1. AMAÇ

Bu politikanın amacı; Adıyaman Üniversitesi'nin kurumsal bilgi varlıklarının gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak üzere gerekli yönetsel ve operasyonel çerçeveyi ortaya koymaktır. Bu doğrultuda; üniversitede iş sürekliliğini sağlamak, bilgi güvenliği risklerini en aza indirmek, güvenlik ihlallerinin önüne geçmek ve meydana gelebilecek güvenlik olaylarının etkilerini azaltarak oluşabilecek zararları minimum seviyede tutmak hedeflenmektedir.

2. KAPSAM

Bu politika; Adıyaman Üniversitesi bünyesinde kurumsal bilgilere erişen, bu bilgileri işleyen veya yöneten akademik ve idari personeli, öğrencileri, ziyaretçileri, üniversite ile iş ilişkisi bulunan üçüncü tarafları (tedarikçiler, yükleniciler vb.) ve eduroam ağı üzerinden üniversite ağına bağlanan tüm kullanıcıları kapsamaktadır.

3. SORUMLULUKLAR

Bu politika metninin hazırlanması ve koordinasyonundan BGYS Yöneticisi; periyodik olarak gözden geçirilmesinden ise Bilgi Güvenliği Kurulu sorumludur. Hazırlanan politika metni Üst Yönetim (Rektörlük) onayı ile yürürlüğe girer. Politikada belirtilen ilke ve kuralların akademik/idari personel ve öğrenciler tarafından bilinmesi ve uygulanması; ziyaretçiler ile üçüncü tarafların (tedarikçi, yükleniciler vb.) ise bu kurallara uyması zorunludur.

4. POLİTİKA İLKELERİ VE TAAHHÜTLER

Bilgi Güvenliği Politikası aşağıdaki hususları güvence altına almayı taahhüt eder:

- T.C. yasaları, yönetmelikler, genelgeler ve işin gerektirdiği yasal mevzuat ile belirlenmiş gereksinimler ile uluslararası anlaşmalardan doğan yükümlülükleri karşılamak; iç ve dış paydaşlara yönelik sorumluluklardan kaynaklanan bilgi güvenliği gereksinimlerini sağlayarak bunlarla uyumlu çalışmalar yürütmek,
- Bilgi varlıklarını bilerek veya bilmeyerek yapılabilecek yetkisiz erişim, kullanım, değiştirilme, açıklanma ve hasara karşı korumak,
- Personelin, öğrencilerin, tedarikçilerin ve ziyaretçilerin yetkileri dahilinde bilgi varlıklarına güvenli, hızlı, doğru ve etkin bir biçimde erişimini sağlamak,
- İş sürekliliğini etkileyebilecek riskleri sistematik bir şekilde tanımlamak, analiz etmek ve kabul edilebilir düzeylere indirmek,
- Görevler ayrılığı ilkesini uygulayarak bilgi güvenliğinin korunmasına yönelik teknolojik yatırımları sürdürmek,
- Tüm kurum çalışanlarına ve gerektiğinde tedarikçi çalışanlarına yönelik, bilgi güvenliği farkındalığını artırıcı düzenli eğitimler sunmak ve sisteme katkılarını teşvik etmek,
- Gerçek ya da şüpheli tüm bilgi güvenliği ihlallerini raporlamak, kayıt altına almak ve tekrarını engelleyici önlemleri devreye almak,
- Bilgi Güvenliği Yönetim Sisteminin (BGYS); Cumhurbaşkanlığı Siber Güvenlik Başkanlığı Bilgi ve İletişim Güvenliği Rehberi, ISO/IEC 27001:2022 standardı şartları ve yasal mevzuat gereksinimleri ile uyumlu olarak belgelendirilmesini, yürütülmesini ve sürekli iyileştirilmesini sağlamak,
- Bilgi Güvenliği Yönetim Sisteminin uygulanması, sürdürülmesi ve iyileştirilmesi için gerekli tüm kaynakları sağlamak,
- Bu politikalara uyulmaması halinde, ilgili mevzuat ve disiplin hükümleri çerçevesinde gerekli idari ve/veya hukuki süreçlerin başlatılmasını sağlamak.