T.C.
YOZGAT BOZOK ÜNİVERSİTESİ
YAPAY ZEKÂ POLİTİKASI

Eğitim-Öğretim, Araştırma, Sağlık ve İdari Süreçler İçin Kurumsal Çerçeve

Belge niteliği	Senatoya Sunulacak Politika Metni
Sürüm	1.1 (v1.0 taslağın sadeleştirilmiş ve hukuki yönden gözden geçirilmiş hâli)
Tarih	27 Ekim 2026
Gözden geçirme	En az her akademik yıl sonunda; ayrıca önemli mevzuat veya teknoloji değişikliğinde
Rehber ilişkisi	Bu Politika, YOBÜ Üretken Yapay Zekâ Kullanım Rehberi v3.0'ın üst düzey kurumsal çerçevesidir. Uygulama ayrıntılarında Rehber v3.0 ve ilgili birim düzenlemeleri esas alınır.

Yönetici Özeti

Yozgat Bozok Üniversitesi, yapay zekâyı eğitim, araştırma, sağlık, toplumsal katkı ve idari süreçlerde insan kapasitesini güçlendiren stratejik bir araç olarak kabul eder. Üniversitenin yaklaşımı, yapay zekâyı toptan yasaklamak veya denetimsiz biçimde serbest bırakmak değil; hukuka uygun, etik, güvenli, şeffaf, erişilebilir, akademik dürüstlüğü koruyan ve insan sorumluluğunu merkeze alan, risk temelli bir yönetişim modeli kurmaktır.

Bu Politika; Üniversitenin tüm yapay zekâ kullanım, geliştirme ve tedarik kararlarında aynı ilkelerin uygulanmasını, eğitimde öğrenme çıktılarının ve araştırmada bilimsel bütünlüğün korunmasını, kişisel ve kurumsal verinin güvenliğini, yüksek etkili uygulamaların insan gözetimi ve etki değerlendirmesi altında yürütülmesini ve tüm mensupların yapay zekâ okuryazarlığının sistematik biçimde geliştirilmesini hedefler.

1. Amaç ve Politika Statüsü

1.1. Bu Politikanın amacı, Üniversitede yapay zekâ sistemlerinin geliştirilmesi, tedariki, kullanımı ve değerlendirilmesine ilişkin kurumsal ilke ve yönetişim esaslarını belirlemektir.

1.2. Bu Politika bir üst çerçeve belgesidir. Ayrıntılı uygulama kuralları; YOBÜ Üretken Yapay Zekâ Kullanım Rehberi v3.0, Yapay Zekâ Koordinatörlüğü Yönergesi, bilgi güvenliği ve kişisel veri koruma düzenlemeleri, sağlık alanına özgü rehberler ve ilgili diğer mevzuatla belirlenir.

1.3. Bu Politika tek başına yeni bir disiplin suçu veya cezası, kişisel veri işleme şartı, akademik yetki ya da kişilerin haklarını sınırlayan bağımsız bir yetki oluşturmaz. Somut fiiller, ilgili mevzuat hükümlerine göre ayrıca değerlendirilir. Alt düzenlemeler bu Politikaya ve üst hukuk normlarına aykırı olamaz; birimler disiplin, meslek veya akreditasyon gereklerine göre daha sıkı kurallar getirebilir.

2. Kapsam

2.1. Politika; eğitim-öğretim, ölçme ve değerlendirme, araştırma ve yayın, sağlık hizmetleri ve sağlık araştırmaları, toplumsal katkı, idari hizmetler, insan kaynakları, satın alma, proje yönetimi ve Üniversite adına yürütülen dijital hizmetleri kapsar.

2.2. Politika, Üniversite adına veya Üniversite kaynakları kullanılarak yürütülen faaliyetlerde aşağıdakileri kapsar:

- Ön lisans, lisans ve lisansüstü öğrencileri;

- Akademik ve idari personel, araştırmacılar, proje personeli, bursiyerler ve stajyerler;
- Üniversite birimleri, kurullar, komisyonlar, merkezler ve koordinatörlükler;
- Üniversite adına hizmet sunan yüklenici, danışman ve dış paydaşlar (sözleşme kapsamı ile sınırlı olmak üzere);
- Üniversitenin geliştirdiği, tedarik ettiği, lisansladığı veya kullanımına izin verdiği yapay zekâ sistemleri.

