OSMANİYE KORKUT ATA ÜNİVERSİTESİ

BİLGİ YÖNETİM SİSTEMİ POLİTİKASI

"Bu politika belgesi, Osmaniye Korkut Ata Üniversitesi'nin Kurumsal Değerler Çerçevesi temel alınarak hazırlanmıştır. Stratejik hedeflerle uyumlu biçimde yürütülen bilgi güvenliği yönetimi süreçlerinde, değer temelli bir yaklaşım esas alınır. Politika, özellikle Etik Sorumluluk, Şeffaflık ve Hesap Verebilirlik, Veriye Dayalı Yönetim, Dijital Dönüşüm, Esneklik ve Dayanıklılık, Kalite Odaklılık ve Kurumsal Öğrenme değerleriyle doğrudan ilişkilidir."

Amaç

Bilgi güvenliğini üniversite genelinde bütüncül ve sürdürülebilir bir sistemle yönetmek; kurumun bilgi varlıklarını korumak, bilgiye güvenli erişimi sağlamak, riskleri minimize etmek ve yasal düzenlemelere tam uyum sağlamak.

Kapsam

Bu politika; Osmaniye Korkut Ata Üniversitesi'ne ait tüm dijital ve fiziksel bilgi varlıklarını, akademik ve idari personeli, öğrencileri, bilgi sistemlerini, iş süreçlerini, üçüncü taraflarla ilişkileri ve tüm bilgi aktarım ortamlarını kapsar; ayrıca üniversite adına hizmet sağlayan dış paydaşlarla yürütülen bilgi güvenliği süreçlerini de içerir.

444 4 658
kalite@osmaniye.edu.tr
www.osmaniye.edu.tr

Fakıuşağı Mah. 80000 Merkez Osmaniye / Türkiye

Temel İlkelerimiz:

Bilgi Güvenliğinin Temel Unsurlarının Güvence Altına Alınması

Gizlilik, bütünlük ve erişilebilirlik esaslarına dayalı olarak bilgi varlıklarının korunmasını sağlamak.

Tüm Bilgi Ortamlarında Güvenlik

Elektronik, yazılı, sözlü, basılı vb. tüm bilgi ortamlarında kapsamlı güvenlik önlemlerini uygulamak.

Risk Tabanlı Bilgi Güvenliği Yaklaşımı

Bilgi varlıklarına yönelik tehditleri belirleyerek, risk analizine dayalı proaktif önlemler almak.

Bilgi Güvenliği Açıklarının Bildirimi ve İzlenmesi

Şüpheli durumların ve güvenlik ihlallerinin zamanında tespit edilmesini ve raporlanmasını sağlamak.

İş Sürekliliği ve Olay Müdahale Hazırlığı

Kesinti ve ihlal durumlarında hızlı müdahale ve toparlanmayı sağlayacak iş sürekliliği ve olay müdahale planlarını kurumsallaştırmak.

Sözleşmelerde Bilgi Güvenliği Uyumu

Tüm sözleşmelerde bilgi güvenliği gerekliliklerinin açıkça belirtilmesini ve uygulanmasını sağlamak.

Bilgiye Erişimde İş Gereksinimi Esası

Bilgiye yalnızca yetkili kişilerin, görev tanımlarına uygun şekilde erişimini sağlamak.

Yetki Bazlı Erişim ve Görev Ayrılığı

Görev tanımlarına göre erişim haklarını yapılandırarak yetkisiz erişim risklerini azaltmak.

Kayıt Tutma ve İzleme (Loglama) Sistemleri

Tüm bilgi sistemlerinde kapsamlı ve güvenli kayıt (log) mekanizmaları kurarak izlenebilirlik sağlamak.

Farkındalık ve Sürekli Eğitim

Kurum genelinde bilgi güvenliği kültürünü yaygınlaştırmak için sürekli eğitim, seminer ve farkındalık çalışmaları yürütmek.

Veri Sınıflandırması ve Hassas Bilgi Yönetimi

Bilgileri hassasiyet derecelerine (gizli, kişisel, kamuya açık vb.) göre sınıflandırmak; her sınıf için uygun koruma ve erişim politikaları geliştirmek.

Gelişim Taahhüdü: Bu Bilgi Güvenliği Yönetim Sistemi Politikası; dijitalleşme, yasal düzenlemeler, teknolojik tehditler, siber güvenlik riskleri ve paydaş ihtiyaçları doğrultusunda düzenli aralıklarla gözden geçirilecek; bilgi güvenliği kültürünün güçlendirilmesi ve sürekli gelişim anlayışıyla güncellenecektir.

Yürürlüğe Girme: Bu politika, Osmaniye Korkut Ata Üniversitesi Senatosu'nun …… tarihli ve ……. sayılı kararıyla yürürlüğe girmiştir.

Gözden Geçirme: Bu politika en geç 2 yılda bir veya ihtiyaç duyulduğunda gözden geçirilir.

Sorumlu Birimler: Bu politikanın uygulanmasından Osmaniye Korkut Ata Üniversitesi Rektörlüğü, Bilgi İşlem Daire Başkanlığı, Dijital Dönüşüm ve Yazılım Ofisi Koordinatörlüğü, Anket Hazırlama ve Değerlendirme Komisyonu, Kalite Koordinatörlüğü ve ilgili akademik/idari birimler sorumludur.

İlişkili Politikalar ve Uyum Göstergesi: Bu bilgi güvenliği yönetim sistemi politikası, Osmaniye Korkut Ata Üniversitesi'nin dijital bilgi varlıklarını koruma, bilgiye güvenli erişim sağlama ve riskleri minimize etme hedefleri doğrultusunda yapılandırılmış olup; üniversitenin diğer stratejik politika belgeleriyle bütüncül bir yapıda uygulanmaktadır. Özellikle dijitalleşme, veri temelli yönetişim, iş sürekliliği, etik sorumluluk ve yasal uyum başlıkları, aşağıdaki politika belgeleriyle detaylandırılmış ve bilgi güvenliği süreçleriyle entegre biçimde yürütülmektedir:

- Kalite Politikası
- Yönetim Sistemi Politikası
- Dijitalleşme ve Akıllı Sistemler Politikası
- Veri Yönetimi ve Karar Destek Politikası
- İnsan Kaynakları Politikası
- Sürdürülebilirlik Politikası

Ulusal ve Uluslararası Uyum Çerçevesi: Bu politika, başta YÖKAK Kurumsal Dış Değerlendirme Programı olmak üzere; ENQA ESG, CHEA, INQAAHE, ISO 21001 ve ISO/IEC 27001 gibi ulusal ve uluslararası kalite ve bilgi güvenliği standartlarıyla tam ve yakın uyum içinde hazırlanmıştır. Politikanın uygulanması ve değerlendirme süreçlerinde bu standartlara göre gizlilik, bütünlük, erişilebilirlik ve risk temelli yönetim esas alınmaktadır.