ISO 27701 Kişisel Veri Yönetim Sistemi ve ISO 27001:2022 Bilgi Güvenliği Yönetim Sistemin ana teması Kişisel Veri ve Bilgi Güvenliği Faaliyetleri kapsamında; insan, alt yapı, yazılım, donanım, 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 ***KVYS-BGYS Politikamız*** kapsamında;

- *İçeriden veya dışarıdan, bilerek ya da bilmeyerek meydana gelebilecek her türlü tehdide karşı bilgi varlıklarını korumak, bilgiye erişebilirliği iş prosesleriyle gerektiği şekilde sağlamak, yasal mevzuat gereksinimlerini karşılamak, sürekli iyileştirmeye yönelik çalışmalar yapmak.*
- *Kişisel veri ve bilgi varlıklarını yönetmek, varlıkların güvenlik değerlerini, ihtiyaçlarını ve risklerini belirlemek, güvenlik risklerine yönelik kontrolleri geliştirmek ve uygulamak.*
- *Yürütülen tüm faaliyetlerde Kişisel Veri ve Bilgi Güvenliği Yönetim Sisteminin üç temel öğesinin sürekliliğini sağlamak.*

  Gizlilik: *Bilgi ve bilgi varlıklarına yetkisiz erişimlerin önlenmesi,*
  Bütünlük: *Bilginin doğruluk ve bütünlüğünün sağlandığının gösterilmesi,*
  Erişebilirlik: *Yetkisi olanların gerektiği hallerde bilgiye ulaşılabilirliğinin gösterilmesi,*

- *Kişisel veri, bilgi varlıkları, değerleri, güvenlik ihtiyaçları, zafiyetleri, varlıklara yönelik tehditlerin, tehditlerin sıklıklarının saptanması için yöntemlerin belirleyeceği çerçeveyi tanımlamak.*
- *Risklerin işlenmesi için finansal kaynak ve personel sağlamak.*
- *Hizmet verilen kapsam bağlamında teknolojik beklentileri gözden geçirerek riskleri sürekli takip etmek.*
- *Ulusal veya uluslararası düzenlemeler, yasa ve ilgili mevzuat gereklerini yerine getirmek; anlaşmalardan doğan yükümlülüklerini karşılamak, iç ve dış paydaşlara yönelik kurumsal sorumluluklarından kaynaklanan bilgi güvenliği gereksinimlerini sağlamak.*
- *Hizmet sürekliliğine yönelik bilgi güvenliği tehditlerinin etkisini azaltmak ve sürekliliğe katkıda bulunmak.*
- *İş süreklilik planları hazırlamak, sürdürmek ve test etmek.*
- *Sürekli iyileştirmeyi sağlamak.*

Faaliyetleri gerekliliklerini yerine getirmeyi sürdüreceğimizi taahhüt ederiz.

HAZIRLAYAN	ONAYLAYAN
YÖNETİM TEMSİLCİSİ	GENEL MÜDÜR