3. Dayanak ve Referans Çerçevesi

Politika, aşağıdaki bağlayıcı mevzuat ile yönlendirici çerçeveler dikkate alınarak hazırlanır ve güncel tutulur. Uluslararası metinler Türkiye'de doğrudan bağlayıcı olmadıkları ölçüde karşılaştırmalı yönetişim ve iyi uygulama referansı olarak kullanılır.

Kaynak / çerçeve	Hukuki niteliği	Politikaya katkısı
2547 sayılı Yükseköğretim Kanunu ve ilgili YÖK düzenlemeleri	Bağlayıcı	Yükseköğretim yetkileri, öğrenci/personel süreçleri, akademik ve etik çerçeve
6698 sayılı Kişisel Verilerin Korunması Kanunu ve ikincil düzenlemeler	Bağlayıcı	Hukuka uygun veri işleme, özel nitelikli veri, veri güvenliği, yurt dışına aktarım
5846 sayılı Fikir ve Sanat Eserleri Kanunu	Bağlayıcı	Eser sahipliği ve kullanım hakları
2019/12 sayılı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi ve ilgili güvenlik rehberleri	Kamu kurumları bakımından idari düzenleme	Bilgi güvenliği, veri sınıflandırma, hizmet sağlayıcı riskleri
Türkiye Yapay Zekâ Eylem Planı (2026–2030), 2026/9 sayılı Cumhurbaşkanlığı Genelgesi (RG 18.08.2026, sayı 33344)	Ulusal stratejik çerçeve	İnsan odaklılık, güvenilirlik, etik sorumluluk, dijital egemenlik, yetkinlik
YÖK, Bilimsel Araştırma ve Yayın Faaliyetlerinde Üretken Yapay Zekâ Kullanımına Dair Etik Rehber (2024)	Yükseköğretim etik rehberi	Şeffaflık, dürüstlük, özen, adalet, gizlilik, hesap verebilirlik
AB Yapay Zekâ Tüzüğü, (AB) 2024/1689 (AB 2026/1744 sayılı Tüzük ile değişik)	Karşılaştırmalı düzenleyici referans; AB bağlantılı süreçlerde ayrıca değerlendirilir	Risk temelli yaklaşım, insan gözetimi, yapay zekâ okuryazarlığı
UNESCO Yapay Zekâ Etiği Tavsiye Kararı (2021) ve GenAI in Education and Research Guidance (2023)	Uluslararası etik/eğitim rehberi	İnsan merkezlilik, eşitlik, eleştirel düşünme, dijital kapsayıcılık
WHO, Ethics and Governance of AI for Health (2021), Large Multi-Modal Models rehberi (2024/2025) ve AI-related health research: ethics review and oversight (2026)	Uluslararası sağlık etiği/yönetişim rehberi	Hasta güvenliği, klinik insan gözetimi, sağlık verisi, etik kurul gözetimi
Avrupa Komisyonu, Living Guidelines on the Responsible Use of Generative AI in Research (3. sürüm, Mayıs 2026)	Araştırma bütünlüğü iyi uygulama rehberi	Şeffaflık, hesap verebilirlik, ajanlı yapay zekâ, hakemlikte gizlilik

4. Kurumsal Yapay Zekâ İlkeleri

4.1. İnsan merkezlilik ve insan sorumluluğu — Yapay zekâ, insan kararını ve mesleki/akademik sorumluluğu destekler; yerine geçmez. Hukuki, akademik, klinik veya idari sonucu olan nihai karar yetkili insan veya kurula aittir.

4.2. Hukuka uygunluk ve etik — Tüm kullanım, geliştirme ve tedarik süreçleri yürürlükteki mevzuata, akademik etik ilkelerine, insan haklarına ve mesleki standartlara uygun yürütülür.

4.3. Risk temelli ve orantılı yönetişim — Yükümlülükler, kullanımın kişi hakları, eğitim, sağlık, araştırma, güvenlik ve kurumsal sonuçlar üzerindeki etkisiyle orantılı belirlenir.

