BİLGİ GÜVENLİĞİ POLİTİKASI

Sağlık Bilimleri Üniversitesi (SBÜ); eğitim-öğretim, araştırma, sağlık hizmeti sunumu ve idari faaliyetleri kapsamında üretilen, işlenen, saklanan ve iletilen tüm bilgi varlıklarının gizliliğini, bütünlüğünü ve erişilebilirliğini korumayı temel bir kurumsal sorumluluk olarak kabul eder. Bu politika, ISO/IEC 27001:2022 standardının gereksinimleri doğrultusunda üniversitemizin tüm kampüslerini (Hamidiye, Gülhane, Selimiye, DETUAM ve diğer kampüsler) ve bu kampüslerde görev yapan personeli, akademisyenleri, öğrencileri, paydaşları, tedarikçileri ile bilgi varlıklarına erişim sağlayan tüm ilgili tarafları kapsar.

SBÜ üst yönetimi, Bilgi Güvenliği Yönetim Sistemi (BGYS) kapsamında;

- Üniversitenin misyon, vizyon ve stratejik hedefleriyle uyumlu bilgi güvenliği hedeflerinin belirlenmesi için bir çerçeve oluşturmayı ve bu hedeflerin düzenli aralıklarla gözden geçirilmesini sağlamayı,
- Bilgi güvenliği risklerinin sistematik olarak belirlenmesi, analiz edilmesi ve değerlendirilmesi amacıyla risk yönetim metodolojisini kurumumuz, personelimiz, akademisyenlerimiz, öğrencilerimiz, paydaşlarımız ve tedarikçilerimiz için kurmayı ve risklere ilişkin uygun kontrol önlemlerinin alınmasını sağlamayı,
- Bilgi İşlem Daire Başkanlığı faaliyetleri kapsamında hizmet kalitesini sürekli iyileştirmeyi,
- Bilgi güvenliği risklerini azaltmak için gerekli insan kaynağı, donanım, yazılım, eğitim ve diğer kaynakları tahsis etmeyi ve bu kaynakların devamlılığını sağlamayı,
- Bilgi güvenliğinin ihlali durumunda gerekli görülen yaptırımları uygulamayı,
- 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) başta olmak üzere bağlı olunan ulusal, uluslararası ve sektörel düzenlemelere, yasal ve ilgili mevzuat gereklerine uymayı, anlaşmalardan doğan yükümlülükleri karşılamayı, iç ve dış paydaşlara yönelik kurumsal sorumluluklarından kaynaklanan bilgi güvenliği gereksinimlerini sağlamayı,
- Tüm personelin ve iş ortaklarının bilgi güvenliğinin sağlanmasındaki süreçlere katılımını ve uymasını sağlamak için bilinçlendirme, eğitim ve teşviki düzenli olarak planlamayı ve uygulamayı,
- Bilgi güvenliği olaylarının raporlanması, değerlendirilmesi ve müdahale süreçlerinin etkin şekilde işletilmesi için gerekli mekanizmaları tesis etmeyi,
- İş sürekliliği yönetimi kapsamında kritik bilgi sistemlerinin kesintisiz hizmet verebilmesi için gerekli planları oluşturmayı ve düzenli olarak test etmeyi,

- BGYS'nin verimliliğini iç ve dış denetimlerle kontrol etmeyi, izlemeyi, gözden geçirmeyi ve sistemi sürekli uyumlu kılmayı, sürekli iyileştirmeyi,

BGYS politikası olarak benimser ve taahhüt eder.