SANKO
ÜNİVERSİTESİ

BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ POLİTİKASI

SANKO Üniversitesi bilgi güvenliği politikası; insan, alt yapı, yazılım, donanım, öğrenci 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 sağlamak;

- Üniversite içerisinden veya dışarıdan, bilerek ya da bilmeyerek meydana gelebilecek her türlü tehdide karşı kuruluşun bilgi varlıklarının gizliliğini, bütünlüğünü ve erişilebilirliğini korumak,
- 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.
- Sadece elektronik ortamda tutulan verilerin değil; yazılı, basılı, sözlü ve benzeri ortamda bulunan tüm verilerin güvenliğini sağlamak,
- Bilgi Güvenliği Yönetimi eğitimlerini tüm personele vererek bilinçlendirmeyi sağlamak,
- Bilgi güvenliğindeki gerçekte var olan veya şüphe uyandıran tüm açıklıkların, BGYS Ekibine rapor edilmesi 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 ve değerlendirmeler sonucunda aksiyon planlarını gözden geçirerek, takibini yapmak.
- Sözleşmelerden doğabilecek her türlü anlaşmazlık ve çıkar çatışmasını engellemek,
- Bilgiye erişilebilirlik ve bilgi sistemleri için iş gereksinimlerini karşılamak,
- Bilgi güvenliği farkındalığının artırılmasına yönelik çalışmaları gerçekleştirmek,
- Tabi olduğu ulusal veya uluslararası düzenlemelerden, yasal ve ilgili mevzuat gereklerini yerine getirmekten, anlaşmalardan doğan yükümlülüklerini karşılamaktan, iç ve dış paydaşlara yönelik kurumsal sorumluluklarından kaynaklanan bilgi güvenliği gereksinimlerini sağlamak,
- Kurum itibarını geliştirmek, bilgi güvenliği temelli olumsuz etkilerden korumaktır.