4.4. Şeffaflık ve beyan — Yapay zekânın içerik, analiz veya karar desteğine anlamlı katkı sağladığı durumlarda kullanım uygun biçimde açıklanır. Kişiler, haklarında yüksek etkili bir süreçte yapay zekâ desteği kullanıldığında mevzuatın izin verdiği ölçüde bilgilendirilir.

4.5. Doğrulama, hesap verebilirlik ve izlenebilirlik — Yapay zekâ çıktısı doğrulanmadan resmî, akademik veya klinik gerçek olarak kabul edilmez. Kurumsal sistemlerde gerekli ölçüde denetim izi tutulur.

4.6. Kişisel veri, mahremiyet ve bilgi güvenliği — Kişisel, özel nitelikli, kurumsal gizli, araştırma, hakemlik ve ticari sır niteliğindeki veriler yalnızca hukuki şartlar ve yetkilendirilmiş sistemler çerçevesinde işlenir.

4.7. Akademik özgürlük, araştırma bütünlüğü ve pedagojik amaç — Yapay zekâ yenilikçi araştırmayı destekleyebilir; bilimsel sorumluluk, kaynak doğrulama, yöntemsel geçerlilik ve yazarlık sorumluluğu araştırmacıda kalır. Eğitimde yapay zekâ kullanımı öğrenme çıktısına hizmet etmeli, öğrencinin temel bilgi, muhakeme ve mesleki becerilerinin gelişimini zayıflatmamalıdır.

4.8. Adalet, ayrımcılık yapmama ve erişilebilirlik — Algoritmik önyargı ve dezavantaj riski değerlendirilir. Engelliler için erişilebilirlik ve makul uyarlama gözetilir; ücretli araca erişim zorunlu tutularak fırsat eşitsizliği yaratılmaz.

4.9. Fikri haklara saygı — Girdi ve çıktıların telif, lisans, marka, patent, ticari sır ve üçüncü kişi haklarına uygunluğu gözetilir.

4.10. Kurumsal kontrol, sürdürülebilirlik ve güncellenebilirlik — Kurumsal verinin işlendiği kritik kullanımlarda, Üniversitenin veri, kayıt ve erişim üzerinde yeterli kontrol sağlayabildiği çözümler tercih edilir. Sistemlerin maliyeti ve çevresel etkisi verimlilik ilkesiyle yönetilir. Teknoloji ve mevzuattaki değişim nedeniyle politika, rehber, eğitim ve sistem envanteri düzenli olarak güncellenir.

5. Risk Temelli Kurumsal Kullanım Modeli

5.1. Üniversite, yapay zekâ kullanımını kişi hakları ve kurumsal sonuçlar üzerindeki etkisine göre düşük etkili, kontrollü/orta etkili ve yüksek etkili olarak sınıflandırır; sınıflandırma Yapay Zekâ Koordinatörlüğünce, ilgili birimle birlikte yapılır. Bu kurum içi sınıflandırma, AB Yapay Zekâ Tüzüğündeki kategorilerin birebir hukuki karşılığı değildir.

5.2. Aşağıdaki kullanım alanları, aksi somut olarak gösterilmedikçe yüksek etkili kabul edilir:

- Öğrenci kabulü, yerleştirme, başarı, notlandırma, mezuniyet, burs, disiplin veya öğrenci risk müdahalesi üzerinde belirleyici etki doğuran sistemler;
- Sınav gözetimi veya sınav güvenliği amacıyla biyometrik ya da davranışsal analiz yapan sistemler;
- Personel seçimi, performansı, iş yükü, terfi, görevlendirme veya kaynak dağıtımını etkileyen sistemler;
- Sağlık hizmetlerinde tanı, tedavi, triyaj, klinik öncelik veya hasta güvenliğini etkileyen sistemler;
- Özel nitelikli kişisel veriyi sistematik veya geniş ölçekte işleyen uygulamalar;
- Kişiler hakkında hukuki veya önemli idari sonuç doğurabilecek otomatik karar ya da öneri sistemleri.

