BİLGİ GÜVENLİĞİ POLİTİKAMIZ

TS EN ISO/IEC 27001:2013 Bilgi Güvenliği Yönetim Sistemin ana teması; **Hizmet İhracatçıları Birliği Genel Sekreterliği'nde**; insan, alt yapı, yazılım, donanım, müşteri bilgileri, kuruluş bilgileri, üçüncü şahıslara ait bilgiler ve finansal kaynaklar içerisinde bilgi güvenliği yönetiminin sağlandığını göstermek, risk yönetimini güvence altına almak, bilgi güvenliği yönetimi süreç performansını ölçmek ve bilgi güvenliği ile ilgili konularda üçüncü taraflarla olan ilişkilerin düzenlenmesini sağlamaktır.

Bu doğrultuda BGYS Politikamızın amacı ile birlikte üst yönetim olarak aşağıdakilerin sağlanacağını taahhüt ederiz:

- İçeriden veya dışarıdan, bilerek ya da bilmeyerek meydana gelebilecek her türlü tehdide karşı **Hizmet İhracatçıları Birliği Genel Sekreterliği** bilgi varlıklarını korumak, bilgiye erişilebilirliği iş prosesleriyle gerektiği şekilde sağlamak, yasal mevzuat gereksinimlerini karşılamak, sürekli iyileştirmeye yönelik çalışmalar yaparak, Bilgi İşlem, İdari İşler ve Satın Alma ile İnsan Kaynakları şubelerinde **TS EN ISO/IEC 27001:2013** standardı kapsamında Bilgi Güvenliği Yönetim Sistemi kurmak,
- 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,

Erişilebilirlik: Yetkisi olanların gerektiği hallerde bilgiye ulaşabildiğinin gösterilmesi,

- HİB' in işlediği ve sakladığı bütün kişisel verileri, Kişisel Verilerin Korunması Kanunu kapsamında hazırlanan, HİB Kişisel Verilerin Korunması ve İşlenmesi Politikası' na uygun olarak korumak, saklamak ve işlemek,
- 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 karşılamaktır.