BİLGİ-KALİTE GÜVENLİĞİ YÖNETİM SİSTEMİ POLİTİKASI
BGYS.PLT.00

HİZMET İHRACATÇILARI BİRLİĞİ GENEL SEKRETERLİĞİ (HİB) üst yönetimi olarak;

HİZMET İHRACATÇILARI BİRLİĞİ GENEL SEKRETERLİĞİ (HİB) Hizmetlerinde**; ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi (BGYS)** standardında kurulan sistemlerin ana teması; insan, altyapı, yazılım, donanım, müşteri bilgileri, kuruluş bilgileri, tüm iş ve işlemler, üçüncü şahıslara ait bilgiler ve finansal kaynaklar içerisinde bilgi güvenliği yönetiminin sağlandığını göstermek, kalite ve risk yönetimini güvence altına almak, bilgi-kalite güvenliği yönetimi süreç performansını ölçmek ve kalite-bilgi güvenliği ve müşteri memnuniyeti ile ilgili konularda üçüncü taraflarla olan ilişkilerin düzenlenmesini sağlamaktır.

Bu doğrultuda ***BGYS Politikamızın*** amacı:

- İçeriden veya dışarıdan, bilerek ya da bilmeyerek meydana gelebilecek her türlü tehdide karşı **HİZMET İHRACATÇILARI BİRLİĞİ GENEL SEKRETERLİĞİ (HİB)** bilgi varlıklarını korumak, bilgiye erişebilirliği iş prosesleriyle gerektiği şekilde sağlamak, yasal mevzuat gereksinimlerini karşılamak, sürekli iyileştirmeye yönelik çalışmalar yapmak,
- Yürütülen tüm faaliyetlerde Bilgi Güvenliği Yönetim Sisteminin üç temel öğesinin sürekliliğini sağlamak.

Gizlilik: Önem taşıyan bilgilere yetkisiz erişimlerin önlenmesi,
Bütünlük: Bilginin doğruluk ve bütünlüğünün sağlandığının gösterilmesi,
Erişebilirlik: Yetkisi olanların gerektiği hallerde bilgiye ulaşılabilirliğinin gösterilmesi,
Liderlik ve Bağlılık: Birliğimiz Üst yönetimi BGYS kurulmasında ve uygulanmasında liderlik etmekte, BGYS uygulamalarına üst düzeyde katılım sağlamaktadır.

- Sadece elektronik ortamda tutulan verilerin değil; yazılı, basılı, sözlü ve benzeri ortamda bulunan tüm verilerin güvenliği ile ilgilenmek.
- Bilgi Güvenliği Yönetimi eğitimlerini tüm personele vererek bilinçlendirmeyi sağlamak.
- Bilgi Güvenliğindeki gerçekte var olan veya şüphe uyandıran tüm açıklıkların, BGYS Ekibine rapor etmek ve BGYS Ekibi tarafından soruşturulmasını sağlamak.
- İş süreklilik planları hazırlamak, sürdürmek ve test etmek.
- Bilgi Güvenliği konusunda periyodik olarak değerlendirmeler yaparak mevcut riskleri tespit etmek. Değerlendirmeler sonucunda, aksiyon planlarını gözden geçirmek ve takibini yapmak.
- Sözleşmelerden doğabilecek her türlü anlaşmazlık ve çıkar çatışmasını engellemek.
- Bilgiye erişilebilirlik ve bilgi sistemleri için iş gereksinimlerini karşılamaktadır.

Taahhüt ederiz.