ENTEGRE YÖNETİM SİSTEMİ POLİTİKASI

BİLTİM Bilgisayar Hizmetleri A.Ş.; bilgi güvenliğinin gerçekleştirilmesi, işletimi, sürekli izlenmesi, gözden geçirilmesi, bakımı ve sürekli iyileştirilmesi için gereken her türlü adımın atılacağını taahhüt eder. Bilgi güvenliği, tüm çalışanların sorumluluğu olup kurumsal kültürün ayrılmaz bir parçasıdır.

Bilgi güvenliği; bilgi varlıklarının gizliliği, bütünlüğü ve erişilebilirliğinin sağlanmasıyla mümkündür:

- Gizlilik: Bilgiye yalnızca yetkili kişilerin erişmesi,
- Bütünlük: Bilginin doğruluğunun ve tamlığının korunması,
- Erişilebilirlik: Bilginin ihtiyaç duyulduğunda yetkili kişilerce kullanılabilir olmasıdır.

BİLTİM A.Ş., Entegre Yönetim Sistemlerini risk bazlı yaklaşım ile uygular, yürütür ve sürekli geliştirir. Yasal, mevzuat ve sözleşme gerekliliklere tam uyum sağlar; ürün ve hizmetlerin müşteri ve paydaş beklentilerini karşılamasını güvence altına alır.

Şirket, iç ve dış paydaşların ihtiyaçlarını dikkate alarak iş süreçlerinin güvenliğini sürdürmeyi ve rekabet avantajını olumsuz etkileyebilecek maddi/manevi kayıpları önlemeyi hedefler.

BİLTİM A.Ş. yukarıda belirtilen ilkelerden taviz vermeden bilgi güvenliği çalışmalarını aşağıda belirtilen amaçlarla gerçekleştirmeyi taahhüt eder;

- Entegre Yönetim Sistemi (“EYS”) ile, uluslararası olarak kabul edilmiş standartlar doğrultusunda planlanır, gerçekleştirilir ve geliştirilir.
- EYS hedefleri, politika çerçevesinde periyodik olarak belirlenir. Sistemin etkinliği, hedeflere ulaşma düzeyi ve risk durumu, üst yönetime periyodik olarak raporlanır. Yönetim, raporlar doğrultusunda stratejik kararlar alır ve gerekli kaynakları tahsis eder.
- EYS’nin sürekli iyileştirilmesi için gerekli iç denetim, yönetimin gözden geçirmesi, düzeltici faaliyetler ile risklerin ve fırsatların belirlenmesi için atılması gerekli adımlar, yönetim ve yönetimin bilgi güvenliği sorumluluğunu verdiği ekipler tarafından sağlanır. Bilgi güvenliği ile ilgili tüm rol ve sorumluluklar belirlenir ve yönetim tarafından yetkilendirmeler yapılır.
- Entegre yönetim sistemi çerçevesinde gerekli çalışmaların gerçekleştirilmesi için kaynaklar ve yönlendirmeler yönetim tarafından sağlanır.
- Tüm çalışanların yetkinliklerinin ve yönetim sistemlerine bağlılıklarının sürdürülmesi amacıyla, düzenli eğitimler ve farkındalık çalışmaları yürütülür. Açık ve şeffaf bir iletişim ortamı oluşturularak, çalışanların bilgi ve deneyimleri doğrultusunda sistemin sürekli iyileştirilmesine katılımı sağlanır.
- Paydaşları ile birlikte kuruluşun rekabet avantajını olumsuz yönde etkileyebilecek maddi ve manevi kayıplar engellenir.
- Entegre Yönetim Sistemi kapsamında, bilgi varlıkları belirlenir, müşteriler, tedarikçiler ve iş ortakları gibi ilgili tarafların bilgi güvenliği beklentileri değerlendirilir, yasal ve sözleşmelere bağlı yükümlülükler değerlendirilir.
- BİLTİM entegre yönetim sistemi ile ilgili tüm yasal, mevzuat ve sözleşme gerekliliklere uymayı taahhüt eder. Tüm sözleşmelerde bilgi güvenliği gereksinimleri, gizlilik hükümleri, veri koruma ve ihlal bildirim yükümlülükleri açıkça tanımlanır.
  Üçüncü taraflarla yapılan anlaşmalarda bilgi güvenliği kontrollerinin entegrasyonu sağlanır.
- Bilgi güvenliği ihlal olayı yaşama ihtimalini düşürmek için gerekli çalışmalar yapılır, yaşanması durumunda koordineli şekilde yanıt verilir.
- Kuruluş, bilgi güvenliği ihlallerine karşı Siber Olay Müdahale Ekibi (SOME) planlarını oluşturur, uygular ve test eder.