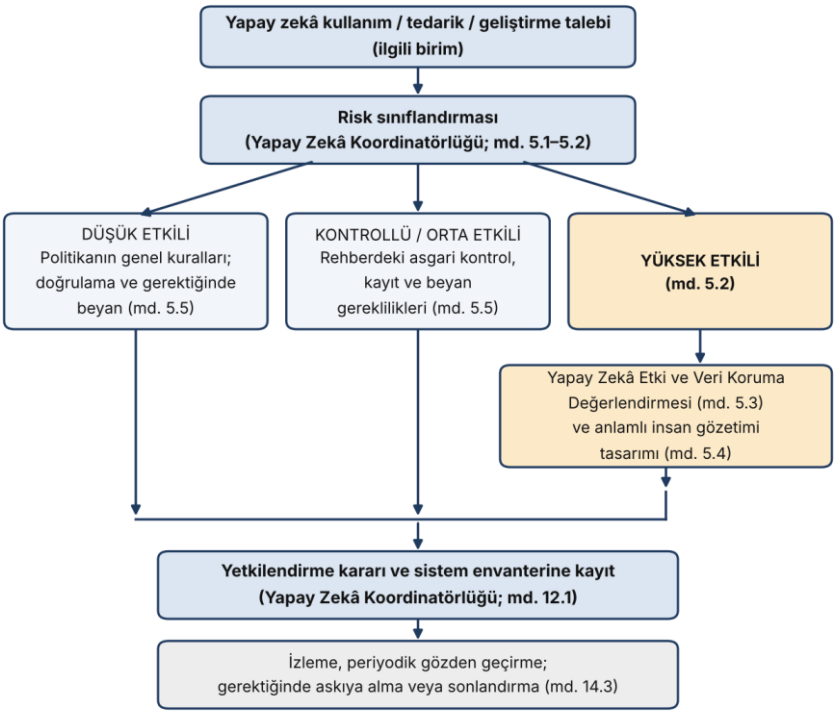
5.3. Yüksek etkili bir sistem devreye alınmadan önce; amaç ve gereklilik, veri kaynağı ve veri koruma şartları, doğruluk ve güvenilirlik, ayrımcılık/önyargı, siber güvenlik, insan gözetimi, açıklanabilirlik, itiraz yolu, erişilebilirlik, tedarikçi koşulları ve izleme planını içeren bir **Yapay Zekâ Etki ve Veri Koruma**

Değerlendirmesi yapılır. Değerlendirme; Yapay Zekâ Koordinatörlüğü, Bilgi İşlem Daire Başkanlığı, Hukuk Müşavirliği ve kişisel verilerden sorumlu birim ile gerekli hâllerde ilgili etik, akademik veya klinik birimin katılımıyla gerçekleştirilir.

5.4. Yüksek etkili sistemlerde yalnızca "insan onayı" bulunması yeterli değildir. İnsan gözetimi gerçek, anlamlı ve müdahale edilebilir olmalı; yetkili kişi sistem önerisini sorgulayabilmeli, reddedebilmeli ve gerekçeli nihai karar verebilmelidir.

5.5. Düşük etkili kullanımlarda bu Politikanın genel ilkeleri, veri ve gizlilik kuralları ile çıktı doğrulama ve gerektiğinde beyan yükümlülükleri uygulanır. Kontrollü/orta etkili kullanımlarda ayrıca Rehberde öngörülen kayıt ve beyan gereklilikleri aranır.

Şekil 1'de, bir yapay zekâ kullanım veya tedarik talebinin Politika kapsamındaki işleyişi özetlenmektedir.



Şekil 1. Risk temelli yapay zekâ kullanım ve tedarik süreci

6. Eğitim-Öğretimde Yapay Zekâ

6.1. Eğitimde temel yaklaşım, yapay zekâyı öğrenme çıktılarıyla uyumlu ve öğrencinin bilişsel bağımsızlığını güçlendirecek biçimde kullanmaktır.

6.2. Derslerde ve değerlendirmelerde izin verilen yapay zekâ kullanımı, Rehber v3.0'daki Seviye 0–5 sistemiyle belirlenir. Her ders veya görev için izin verilen, kısıtlanan ve beyan edilmesi gereken kullanım dönem başında açıkça ilan edilir.

