. Birimleri ile ilgili varlık envanteri ve risk analiz çalışmalarının yapılması,

4.3.2. Sorumluluğu altında bulunan bilgi varlıklarında bilgi güvenliği risklerini etkileyecek bir değişiklik olduğunda, risk değerlendirmesi yapılması için Bilgi Güvenliği Yetkilisinin bilgilendirilmesi,

4.3.3. Birim çalışanlarının politika ve prosedürlere uygun çalışmasını sağlanması,

4.3.4. Birimleri ile ilgili bilgi güvenliği kapsamında farkındalığın oluşması, iletişimin sağlanması, dokümantasyon gereksinimlerinin sağlanması,

4.3.5. Bilgi güvenliğine ilişkin mevcut yapının sürdürülmesi ve sürekli iyileştirmelerin sağlanmasından sorumludur.

4.4. Tüm Çalışanların Sorumluluğu

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

4.4.2. Kendi birimi ile ilgili bilgi güvenliği hedeflerinin takibini yapmak ve hedeflere ulaşılmasını sağlamaktan,

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

4.4.4. Üçüncü taraflar ile yapılan sözleşmelere ilave olarak gizlilik sözleşmesi yapmak ve bilgi güvenliği gereksinimlerini sağlamaktan sorumludur.

4.5. Üçüncü Tarafların Sorumluluğu

Bilgi güvenliği politikasının bilinmesi ve uygulanması ile bilgi güvenliği kapsamında belirlenen davranışlara uyulmasından sorumludur.

5. Bilgi Güvenliği Hedefleri

Bilgi Güvenliği Politikası, Şirket çalışanlarına firmanın güvenlik gereksinimlerine uygun şekilde hareket etmesi konusunda yol göstermek, bilinç ve farkındalık seviyelerini arttırmak ve bu şekilde şirketin temel ve destekleyici iş faaliyetlerinin en az kesinti ile devam etmesini sağlamak, güvenilirliğini ve imajını korumak ve üçüncü taraflarla yapılan sözleşmelerde belirlenmiş uygunlukları sağlamak amacıyla firmanın tüm işleyişini etkileyen fiziksel ve elektronik bilgi varlıklarının korunmasını hedefler. Yönetim Tarafından belirlenen hedefler periyodik olarak Gözden Geçirme toplantılarında gözden geçirilir.

6. Risk Yönetim Çerçevesi

Şirketin risk yönetim çerçevesi; Bilgi güvenliği risklerinin tanımlanmasını, değerlendirilmesini ve işlenmesini kapsar. Risk Analizi, uygulanabilirlik bildirgesi ve risk işleme planı, bilgi güvenliği risklerinin nasıl kontrol edildiğini tanımlar. Risk işleme planının yönetiminden ve gerçekleştirilmesinden Bilgi Güvenliği Yetkilisi sorumludur.

7. Bilgi Güvenliği Genel Esasları

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

7.2. Bu kural ve politikalar, aksi belirtilmedikçe, sadece elektronik ortamda tutulan verilerin değil; yazılı, basılı, sözlü ve benzeri ortamda bulunan tüm verilerin güvenliği için dikkate alınması esastır.

7.3. Şirket tarafından çalışanlara veya üçüncü 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.

7.4. Çalışanlar ve tedarikçiler ile gizlilik anlaşmaları yapılır.

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

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

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

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

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

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

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

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

7.13. 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.

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

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

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

7.17. 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. Politikanın İhlali ve Yaptırımlar

Bilgi Güvenliği Politikasına uyulmadığının tespit edilmesi durumunda, bu ihlalden sorumlu olan çalışanlar için Disiplin Yönergesi'ne göre üçüncü taraflar için de geçerli olan sözleşmelerde geçen ilgili maddelerinde belirlenen yaptırımlar uygulanır.

9. Bilgi Güvenliği Politika Dokümanı Güncellenmesi ve Gözden Geçirilmesi

Şirket Bilgi Güvenliği Politikası Bilgi Güvenliği Yetkilisi tarafından yılda en az bir kere gözden geçirilir ve gerekli görülmesi durumunda güncellenerek Yönetim Kurulu onayına sunulur. Güvenlik teknolojilerindeki gelişmelere bağlı olarak ortaya çıkan ihtiyaçları içerecek yeni politikalar üretilir. 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.

10. Bilgi Güvenliği Politikasını Uygulama Sorumluluğu

Tüm çalışanların Bilgi Güvenliği Politikası'ndan haberdar olması sağlanır. Politikanın son hali tüm personele duyurulur ve personelin sürekli olarak erişebileceği ortak bir alanda yayımlanır. Personel kendisini ilgilendiren genel hükümlere uymak zorundadır. Personelin kendisini ilgilendiren genel hükümlere uyup uymadığının kontrol edilmesi sorumluluğu personelin birim yöneticisindedir. Bilgi güvenliği politikalarına uyum düzenli olarak izlenir.

11. Yürürlük

Bilgi güvenliğine ilişkin bu düzenleme, üst yönetimin onay tarihi itibariyle yürürlüğe girer. Şirket'in bilgi güvenliğine ilişkin tüm uygulama ve iş akışları politika hükümleriyle uyumlu şekilde oluşturulur/güncellenir.