



BİLGİ GÜVENLİĞİ POLİTİKASI

Hitit Üniversitesi, bilgi güvenliğini; stratejik planı, kurumsal kalite güvencesi sistemi ve dijital dönüşüm hedefleriyle bütünleşik biçimde ele alan, risk temelli ve sürekli iyileştirmeye dayalı bir yönetim yaklaşımı çerçevesinde yönetir. Bu kapsamda bilgi güvenliğini sağlamaya yönelik süreçlerini, üniversitenin tüm akademik ve idari faaliyetlerinde güvenilir, sürdürülebilir ve şeffaf bir dijital ortamın oluşturulması ile yürütmeyi temel ilke olarak benimser.

Bu doğrultuda Hitit Üniversitesi bilgi güvenliği politikası;

- Üniversitenin ve paydaşlarının bilgi varlıklarına güvenli ve kontrollü biçimde erişmesini; kurum bünyesinde üretilen veya kullanılan tüm bilginin gizliliğinin, bütünlüğünün ve erişilebilirliğinin korunmasını,
- Akademik, idari ve araştırma süreçlerinde kullanılan dijital ve fiziksel bilgi varlıklarının yetkisiz erişim, değiştirme, kayıp, bozulma ve kötüye kullanıma karşı korunmasını,
- Bilgi varlıklarına yönelik tehdit ve risklerin sistematik biçimde tanımlanmasını, değerlendirilmesini ve yönetilmesini,
- Kurumun itibarı, güvenilirliği ve paydaş güveninin bilgi güvenliği uygulamaları yoluyla güçlendirilmesini,
- Ulusal mevzuat, uluslararası standartlar ve üniversitenin tabi olduğu yasal yükümlülükler çerçevesinde bilgi güvenliği gerekliliklerinin eksiksiz yerine getirilmesini,
- Kişisel veriler, akademik veriler, araştırma çıktıları, öğrenci ve personel bilgileri ile kurumsal verilerin korunmasını ve güvenli biçimde işlenmesini,
- Bilgi güvenliği ihlallerinin önlenmesini; meydana gelmesi halinde etkilerinin en aza indirilmesini ve gerekli müdahale ve bildirim süreçlerinin işletilmesini,
- Üniversitenin dijital hizmetlerinin sürekliliğini destekleyecek yedekleme, kurtarma, erişim kontrolü ve olay yönetimi mekanizmalarının kurulmasını ve işletilmesini,
- Bilgi güvenliği süreçlerini destekleyecek teknik altyapı, yazılım, donanım ve insan kaynağının sürdürülebilir biçimde sağlanmasını,
- Bilgi güvenliği uygulamalarının kurumsal kalite güvencesi ve risk yönetimi süreçleri ile bütünleşik biçimde izlenmesini, değerlendirilmesini ve iyileştirilmesini,
- Bilgi güvenliğini sağlamaya yönelik faaliyetlerini kurumsal kalite güvencesi sisteminin bir parçası olarak uygulamayı, izlemeyi ve sürekli geliştirme çerçevesinde yönetmeyi

esas alır.