6.3. Öğrencinin cezalandırılabilmesi için yalnızca bir "yapay zekâ skoru" veya dedektör sonucu yeterli değildir. Akademik usulsüzlük şüphesi, somut ve çoklu göstergelerle ve öğrencinin açıklama hakkı korunarak değerlendirilir; disiplin işlemleri yalnızca ilgili mevzuatın unsurları oluştuğunda yürütülür.

6.4. Üniversite; mezunların yapay zekâ okuryazarlığı, çıktı doğrulama, etik ve güvenli kullanım, veri koruma ve insan-yapay zekâ iş birliği yetkinliklerini program çıktılarıyla ilişkilendirir. Bölümler, alanlarına özgü yetkinlikleri müfredatta görünür kılar.

6.5. Belirli bir ticari veya ücretli yapay zekâ aracının öğrenci tarafından edinilmesi, Üniversitece eşit erişimle sağlanmadıkça, zorunlu değerlendirme koşulu yapılamaz.

7. Bilimsel Araştırma, Yayın ve Proje Süreçleri

7.1. Yapay zekâ; araştırma tasarımı, literatür keşfi, kodlama, veri analizi, görselleştirme ve yazım desteğinde kullanılabilir. Bilimsel iddia, veri, yöntem, sonuç, kaynak ve yorumların doğruluğundan araştırmacı sorumludur.

7.2. Yapay zekâ sistemi yazar olamaz ve yazar olarak gösterilemez. Alan, dergi, fon sağlayıcı veya etik kurul kuralları daha sıkı değilse, araştırma ürününe anlamlı katkı sağlayan yapay zekâ kullanımı uygun yerde açıklanır.

7.3. Uydurma kaynak, veri, görüntü, analiz veya bulgunun gerçekmiş gibi sunulması ile araştırmacının kendi yapması gereken bilimsel muhakemeyi yapay zekâya yaptırıp sorumluluğu devretmesi kabul edilemez.

7.4. Hakem, panelist, jüri veya değerlendirici sıfatıyla erişilen gizli başvuru, makale, tez, proje veya değerlendirme materyali, açık yetki ve uygun güvenli altyapı bulunmadıkça üçüncü taraf yapay zekâ sistemlerine yüklenemez.

7.5. Ajanlı yapay zekâ sistemlerinin dış kaynaklara erişmesi, dosya yüklemesi, kod çalıştırması, işlem yapması veya üçüncü taraflarla etkileşmesi durumunda yetki sınırları ve denetim kayıtları ayrıca tanımlanır.

8. Sağlık Bilimleri, Klinik Hizmetler ve Sağlık Araştırmaları

8.1. Sağlık alanında yapay zekâ kullanımı; hasta güvenliği, klinik sorumluluk, kişisel sağlık verileri, tıbbi cihaz düzenlemeleri, etik kurul gereklilikleri ve mesleki standartlar nedeniyle genel kullanımlardan daha sıkı risk yönetimine tabidir.

8.2. Yapay zekâ çıktısı; tanı, tedavi, reçete, triyaj veya klinik kararın tek ve otonom belirleyicisi olamaz. Yetkili sağlık meslek mensubunun bağımsız değerlendirmesi ve nihai sorumluluğu korunur.

8.3. Hasta veya araştırma katılımcısına ait tanımlanabilir sağlık verileri, özel nitelikli kişisel veri olarak 6698 sayılı Kanunun ilgili hükümlerine uygun işleme şartının bulunması ve yalnızca Üniversitece yetkilendirilmiş güvenli altyapıda yapay zekâ sistemleriyle işlenebilir.

8.4. Sağlık alanında geliştirilen veya tedarik edilen yapay zekâ sistemlerinin tıbbi cihaz niteliği, klinik performansı ve güvenlik gereklilikleri ayrıca değerlendirilir. Sağlık araştırmalarında etik kurul gözetimi, WHO'nun güncel rehberleri de iyi uygulama referansı alınarak yürütülür.

9. İdari Süreçler ve Kurumsal Karar Desteği

9.1. Yapay zekâ; taslak hazırlama, sınıflandırma, özetleme, veri analizi, raporlama ve karar desteği amacıyla kullanılabilir. Resmî yazı, hukuki görüş, bütçe/ihale kararı, personel işlemi veya benzeri kurumsal işlemin doğruluğu ve hukuka uygunluğu yetkili personel ve birime aittir.

