BİLGİ GÜVENLİĞİ POLİTİKASI

1. **Amaç :** Bu politikanın amacı, hukuka, yasal, düzenleyici ya da sözleşmeye tabi yükümlülüklere ve her türlü güvenlik gereksinimlerine ilişkin ihlalleri önlemek için, üst yönetimin yaklaşımını ve hedeflerini tanımlamak, 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, kalite güvence, satın alma, insan kaynakları, hukuk, satış, pazarlama, iç denetim ve bilgi işlem faaliyetlerinden elde edilen elektronik bilgi varlıkların korunması, şirket bünyesinde tutulan kişisel verilerin kanun kapsamında işlenmesi, saklanması, korunması, gizliliğinin ve bütünlüğünün bozulmaması için kullandığı bilgi güvenliği süreçlerini kapsar.

2.1. İç Kapsam

İdare, kuruluşa ilişkin yapı, roller ve yükümlülükler;

2.1.1. Şirket Üst Yönetimi bünyesinde bulunan kapsam dahilindeki departmanlar;, İç Kontrol ve Uyum, Kredi Risk Yönetimi, Kredi Tahsis, Kredi Operasyon, Risk İzleme&Takip Müşteri İletişim Merkezi, Mali ve İdari İşler, Bilgi Teknolojileri, Süreç Yönetimi, Finans, İnsan Kaynakları, İdari İşler, Bütçe Raporlama, Hukuk, Satış, Pazarlama

2.1.2. Genel Yönetim Organizasyon Şemasında belirtilmiş roller ve görev tanımlarındaki sorumluluklar.

2.1.3. Yerine getirilecek politikalar, prosedürler, hedefler ve stratejiler;

2.1.3.1. Bilgi Güvenliği Yönetim Sistemi Politikası,

2.1.3.2. Tüm Bilgi Güvenliği yönetim sistemleri prosedürleri,

2.1.3.3. Yönetimce belirlenmiş yıllık Bilgi Güvenliği yönetim sistemleri hedefleri,

2.1.3.4. Kaynaklar ve bilgi birikimi cinsinden anlaşılan yetenekler (örneğin, anapara, zaman, kişiler, süreçler, sistemler ve teknolojiler),

2.1.3.5. Bilgi Güvenliği Yönetim Sisteminin kurulması, işletilmesi ve sürdürülmesi için yönetim tarafından atanan Yönetim Temsilcileri ve Bilgi Güvenliği Yönetim Sistemi ekibi,

2.1.3.6. İç paydaşlarla ilişkiler ve onların algılamaları ve değerleri, kuruluşun kültürü, kuruluş tarafından uyarlanan standartlar, kılavuzlar ve modeller, sözleşmeye ilişkin ilişkilerin; biçim ve genişliğini kapsamaktadır.

2.2. Dış Kapsam

2.2.1. Uluslararası, ulusal, bölgesel veya yerel olmak üzere, sosyal ve kültürel, politik, yasal, mevzuata ilişkin, finansal, teknolojik, ekonomik, doğal ve rekabetçi ortam,

2.2.2. Küresel Rekabet Hukuku, Politikaları ve Prosedürleri,

2.2.3. Tedarikçi ve müşteri verilerinin gizliliği,

2.2.4. Kalite Odaklılık,

2.2.5. Kuruluşun hedefleri üzerinde etkisi bulunan paydaşlarla ilişkiler ve onların algılamaları ve değerleri;

2.2.6. Müşteri memnuniyetin sağlanması için Üst Yönetim dahil tüm Şirket çalışanları,

2.2.7. İlgili tüm yasal mevzuat, düzenleyici, sözleşmeden doğan şartlar, standartlar,

2.2.8. TSE ve diğer kuruluşlarla olan ürün belgelendirmeleri dış kapsamdır.

3. Tanımlar

3.1. **BGYS:** Bilgi Güvenliği Yönetim Sistemi.

3.2. **Envanter:** Firma için önemli olan her türlü bilgi varlığı.

3.3. **Üst Yönetim:** Şirket Üst Yönetimidir.

3.4. **Know-How:** Bir şeyi yapabilme yetkinliğidir.

3.5. **Bilgi Güvenliği:** 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.

3.6. **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)

3.7. **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)

3.8. **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.

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

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

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

3.9.3. Bilginin transfer edilmesini sağlayan ağlar,

3.9.4. Tesisler ve özel alanlar,

3.9.5. Bölümler, birimler, ekipler ve çalışanlar,

3.9.6. Çözüm ortakları,

3.9.7. Üçüncü taraflardan sağlanan servis, hizmet veya ürünlerdir.