- Tüm bilgi sistemleri, cihazlar ve ağ bileşenleri; yetkisiz erişimi, yetki aşımını ve güvenlik açıklarını en aza indirmek amacıyla kurum tarafından belirlenen güvenlik standartları ve en iyi uygulamalar doğrultusunda güvenli bir şekilde yapılandırılır ve yönetilir. Kritik güvenlik yamaları ve güncellemeler düzenli olarak uygulanır.
- Entegre yönetim sistemi kapsamında riskleri yönetmek için, risk değerlendirme, risk analizi ve risk işleme çalışmaları gerçekleştirilerek, gerekli tedbirler ve olası riskleri önlemek için çalışmalar gerçekleştirilir.
- Müşteri ve paydaşlarının kişisel verileri dahil tüm bilgilerinin yetkisiz kişilerin eline geçmesi engellenir. Kişisel Verilerin Korunması Kanunu dahil ilgili kanun ve yönetmeliklerle uyumlu hale gelmesi için gereken çalışmalar yapılır.
- Yeni teknolojilerin devreye alınması öncesinde, bilgi güvenliği perspektifinden güvenlik değerlendirmeleri gerçekleştirilir.
- Bilgi güvenliğini etkin biçimde yöneterek bilgi güvenliği kaynaklı yaşanabilecek zararlar asgariye indirilir.
- Kritik iş süreçlerinde yaşanabilecek kesintilerin önüne geçilmesi için gerekli düzenlemeler yapılır, geçilemediği durumda hedeflenen kurtarma süresi içerisinde tekrar çalışabilir hale gelmesi sağlanır.
- Bilgi Güvenliği Yönetim Sistemi kapsamında müşterilerimizin bilgi varlıklarının gizliliği, bütünlüğü ve erişilebilirliği sağlanır.
- Entegre yönetim sistemi içerisinde ele alınan değişiklik süreçlerinin yaşam döngüsü içerisinde işletilmesi sağlanır.
- Yönetim sistemlerinin amaçlanan sonuçları yerine getirme başarısı periyodik olarak gözden geçirilir, gerekli iyileştirmelerin zamanında hayata geçirilmesi güvence altına alınır.
- Müşterilerine ve paydaşlarına sunduğu ürün ve hizmetlere ilişkin faaliyetlerinin güvenliğinin sağlanmasına önem vermekte, İş süreçleri ile entegre, uyumlu ve dengeli olması hedeflenir.
- Entegre ve dinamik iş stratejisi bilgi varlıklarının güvenliğini ve sürekliliğini gerekli kılar.
- Güvenli çalışma alanları, arşiv odaları, sistem odaları gibi kurum içi çalışma bölgelerinde ve kurum çevresinde güvenliğin sağlanması için gerekli önlemlerin alınması sağlanır.
- Tedarikçi ilişkilerinin güvenli bir şekilde yürütülmesi amacıyla; tedarik hizmetlerinin gözden geçirilmesi, meydana gelen değişikliklerin yönetilmesi için politikalar oluşturulur, özellikle bilgi teknolojileri tedarikçileri ile yapılan/yapılacak olan ve bilgi güvenliği risklerinin ifade edildiği anlaşmalarda güvenlik gereksinimleri belirlenir.

Abdulkadir ÜÇÜNCÜ

Genel Müdür