9.2. Yapay zekâ çıktısı mevzuatın, resmî veri kaynağının, yetkili kurul kararının veya uzman görüşünün yerine geçmez; sayısal ve hukuki bilgiler birincil kaynaktan doğrulanır.

9.3. Personel veya öğrenci hakkında önemli sonuç doğuran idari kararlar yalnızca yapay zekâ önerisine dayanılarak verilemez; anlamlı insan değerlendirmesi, gerekçe ve uygun itiraz mekanizması sağlanır.

10. Kişisel Veri, Bilgi Güvenliği ve Fikri Mülkiyet

10.1. Yapay zekâ sistemine veri aktarımı, verinin niteliğine, işleme amacına ve sistemin yetkilendirme düzeyine göre yapılır. Veri minimizasyonu, amaçla sınırlılık ve güvenlik varsayılan ilkedir.

10.2. Kişisel veya özel nitelikli kişisel veri, araştırma katılımcısı verisi, yayımlanmamış araştırma verisi, proje/hakemlik materyali, sınav materyali, ticari sır, erişim bilgisi ve kurum içi gizli veri yetkilendirilmemiş yapay zekâ sistemlerine girilemez.

10.3. Yurt dışına kişisel veri aktarımı, 6698 sayılı Kanunun 9 uncu maddesi ve ikincil düzenlemelere uygun gerçekleştirilir. Uygun güvence olarak standart sözleşmenin kullanıldığı durumlarda sözleşme imzalandıktan sonra beş iş günü içinde Kişisel Verileri Koruma Kurumuna bildirim yapılır.

10.4. Biyometrik veri niteliği, verinin kişiyi benzersiz biçimde tanımlama veya kimlik doğrulama amacıyla özel teknik işlemden geçirilip geçirilmediğine göre değerlendirilir. Yüz, ses veya göz hareketine ilişkin her veri otomatik olarak biyometrik özel nitelikli veri sayılmaz; ancak her hâlükârda kişisel veri ve temel hak riskleri ayrıca analiz edilir.

10.5. Yapay zekâ kullanılırken üçüncü kişilere ait eser, veri tabanı, yazılım, marka, patent, ticari sır ve lisans koşullarına uyulur. Yapay zekâ tarafından üretilen içeriğin özgün veya hak ihlali içermediği varsayılamaz; akademik ve kurumsal kullanımdan önce kaynak, lisans ve benzerlik riski uygun ölçüde kontrol edilir.

10.6. Üniversitenin adı, logosu, kurumsal kimliği veya resmî temsil yetkisi yapay zekâ ile oluşturulan yanıltıcı içeriklerde kullanılamaz.

11. Kabul Edilemez Kullanımlar

Mevzuatın ayrıca yasakladığı fiiller saklı kalmak üzere, Üniversite kaynakları veya Üniversite adına yürütülen süreçlerde aşağıdaki kullanımlar kabul edilemez. Bu kullanımların yaptırımı 1.3 uyarınca ilgili mevzuata göre belirlenir.

- Kişiler hakkında hukuki, akademik, klinik veya önemli idari sonucu olan kararın yalnızca otomatik yapay zekâ çıktısıyla verilmesi;
- Kişisel, özel nitelikli, gizli veya korunması gereken kurumsal verinin ya da hakemlik, proje değerlendirme ve sınav güvenliği gibi gizlilik yükümlülüğü altındaki materyalin yetkisiz sistemlere aktarılması;
- Sahte veri, kaynak, kanıt, resmî belge, akademik kayıt veya yanıltıcı kurumsal içerik üretilmesi ve gerçekmiş gibi sunulması;
- Rıza veya hukuki dayanak olmaksızın kişilerin görüntü ya da sesinin yanıltıcı biçimde taklit edilmesi veya “deepfake” üretimi;
- Ayrımcılık, taciz, yıldırma, nefret söylemi, siber zorbalık veya kişilere zarar verme amacıyla kullanım;
- Üniversite veya üçüncü taraf bilgi sistemlerine yetkisiz erişim, güvenlik önlemlerini aşma veya kötüye kullanım amacıyla yapay zekâ kullanılması.

