BGYS HEDEFLERİ VE PRENSİPLERİ

BGYS Politikası, İKÜ çalışanları ve ilgili tarafların bilgi güvenliği gereksinimlerine uygun şekilde hareket etmesi konusunda yol göstermek, personelin bilinç ve farkındalık seviyelerini artırmak ve bu şekilde İKÜ bünyesinde oluşabilecek riskleri asgari düzeye indirmek, İKÜ'nün itibarını ve bilgi güvenliği imajını korumak, üçüncü taraflarla yapılan sözleşmelerde belirlenmiş gizlilik ve uygunluğu temin etmek, teknik açıdan bilgi güvenliği tedbirlerini almak, kurumun temel ve destekleyici iş faaliyetlerinin en az kesinti ile devam etmesini sağlamayı hedeflemektedir.

BGYS kapsamındaki bilgi varlığı ve iş süreçlerinde gizlilik, bütünlük ve erişilebilirlik prensiplerine uygun tedbirler alınmasına istinaden, risk yönetimi faaliyetleri gerçekleştirilmektedir. Söz konusu risk yönetimi faaliyetlerinde amaç, İKÜ bünyesinde bulunan bilgi varlıkları için risk seviyesini kabul edilebilir risk seviyesinin altında tutmaktır. Risk yönetimi ve kontrollerin uygulanması dinamik bir BGYS sürecinin parçasıdır. Kabul edilebilir risk seviyesinin altında kalan bilgi varlıkları için de aksiyonlar atanarak iyileştirme çalışmaları yapılması amaçlanmaktadır.

Temel prensiplerimiz; Bilgi güvenliği kapsamında yer alan basılı ve elektronik ortamdaki tüm bilgilerin, yasal mevzuat ışığında ve risk değerlendirme metotları kullanılarak "gizlilik, bütünlük ve erişilebilirlik" ilkelerine göre yönetilmesi amacıyla;

i. Bilgi güvenliği standartlarının gerekliliklerini yerine getirmek,
ii. Bilgi güvenliği ile ilgili tüm yasal mevzuata BGYS kılavuzu çerçevesinde uyum sağlamak,
iii. Bilgi varlıklarına yönelik riskleri tespit etmek ve sistematik bir şekilde riskleri yönetmek,
iv. BGYS'yi sürekli gözden geçirmek ve iyileştirilmesi için BGYS'ye katkıda bulunmak,
v. Bilgi güvenliği farkındalığını artırmak için teknik ve davranışsal yetkinlikleri geliştirecek şekilde eğitimler gerçekleştirme vizyon ve misyonuyla hareket etmektedir.

BİLGİ GÜVENLİĞİ İLKELERİ

1.1. Bilgi güvenliği ilkeleri, İKÜ bilgi güvenliği ile ilgili genel kuralları ortaya koyar. Bu ilkeler kullanıcılara çeşitli konu ve kavramlarla ilintili beklenen davranışları tanımlar.

1.2. Bilgi sistemleri ve teknolojileri altyapısını kullanan ve bilgi kaynaklarına erişen İKÜ Personeli:

i. Kişisel ve elektronik iletişimde ve üçüncü taraflarla yapılan bilgi alışverişlerinde kuruma ait bilginin gizliliğini sağlamalı,
ii. Kritiklik düzeylerine göre işlediği bilgiyi yedeklemeli,
iii. Risk düzeylerine göre belirlenen güvenlik önlemlerini almalı,
iv. Bilgi güvenliği ihlal olaylarını Bilgi Güvenliği Yetkilisine bildirmeli, raporlamalı ve bu ihlalleri engelleyecek önlemleri almalıdır.

1.3. İKÜ sahipliğindeki bilgi kaynakları (duyuru, doküman vb.) yetkisiz olarak 3.kişilere iletilemez.

1.4. İKÜ bilişim kaynakları, T.C. Yasalarına ve bunlara bağlı yönetmeliklere aykırı faaliyetler amacı ile kullanılamaz.

1.5. İKÜ'nün tüm çalışanları; bu politika ile diğer desteklenen politikalara, prosedürlere ve talimatlarına, formlar ve sözleşme gerekliliklerine uymakla sorumludur.

1.6. İş süreçlerinin gereksinimi olarak her türü bilgi, en az kesintiyle kapsam dâhilindeki birimler, hizmet verenler ve gereken üçüncü taraflarca erişilebilir olacaktır.

1.7. Bilgilerin bütünlüğü her durumda korunacaktır.

1.8. Hizmet alanlar ve verenler ya da üçüncü taraflara ait olmasına bakılmaksızın, üretilen ve/veya kullanılan bilgilerin gizliliği her durumda güvence altına alınacaktır.

1.9. BGYS'nin tasarımı, uygulaması ve sürdürülmesi aracılığıyla riskler kabul edilebilir düzeye indirilecektir.

1.10. Bilgi; bilginin elektronik iletişimi, üçüncü taraflarca paylaşımı, araştırma amaçlı kullanımı, fiziksel ya da elektronik ortamda depolanması gibi kullanım biçimlerinden bağımsız olarak korunacaktır.