



POL.021 BİLGİ GÜVENLİĞİ POLİTİKASI

- Üst yönetim bilgi güvenliği ve kişisel veri güvenliği gereksinimlerini tanımlanmış, kabul edilmiş kuralları uygulamayı taahhüt eder.
- Kurum çalışanları ve ilgili taraflar bilgi güvenliği ve kişisel veri güvenliği şartlarına uygun çalışmakla yükümlüdür.
- Üst yönetim, kurumsal ve kişisel bilgilerin gizlilik, bütünlük, erişilebilirlik kayıplarını önlemek, en aza indirmeyi taahhüt eder.
- Üst yönetim bilgi ve kişisel veri güvenliğinin sürekli iyileştirilmesini taahhüt eder.
- Üst yönetim, yasa, mevzuat, sözleşme ve regülasyonlara uyum sağlayacağını taahhüt eder.
- BGYS ve KVYS'nin hayata geçirilmesi, işletilmesi ve iyileştirilmesi için çalışmalarını, ilgili tarafların katkısıyla yürütür. BGYS ve KVYS dokümanlarının gerektiği zamanlarda güncellenmesi BGYS Yöneticisinin sorumluluğundadır. Kurum Bilgi Güvenliği Politikası kapsamında; Kurum Üst Yönetimi ve Bilgi İşlem Birimi olarak aşağıdaki standartları uygulayacaktır.;
- Kurum'un yasal uygunluğunu ve kurumsal imajını korumak,
- Personelin ve kurum dışı tarafların bilgi varlıklarına ve kişisel verilerine güvenli bir şekilde erişimini sağlamak,
- İş sürekliliğini ve sürdürülebilirliğini sağlamak,
- Bilgi ve kişisel veri güvenliği ihlali durumunda yaptırımları sağlamak amacıyla, kurum çapında gizliliği, bütünlüğü ve erişilebilirliği tüm fiziksel ve elektronik bilgi varlıklarını korumak için taahhütte bulunmuştur.
- Kişisel veri ve bilgi güvenliği gereksinimleri kurumsal hedefler ile aynı doğrultuda olacaktır.
- BGYS ve KVYS bilgi ile ilgili riskleri kabul edilebilir düzeylere indiren ve bilgi paylaşımı olanağı veren bir mekanizma olacaktır.
- Kurum'un mevcut stratejik iş planı ve risk yönetimi çerçevesi, BGYS ve KVYS'nin kurulup sürekliliğinin sağlanması için ilgili riskleri tanımlamak, belirlemek, değerlendirmek ve kontrol etmek işlevini yerine getirmektedir.
- Risk değerlendirme, Uygulanabilirlik Bildirimi ve risk müdahale planı, bilgi ile ilgili risklerin nasıl kontrol edildiğini açıklamaktadır.
- Bilgi İşlem Müdürü ve Bilgi Güvenliği Yöneticisi, risk müdahale planının yönetiminden ve sürdürülmesinden sorumludur.
- Ek risk değerlendirmeleri, gerekli olduğu takdirde, belirli riskler için uygun kontroller belirlemek amacıyla yürütülebilir. İş sürekliliği ve beklenmedik durum planları, veri yedekleme prosedürleri, virüslerden ve bilgisayar korsanlarından sakınma, erişim kontrol sistemleri ve bilgi güvenliği ihlal bildirimleri, bu politika için esastır. Bu alanların her biri için kontrol hedefleri BGYS ve KVYS Uygulanabilirlik Bildirgesinde yer alır ve belirli, dokümanite edilmiş politikalar ve prosedürler ile desteklenir.

Revizyon No : 2 Dokümanı Oluşturan : Ali Rıza Tali Oluşturma Tarihi : 30.7.2024 Dokümanı Değiştiren : Ali Rıza Tali Değiştirme Tarihi : 10.11.2024 Dokümanı Onaylayan :



POL.021 BİLGİ GÜVENLİĞİ POLİTİKASI

- Tüm Kurum çalışanlarının ve BGYS ve KVYS' de tanımlanan belirli kurum dışı tarafların bu politikaya ve bu politikayı uygulayan BGYS ve KVYS' ne uymaları amacıyla tüm personel uygun eğitimi alacaklardır.
- Bilgi Güvenliği Yönetim sistemi ve Kişisel Veri Ynetim sistemi standartında tanımlanan gerekliliklerle uyumlu olarak tasarlanmış, sürekli iyileştirilmesi ve sistematik değerlendirme ile geliştirilmesi için üst yönetim tarafından gerekli kaynaklar ayrılmıştır.
- Kurum Bilgi Güvenliği Yönetim Sistemi ve Kişisel Veri Yönetim Sistemi sertifikasyonunu sürdürülebilir kılmayı taahhüt etmiştir.

**Revizyon No : 2 Dokümanı Oluşturan : Ali Rıza Tali Oluşturma Tarihi :
30.7.2024 Dokümanı Değiştiren : Ali Rıza Tali Değiştirme Tarihi :
10.11.2024 Dokümanı Onaylayan :**