12. Tedarik, Envanter ve Yetkilendirme

12.1. Üniversite adına tedarik edilen, geliştirilen veya kurumsal süreçte düzenli kullanılan yapay zekâ sistemleri, Yapay Zekâ Koordinatörlüğünce tutulan envantere kaydedilir ve yetkilendirilmiş sistem listesine alınır. Yüksek etkili sistemler, 5.3 uyarınca değerlendirme tamamlanmadan yetkilendirilmez.

12.2. Envanterde en az sistemin amacı, sorumlu birimi, sağlayıcısı/modeli, veri sınıfları, kullanıcı grupları, risk/etki düzeyi, yurt dışı aktarım durumu, insan gözetimi, loglama, sözleşme ve gözden geçirme tarihi yer alır.

12.3. Yeni tedariklerde teknik performans ve fiyatın yanı sıra veri koruma, güvenlik, açıklanabilirlik, önyargı, erişilebilirlik, sağlayıcı bağımlılığı, birlikte çalışabilirlik, çevresel maliyet ve hizmetten çıkış koşulları değerlendirilir. Sözleşmelerde; verinin işlendiği/saklandığı ülkeler, alt işleyenler, saklama süresi, model eğitiminde kullanım, erişim kontrolü, güvenlik, olay bildirimi, denetim hakkı, veri taşınabilirliği, hizmet sonlandırma ve silme hükümleri ele alınır.

12.4. Açık kaynak/açık ağırlıklı modellerin kullanımı da güvenlik, lisans, veri sızıntısı, model tedarik zinciri ve bakım risklerinden muaf değildir; aynı risk temelli yaklaşım uygulanır.

13. Yapay Zekâ Okuryazarlığı ve Yetkinlik

13.1. Üniversite, yapay zekâ sistemlerini kullanan akademik ve idari personel ile öğrenciler için rol ve risk düzeyine uygun yapay zekâ okuryazarlığı eğitimleri yürütür.

13.2. Asgari yetkinlik alanları; yapay zekânın çalışma mantığı ve sınırlılıkları, halüsinasyon ve doğrulama, önyargı, veri güvenliği, akademik dürüstlük, telif, etik, istem tasarımı, ajanlı sistem riskleri ve insan gözetimidir.

13.3. Yüksek etkili sistemleri kullanan veya yöneten personele genel farkındalık eğitiminden daha ileri, göreve özgü eğitim verilir ve gerektiğinde yetkilendirme şartı aranır.

14. Yönetişim, İzleme ve Olay Bildirimi

14.1. Sorumluluklar.

Birim / rol	Temel sorumluluk
Senato	Politikayı kabul eder; temel kurumsal ilkeleri ve önemli politika değişikliklerini onaylar.
Rektörlük	Politikanın kurum genelinde uygulanmasını sağlar; gerekli kaynak ve yetkilendirmeleri belirler.
Yapay Zekâ Koordinatörlüğü	Uygulamayı koordine eder; rehberleri, sistem envanterini ve yetkilendirilmiş sistem listesini günceller; eğitim ve izlemeyi yürütür; teknik/etik görüş sağlar.
Hukuk Müşavirliği	Hukuki risk, sözleşme ve mevzuat yorumuna ilişkin görüş sağlar; disiplin yetkilerini üstlenmez.
Bilgi İşlem Daire Başkanlığı	Bilgi güvenliği, teknik mimari, erişim, loglama, entegrasyon, olay müdahalesi ve teknik tedarik incelemesini yürütür.
Kişisel verilerden sorumlu birim/kurul	KVKK uyumu, veri envanteri, aydınlatma, yurt dışı aktarım ve veri ihlali süreçlerini yürütür.
Kalite Koordinatörlüğü ve Kalite Komisyonu	Politika göstergelerini kalite güvence sistemine ve PUKÖ döngüsüne entegre eder.
Etik kurullar ve araştırma/proje birimleri	Araştırma etiği, proje ve yayın süreçlerindeki alana özgü riskleri değerlendirir.
Akademik birimler	Ders ve program düzeyinde uygulama esaslarını belirler; yapay zekâ seviyelerini, öğrenci bilgilendirmesini ve alan yetkinliklerini uygular.
Tüm kullanıcılar	Yapay zekâ çıktısını doğrulamak, veri ve gizlilik kurallarına uymak, gerekli beyanı yapmak ve kendi görev alanlarındaki nihai sorumluluğu taşımakla yükümlüdür.

