TS EN ISO 27001:2013 Bilgi Güvenliği Yönetim Sisteminin ana teması; Haker; insan, altyapı, yazılım, donanım, kullanıcı bilgileri, cari bilgiler, 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 Politikamız'ın** amacı;

- İçeriden veya dışarıdan, bilerek ya da bilmeyerek meydana gelebilecek her türlü tehdide karşı Haker'in bilgi varlıklarını korumak, bilgiye erişilebilirliği iş süreçleriyle gerektiği şekilde sağlamak, yasal mevzuat gereksinimlerini karşılamak, sürekli iyileştirmeye yönelik çalışmalar yapmak,
- Bilgi güvenliği temel unsurları gizlilik, bütünlük ve erişilebilirliğe bağlı olarak, kullanıma sunulan bilgi varlıklarının izinsiz veya yetkisiz bir biçimde erişimi, kullanımı, değiştirilmesi, ifşa edilmesi, ortadan kaldırılması, el değiştirmesi ve hasar verilmesini önlemek,
- Bilgi güvenliği varlıklarında sadece elektronik ortamda tutulan verilerin değil; yazılı, basılı, sözlü ve benzeri ortamda bulunan tüm verilerin güvenliği ile ilgilenmek,
- Haker'in kuruluş amacı doğrultusunda 6698 sayılı kanunun yasal şartlarının uygulanmasını sağlayacak tedbirleri almak, uygulamak ve sürekli iyileştirmek,
- Yasalar çerçevesinde sistemimize kayıt olan müşterilerimizin sunulan hizmet kapsamında ağ bağlatısı mimarisinin ip adresi bazlı yapılan saldırılardan belirli seviyede korumak.
- Bilgi Güvenliği Yönetimi ve farkındalık eğitimlerini tüm personele vererek bilinçlendirmeyi sağlamak,
- BTK / USOM birimi tarafından tespit edilen zafiyetlerin önüne geçilmesini sağlamak.
- Haker personelinin bilgi güvenliğine bilinçli yaklaşımı ve sorumluluk alanlarına düşen görevleri yerine getirmesi, yayınlanan politika, prosedür, talimat ve duyurulara azami derecede özen göstermesini sağlamak,
- Bilgi Güvenliğini hedef alan gerçekte var olan veya şüphe uyandıran tüm açıklıkları Haker kapsamı ile bilgi güvenliği olay yönetimi kapsamında değerlendirilmesi ve yapılan değerlendirmeler neticesinde, mevcut kontrollerin güncellenmesi veya yeni kontrollerin devreye alınması faaliyetleri en kısa zamanda gerçekleştirilmesini 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,
- Bilgi Güvenliği Politikamızda yer alan amaçları destekleyen çalışmaların, her yıl oluşturulan Bilgi Güvenliği Hedeflerinde yer almasını ve bu çalışmaların ilerleme durumlarının, yıl içinde takip edilmesini ve raporlanmasını sağlamak,
- Bilgi Güvenliği Yönetim Sisteminin sürekli iyileştirilmesi sağlamak ve sürekli iyileştirmeye yönelik çalışmaların yönetim tarafından gözden geçirilmesini sağlamaktır.