1.1. Genel Esaslar

- Bu politika ile çerçevesi çizilen bilgi güvenliği gereksinimleri ve kurallarına ilişkin ayrıntılar, BGYS politikaları ile düzenlenir. Çalışanlar ve 3. taraflar bu prosedürleri bilmek ve çalışmalarını bu kurallara uygun şekilde yürütmekle yükümlüdür.
- Bu politikaların, aksi belirtilmedikçe, basılı veya elektronik ortamda depolanan ve işlenen tüm bilgiler ile bütün bilgi sistemlerinin kullanımı için dikkate alınması esastır.
- 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.
- Firma 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 firmaya aittir.
- Kritik iş süreçlerini büyük felaketlerin ve işletim hatalarının etkilerinden korumak amacıyla iş sürekliliği yönetimi uygulanır.
- Çalışanların bilgi güvenliği farkındalığını artıracak ve sistemin işleyişine katkıda bulunmasını sağlayacak eğitimler düzenli olarak mevcut firma çalışanlarına ve yeni işe başlayan çalışanlara verilir.
- Bilgi güvenliğinin gerçek ya da şüpheli tüm ihlalleri rapor edilir; ihlallere sebep olan uygunsuzluklar tespit edilir, ana sebepleri bulunarak tekrar edilmesini engelleyici önlemler alınır.
- Bilgi güvenliğinde tüm çalışanlar, Varlıkların Kabul Edilebilir Kullanım Kurallarına uygun olarak çalışmayı taahhüt eder.

1.2. Bilgi Güvenliği

Bilgi, diğer önemli ticari ve kurumsal varlıklar gibi, bir işletme ve kurum için değeri toplantılarında olan ve bu belirlenir nedenle uygun olarak korunması gereken bir varlıktır. Bilgi güvenliği iş sürekliliğini sağlamak, doküman Üst kayıpları en aza indirmek için tehlike ve tehdit alanlarından korur.

Bilgi güvenliği, bu politikada aşağıdaki bilgi niteliklerinin korunması olarak tanımlanır:

- Gizlilik: Bilginin sadece erişim yetkisi verilmiş kişilere erişilebilir olduğunu garanti etmek,
- Bütünlük: Bilginin ve işleme yöntemlerinin doğruluğunu ve yetkisiz değiştirilememesini temin etmek,
- Erişilebilirlik: Yetkili kullanıcıların, gerek duyulduğunda bilgiye ve ilişkili kaynaklara en hızlı şekilde erişebileceklerini garanti etmek.

Bilgi güvenliği politikası dokümanı, yukardaki korumaları ve gereksinimleri sağlayabilmek için oluşturulmuş denetimlerin uygulanması sırasında kullanılacak en üst seviyedeki prensiplerin belirtildiği dokümandır.

2. Temel BGYS Prensipleri

2.1.1. Dış kaynak kullanım durumlarında oluşabilecek güvenlik gereksinimleri analiz edilerek güvenlik şart ve kontrolleri şartname ve sözleşmelerde ifade edilir.

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

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

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

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

Hazırlayan	Onaylayan
Eğitim ve İş Güvenliği Uzmanı Yönetim Temsilcisi	Üst Yönetim Temsilcisi

2.1.6. Firmaya ait bilgi varlıkları için firma içinde ve dışında maruz kalabilecekleri fiziksel tehditlere karşı gerekli kontrol ve politikalar geliştirilir ve uygulanır.
2.1.7. Kapasite yönetimi, üçüncü taraflarla ilişkiler, yedekleme, sistem kabulü ve diğer güvenlik süreçlerine ilişkin prosedür ve talimatlar geliştirilir ve uygulanır.
2.1.8. 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.
2.2. Erişim hakları ihtiyaç nispetinde atanır. Erişim kontrolü için mümkün olan en güvenli teknoloji ve teknikler kullanılır.

- Başta kullanıcı bilgisayarları ve sunucular olmak üzere mümkün olan tüm sistemler, zararlı yazılımlara karşı korunması için “Eset Nod32 Antivirus programı ve Fidye yazılımları için Sophos yazılımı kullanılmaktadır.
- Bilgisayar üzerindeki Usb disk portları sadece okunabilir olarak konfigüre edilir.
- Sistem temini ve geliştirilmesinde güvenlik gereksinimleri belirlenir, sistem kabulü veya testlerinde güvenlik gereksinimlerinin karşılanıp karşılanmadığı kontrol edilir.
- Bilgi güvenliği ihlal olayları ve zayıflıklarının raporlanması için gerekli altyapı oluşturulur. İhlal olay kayıtları tutulur, gerekli düzeltici önleyici faaliyetler uygulanır ve düzenlenen farkındalık eğitimleri vasıtasıyla güvenlik olaylarından öğrenme sağlanır.
- Kritik altyapı için süreklilik planları hazırlanır, bakımı ve tatbikatı yapılır.
- 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.
- Bilgi güvenliği yönetim sistemi iyileştirme faaliyetleri ile sürekli olarak iyileştirilmesi sağlanır.
- Bilgi güvenliği yönetim sistemi performansı düzenli aralıklarla ölçülerek yönetim temsilcisi tarafından üst yönetime YGG toplantılarında sunulur.

3. Yönetimin Taahhüdü

Kurumun belirlediği hedef ve politikalarını gerçekleştirmek için Bilgi Güvenliği Yönetim Sistemini ISO/IEC 27001’de belirtilen gereksinimleri yerine getirecek şekilde kurarak yürütür.

Kurum yönetimi, tanımlanmış, yürürlüğe konmuş ve uygulanmakta olan Bilgi Güvenliği Yönetim Sistemine uyacağını ve sistemin verimli şekilde çalışması için gerekli olan kaynakları tahsis edeceğini, etkinliğini, sürekli iyileştireceğini ve bunun tüm çalışanlar tarafından anlaşılmasını sağlayacağını taahhüt eder. Bu taahhüdün sonucu olarak, firma genelinde bilgi güvenliği farkındalık programları düzenler ve alt yapı yatırımlarını sürdürür.

BGYS kurulurken üst yönetim tarafından BGYS Yönetim Temsilcisi ve Bilgi Güvenliği Ekibi üyeleri atama yazısı ile atanır. BGYS Yönetim Temsilcisi ve Bilgi Güvenliği Ekibi üyeleri değiştiğinde, işten ayrıldığında üst yönetim tarafından doküman revize edilerek atama tekrar yapılır. BGYS Yönetim temsilcisi belirlemek ve değiştirmek üst yönetimin yetkisindedir.

Yönetim kademelerindeki yöneticiler güvenlik konusunda alt kademelerde bulunan personele sorumluluk verme ve örnek olma açısından yardımcı olurlar. Üst kademelerden başlayan ve uygulanan bir güvenlik anlayışıyla, firmanın en alt kademe personeline kadar inilmesi zorunludur. Bu yüzden kurum yöneticilerinin gerek yazılı gerekse sözlü olarak güvenlik prosedürlerine uymaları, güvenlik konusundaki çalışmalara katılmaları konusunda güvenlik ile ilgili çalışmalarda bulunan personele destek olurlar.

Kurum üst yönetimi, bilgi güvenliği kapsamlı çalışmalar için gerek duyulan bütçeyi oluşturur.

Hazırlayan	Onaylayan
Eğitim ve İş Güvenliği Uzmanı Yönetim Temsilcisi	Üst Yönetim Temsilcisi