



Yozgat Bozok Üniversitesi

Yapay Zeka, Nesnelerin İnterneti Ve Gelişmiş Dijital Teknolojiler Politikası

1. Amaç

Bu politikanın amacı; yapay zekâ (YZ), nesnelerin interneti (IoT), büyük veri, veri analitiği, dijital ikiz, robotik süreç otomasyonu (RPA), bulut bilişim ve diğer gelişmiş dijital teknolojilerin üniversitenin akademik, idari ve destek hizmetlerinde etkin, güvenli, etik ve sürdürülebilir şekilde kullanılmasına ilişkin temel ilke ve esasları belirlemektir. Üniversite; dijital teknolojileri karar alma süreçlerini desteklemek, operasyonel verimliliği artırmak, kaynak kullanımını optimize etmek, eğitim-öğretim faaliyetlerini geliştirmek, araştırma kapasitesini güçlendirmek ve paydaşlara sunulan hizmetlerin kalitesini yükseltmek amacıyla kullanmayı hedeflemektedir.

2. Kapsam

Bu politika; akademik ve idari birimleri, öğretim elemanlarını, idari personeli, öğrencileri, araştırma merkezlerini ve üniversite adına hizmet sunan üçüncü tarafları kapsamaktadır. Üniversite bünyesinde kullanılan veya geliştirilmesi planlanan tüm yapay zekâ, IoT ve diğer gelişmiş dijital teknoloji çözümleri bu politika hükümlerine tabidir.

3. Temel İlkeler

- **İnsan Merkezli Yaklaşım:** Yapay zekâ, nesnelerin interneti, büyük veri, veri analitiği, dijital ikiz, robotik süreç otomasyonu ve bulut bilişim sistemleri insan kararlarının yerini almak yerine karar süreçlerini desteklemek amacıyla kullanılacaktır. Nihai sorumluluk ilgili yönetici, akademisyen veya görevli personelde olacaktır.
- **Etik ve Şeffaflık:** Gelişmiş dijital teknoloji uygulamalarının kullanım amacı, veri kaynakları ve üretilen sonuçların niteliği mümkün olduğunca şeffaf şekilde yönetilecektir. Sistemlerin ayrımcılık, önyargı veya adaletsiz sonuçlar üretmemesi için gerekli tedbirler alınacaktır.
- **Veri Güvenliği ve Mahremiyet:** Tüm dijital teknolojiler; 6698 Sayılı Kişisel Verilerin Korunması Kanunu, Bilgi Güvenliği Yönetim Sistemi gereksinimleri, Üniversitenin bilgi güvenliği politikaları ve ilgili ulusal/uluslararası mevzuat çerçevesinde, bilginin gizlilik, bütünlük ve erişilebilirlik ilkeleri korunarak kullanılacaktır.
- **Güvenilirlik ve Hesap Verebilirlik:** Üniversite bünyesinde kullanılan yapay zekâ ve IoT sistemlerinin doğruluğu, güvenilirliği ve izlenebilirliği düzenli olarak değerlendirilecektir.
- **Sürekli İyileştirme:** Dijital teknolojilerin performansı, faydaları ve riskleri düzenli olarak gözden geçirilecek; teknolojik gelişmeler doğrultusunda sürekli iyileştirme faaliyetleri yürütülecektir.

4. Kullanım Alanları

- **Akademik Süreçler:** Yapay zekâ ve gelişmiş dijital teknolojiler; öğrenme analitiği, akademik danışmanlık destek sistemleri, dijital eğitim içeriklerinin geliştirilmesi, araştırma verilerinin analizi, bilimsel yayın ve proje yönetimi, akademik performans değerlendirme süreçleri ile kütüphane ve bilgi erişim hizmetleri gibi alanlarda akademik dürüstlük ilkelerine uygun olarak kullanılabilir.
- **İdari Süreçler:** İdari iş ve işlemlerin optimizasyonu amacıyla bu teknolojiler; elektronik belge yönetimi, insan kaynakları süreçleri, satın alma ve bütçe planlama, kurumsal performans yönetimi, risk yönetimi, talep ve şikâyet yönetimi, kurumsal karar destek sistemleri ile süreç otomasyonu ve iş akışı yönetimi alanlarında kullanılabilir.



