BİLGİ GÜVENLİĞİ VE YÖNETİMİ POLİTİKASI

www.ozal.edu.tr

MALATYA TURGUT ÖZAL ÜNİVERSİTESİ
BİLGİ GÜVENLİĞİ VE YÖNETİMİ POLİTİKASI

1 Politikanın amacı	**:**	Malatya Turgut Özal Üniversitesinde **TS EN ISO/IEC 27001:2023 Bilgi Güvenliği Yönetim Sistemi** (BGYS) standardı doğrultusunda; üniversitenin akademik, idari ve teknik süreçlerinde yer alan bilgi varlıklarını güvence altına alarak bilgi güvenliği risklerini yönetmek ve kurumsal sürekliliği desteklemektir.
2 Politikanın hedefleri	:	1. Üniversitenin sahip olduğu tüm bilgi varlıklarını iç ve dış tehditlere, kasıtlı veya kazara oluşabilecek zarar ve kayıplara karşı korumak. 2. Bilgi güvenliğinin üç temel bileşeni olan **gizlilik**, **bütünlük** ve **erişilebilirlik** ilkelerinin sürekliliğini temin etmek. 3. Elektronik, yazılı, basılı, sözlü veya diğer ortamlarda bulunan tüm verilerin yetkisiz erişim, ifşa, değişiklik ya da kayba karşı güvenliğini sağlamak. 4. Tüm akademik ve idari personel ile öğrencilerin bilgi güvenliği konularında bilinç düzeylerini artırmak amacıyla düzenli eğitim ve bilgilendirme faaliyetleri yürütmek. 5. Mevcut veya şüpheli güvenlik açıklarının ve olaylarının Bilgi Güvenliği Yönetim Sistemi (BGYS) Ekibi'ne bildirilmesini teşvik etmek, bu bildirimleri titizlikle incelemek ve gerekli müdahaleleri gerçekleştirmek. 6. Kurumsal faaliyetlerin kesintiye uğramadan devam edebilmesi için bilgi sistemlerine ilişkin **iş sürekliliği planları** hazırlamak, güncellemek ve periyodik olarak test etmek. 7. Bilgi güvenliği ile ilgili riskleri periyodik olarak değerlendirmek, uygun kontrol önlemleri ile bu riskleri kabul edilebilir seviyelere indirmek ve gerekli aksiyon planlarını uygulamaya koymak. 8. Üniversite ile çalışan, hizmet veren veya bilgi paylaşımında bulunan üçüncü taraflarla yapılan sözleşmelere bilgi güvenliği hükümleri ekleyerek anlaşmazlıkları ve çıkar çatışmalarını önlemek. 9. BGYS performansını izleyerek, iç denetim ve yönetim gözden geçirme süreçleriyle sistemin etkinliğini sürekli geliştirmek.
3 Politika İlkeleri	:	**Gizlilik:** Bilgiye yalnızca yetkili kişilerin erişebilmesini sağlamak; yetkisiz erişimleri, ifşaları ve sızıntıları önlemek. **Bütünlük:** Bilginin doğruluğunu, eksiksizliğini ve güvenilirliğini korumak; yetkisiz değişikliklerin ve bozulmaların önüne geçmek.

	Erişilebilirlik: Bilgiye ihtiyaç duyan yetkili kullanıcıların zamanında ve kesintisiz bir şekilde erişimini temin etmek. **Yasal ve Mevzuatsal Uyum:** Ulusal ve uluslararası yasal düzenlemelere, sektör standartlarına, yükseköğretim mevzuatına ve üniversite iç yönergelerine tam uyum sağlamak. **Risk Temelli Yaklaşım:** Bilgi güvenliği tehdit ve zafiyetlerine karşı sistematik risk değerlendirmeleri yapmak ve bu riskleri yönetilebilir seviyelere indirmek. **Sürekli İyileştirme:** Bilgi Güvenliği Yönetim Sistemi'nin (BGYS) etkinliğini artırmak amacıyla sistematik gözden geçirme ve iyileştirme faaliyetlerini sürdürülebilir şekilde yürütmek. **Farkındalık ve Eğitim:** Tüm paydaşların bilgi güvenliği konusunda bilinçlenmesini sağlamak amacıyla düzenli eğitim, bilgilendirme ve farkındalık çalışmaları gerçekleştirmek. **İzlenebilirlik ve Hesap Verebilirlik:** Tüm bilgi güvenliği faaliyetlerinin kayıt altına alınması, izlenebilirliğinin sağlanması ve sorumlulukların açıkça tanımlanarak hesap verilebilirliğin güvence altına alınması.
4 Politika uygulama prosedürü :	1. Kurumun bilgi varlıklarına yönelik iç ve dış tehditler belirlenir, risk değerlendirme süreçleri (etki–olasılık, risk iştahı, kabul kriterleri) uygulanır ve sonuçlar kayıt altına alınır. 2. Risklerin yönetimi amacıyla teknik, idari ve fiziksel kontroller risk değerlendirme sonuçlarına göre seçilir, standartlara uygun biçimde uygulanır ve etkinliği periyodik olarak doğrulanır. 3. BGYS performansı tanımlı göstergeler ve hedef değerler üzerinden düzenli aralıklarla ölçülür, izlenir ve raporlanır. 4. BGYS'nin uygunluk, etkinlik ve sürekliliğini değerlendirmek üzere belirli periyotlarla iç denetimler gerçekleştirilir, bulgulara yönelik düzeltici–önleyici faaliyetler planlanır ve kapatılması izlenir. 5. BGYS'nin yeterliliği ve etkinliği periyodik Yönetimin Gözden Geçirmesi toplantılarında gözden geçirilir, kararlar aksiyon planlarına bağlanır ve gerçekleşmeler izlenir. 6. Geri bildirimler, iç denetim sonuçları, yönetimin gözden geçirmeleri ve güvenlik olayları analiz edilerek BGYS'de sürekli iyileştirme sağlanır ve sistemsel düzeltmeler uygulanır. 7. Üniversite personeli, öğrenciler ve paydaşlar nezdinde bilgi güvenliği farkındalığı oluşturulması

	için eğitim, duyuru ve tatbikatlar düzenlenir ve kurumsal bilgi güvenliği kültürü sürekli geliştirilir.
5 Taahhüt	Bu politika, belirlenen amaç–hedef–ilkeler ve uygulama prosedürlerine uygun biçimde BGYS'nin TS EN ISO/IEC 27001:2023 ve ilgili mevzuata tam uyumla kurulmasını, etkin işletilmesini ve PUKÖ ile sürekli iyileştirilmesini garanti altına alır.