4. **Sorumluluklar** Sorumluluk ve yetkileri belirlenmiş görevlerin nitelik ve yeterlilikleri görev tanımlarında tanımlanmıştır. Bilgi güvenliği ile ilgili faaliyetlerin sürdürülmesinden ve geliştirilmesinden Bilgi İşlem Ekibi ve Yönetim Temsilcisi sorumludur. BGYS Ekibi ve Yönetim Temsilcileri Üst Yönetim tarafından atanmıştır. Kapsam içindeki departmanlardan BGYS temsilcileri belirlenmiştir. BGYS ekip üyesi olarak isim bazında atamaları yapılmıştır.

4.1. Yönetim Sorumluluğu

4.1.1. Şirket Yönetimi, tanımlanmış, yürürlüğe konmuş ve uygulanmakta olan Bilgi Güvenliği Sistemine uyacağını ve sistemin verimli şekilde çalışması için gerekli kaynakları tahsis edeceğini, sistemin tüm çalışanlar tarafından anlaşılmasının sağlayacağını taahhüt eder.

4.1.2. BGYS kurulumu sırasında BGYS Yönetim Temsilcisi atama yazısı ile atanır. Gerekli olduğu durumlarda üst yönetim tarafından doküman revize edilerek atama tekrar yapılır.

4.1.3. 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 yada sözlü

olarak güvenlik talimatlarına uymaları, güvenlik konularındaki çalışmalara katılmaları yönünde çalışanlarına destek olurlar.

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

4.2. Yönetim Temsilcisi Sorumluluğu

4.2.1. BGYS (Bilgi Güvenliği Yönetim Sistemi)'nin planlanması, kabul edilebilir risk seviyesinin belirlenmesi, risk değerlendirme metodolojisinin belirlenmesini,

4.2.2. BGYS kurulumunda 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. BGYS uygulamalarının yürütülmesi ve yönetilmesi, değerlendirmelerin, iyileştirmelerin ve risk değerlendirmelerinin sürekliliğinin sağlanması,

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

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

4.3. BGYS Ekip Üyeleri Sorumluluğu

4.3.1. Bölümleri 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 Yönetim Temsilcisini bilgilendirmesi,

4.3.3. Departman çalışanlarının politika ve prosedürlere uygun çalışmasını sağlanması,

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

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

4.4. **İç Denetçi Sorumluluğu** İç denetim planı doğrultusunda, görev verilen iç denetimlerde denetim faaliyetlerinin yapılmasından ve raporlanmasından sorumludur.

4.5. **Bölüm Yöneticileri Sorumluluğu** Bilgi Güvenliği Politikasının uygulanması ve çalışanların esaslara uymasının sağlanmasından, 3.

tarafların politikadan haberdar olmasının sağlanmasından ve fark ettiği bilgi sistemleri ile ilgili güvenlik ihlal olaylarının bildirilmesinden sorumludurlar.

4.6. Tüm Çalışanların Sorumluluğu

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

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

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

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

4.7. Üçüncü Tarafların Sorumluluğu Bilgi güvenliği politikasının bilinmesi ve uygulanması ile BGYS 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 belirlenmiş periyotlarda izlenir ve Yönetim Gözden Geçirme toplantılarında gözden geçirilir.

6. Risk Yönetim Çerçevesi Firmanın 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 BGYS Yürütme ve Yönetim Komitesi sorumludur. Tüm bu çalışmalar, varlık envanteri ve risk değerlendirme talimatında detaylı olarak açıklanır.

7. Bilgi Güvenliği Genel Esasları

7.1. 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.

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

7.3. Bilgi Güvenliği Yönetim Sistemi, 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.

7.4. BGYS'nin hayata geçirilmesi, işletilmesi ve iyileştirilmesi çalışmalarını, ilgili tarafların katkısıyla yürütür. BGYS dokümanlarının gerektiği zamanlarda güncellenmesi BGYS Yönetim Temsilcisi sorumluluğundadır.

7.5. 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.

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

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

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

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

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

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

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

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

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

7.15. 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.

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

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

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

7.19. 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.

8. **Politikanın İhlali ve Yaptırımlar** Bilgi Güvenliği Politikasına ve Standartlarına uyulmadığının tespit edilmesi durumunda, bu ihlalden sorumlu olan çalışanlar için Disiplin Yönergesi ve Prosedürü 'ne göre 3. Taraflar için de geçerli olan sözleşmelerde geçen ilgili maddelerinde belirlenen yaptırımlar uygulanır.

9. **Yönetimin Gözden Geçirmesi** Yönetim gözden geçirme toplantıları BGYS Kalite Yönetim Temsilcisi 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 gerçekleştirilmektedir.

10. **Bilgi Güvenliği Politika Dokümanı Güncellenmesi ve Gözden Geçirilmesi** Politika dokümanının sürekliliğinin sağlanmasından ve gözden geçirilmesinden BGYS Yönetim Temsilcileri sorumludur. 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.