- **Akıllı Kampüs Uygulamaları:** IoT ve akıllı sistemler; enerji yönetimi, aydınlatma sistemleri, ısıtma ve iklimlendirme, su tüketimi izleme, güvenlik sistemleri, otopark yönetimi, çevresel izleme ile bina ve tesis yönetimi amaçlarıyla kullanılabilir.

5. Karar Destek ve Veri Yönetimi

Üniversite, veri temelli yönetim anlayışını benimser. Bu kapsamda; kurumsal verilerin bütünlüğü korunur ve veri kalitesi düzenli olarak izlenir. Karar destek sistemleri doğrulanabilir verilere dayandırılır. Yapay zekâ (YZ), nesnelerin interneti (IoT), büyük veri, veri analitiği, dijital ikiz, robotik süreç otomasyonu (RPA), bulut bilişim ve diğer gelişmiş dijital teknolojiler tarafından üretilen çıktılar kritik kararlarda tek başına belirleyici unsur olarak kullanılamaz; tüm karar süreçlerinde insan denetimi ve süzgeci mutlak surette sağlanır.

6. Risk Yönetimi

Yapay zekâ (YZ), nesnelerin interneti (IoT), büyük veri, veri analitiği, dijital ikiz, robotik süreç otomasyonu (RPA), bulut bilişim ve diğer gelişmiş dijital teknolojilere ilişkin siber güvenlik riskleri, veri gizliliği riskleri, operasyonel riskler, hukuki ve etik riskler ile algoritmik önyargı riskleri düzenli olarak belirlenir, değerlendirilir ve uygun kontroller uygulanır. Tüm kritik sistemler için iş sürekliliği ve olağanüstü durum planları hazırlanarak güncel tutulur.

7. Yasaklı Kullanımlar

Kurumsal gizlilik içeren bilgilerin, şifrelerin, personele veya öğrencilere ait kişisel verilerin, gerekli maskeleyme ve anonimleştirme süreçlerinden geçirilmeden üçüncü taraf açık yapay zekâ sistemlerine aktarılması kesinlikle yasaktır. İnsan denetimi olmaksızın kritik kurumsal kararların tamamen otonom sistemlere bırakılması, akademik sahtecilik, intihal veya telif hakkı ihlali barındıran yapay içerik üretimi kabul edilemez kullanım senaryoları olarak değerlendirilir.

8. Yetki ve Sorumluluklar

- **Üst Yönetim:** Dijital dönüşüm stratejisini belirler, gerekli kaynak tahsisini sağlar ve politikanın uygulanmasını destekler.
- **Bilgi İşlem Daire Başkanlığı:** Teknolojik altyapıyı ve sunucu elemanlarını yönetir, siber güvenlik tedbirlerini ve sızma testlerini uygular, sistemlerin sürekliliğini ve log bütünlüğünü sağlar.
- **Akademik ve İdari Birimler:** Teknolojileri amaçlarına uygun ve etik sınırlar dahilinde kullanır, işlenen verinin kalitesini ve doğruluğunu sağlar, politika hükümlerine uyumu gözetir.
- **Kullanıcılar:** Sistemleri etik, akademik dürüstlüğe uygun ve güvenli şekilde kullanır; yetkisiz veri paylaşımından kaçınarak kurumsal bilgi güvenliği kurallarına eksiksiz uyum sağlar.

9. Eğitim ve Farkındalık

Üniversite, gelişmiş dijital teknolojilerin kullanımını esnasında oluşabilecek siber güvenlik ve veri ihlali risklerini asgariye indirmek amacıyla, akademik/idari personele ve öğrencilere yönelik yapay zekâ okuryazarlığı ve teknoloji güvenliği eğitimleri ile farkındalık faaliyetleri düzenler.

10. İzleme ve Gözden Geçirme

Bu politika en az yılda bir kez veya ihtiyaç duyulması halinde daha kısa aralıklarla gözden geçirilir. Teknolojik gelişmeler, mevzuat değişiklikleri, kalite güvence standartları ve kurumsal ihtiyaçlar doğrultusunda güncellenerek Üniversite Senatosunun onayı ile yürütülür.