14.2. Olay bildirimi. Kişisel veya kurumsal verinin yetkisiz sisteme aktarılması, güvenlik açığı, önemli yanlış karar/çıktı, ayrımcı sonuç veya politika ihlali fark edildiğinde olay, uygulanabilir mevzuat ve kurum içi süreçlere göre gecikmeksizin bildirilir. Rehber v3.0'da öngörülen 24 saatlik iç bildirim hedefi uygulanır; kanuni bildirim süreleri saklıdır.

14.3. İzleme ve gözden geçirme. Politika, kalite güvence sisteminin PUKÖ döngüsüne bağlanır. Üniversite; eğitim kapsamı, sistem envanteri, yüksek etkili sistem sayısı ve değerlendirmeleri, veri güvenliği olayları, kullanıcı geri bildirimi, akademik bütünlük vakaları ve erişim eşitliği gibi göstergeleri izler. Yapay zekâ sistemleri ilk onayla sınırsız süre için uygun kabul edilmez; risk düzeyine göre performans, güvenlik, önyargı, veri koruma ve kullanıcı etkisi periyodik olarak gözden geçirilir, gerektiğinde kullanım askıya alınır veya sonlandırılır.

15. Uygulama Belgeleri, Yürürlük ve Güncelleme

15.1. Politikanın uygulanmasında Rehber v3.0, ilgili yönergeler, yetkilendirilmiş yapay zekâ sistemleri listesi, yapay zekâ etki değerlendirme formu, veri koruma ve bilgi güvenliği belgeleri ile birim rehberleri kullanılır.

15.2. Politika, Yozgat Bozok Üniversitesi Senatosunun kabulü tarihinde yürürlüğe girer ve Üniversitenin resmî internet sayfasında yayımlanır. İdari süreçler, tedarik ve sağlık hizmetlerine ilişkin hükümlerin uygulanması, Rektörlükçe onaylanacak uygulama düzenlemeleriyle tamamlanır.

15.3. Politika en az her akademik yıl sonunda; ayrıca önemli mevzuat değişikliği, yeni yüksek etkili teknoloji, ciddi veri/güvenlik olayı veya kurumsal ihtiyaç ortaya çıktığında gözden geçirilir.

Politikanın Yayımlandığı Senatonun		
Tarih ve Sayısı	Tarihi	Karar No
	04.11.2026	2026.035.198

EK. Seçilmiş Kaynaklar

1. YÖK (2024), Yükseköğretim Kurumları Bilimsel Araştırma ve Yayın Faaliyetlerinde Üretken Yapay Zekâ Kullanımına Dair Etik Rehber. https://www.yok.gov.tr/Documents/2024/yapay-zeka-kullanimina-dair-etik-rehber.pdf
2. Türkiye Yapay Zekâ Eylem Planı (2026–2030), 2026/9 sayılı Cumhurbaşkanlığı Genelgesi, Resmî Gazete 18.08.2026, sayı 33344; plan metni: https://www.sanayi.gov.tr/yapayzekaeylemplani
3. Kişisel Verileri Koruma Kurumu, yurt dışına kişisel veri aktarımı ve standart sözleşme uygulamaları: https://www.kvkk.gov.tr/
4. European Union, Regulation (EU) 2024/1689 (Artificial Intelligence Act): https://eur-lex.europa.eu/eli/reg/2024/1689/oj
5. European Union, Regulation (EU) 2026/1744 (Digital Omnibus on AI), AB Resmî Gazetesi, Temmuz 2026.
6. European Commission, Living Guidelines on the Responsible Use of Generative AI in Research, 3. sürüm, Mayıs 2026.
7. UNESCO (2023), Guidance for Generative AI in Education and Research: https://unesdoc.unesco.org/ark:/48223/pf0000386693
8. WHO (2021), Ethics and Governance of Artificial Intelligence for Health: https://www.who.int/publications/i/item/9789240029200
9. WHO (2024/2025), Ethics and Governance of AI for Health: Guidance on Large Multi-Modal Models: https://www.who.int/publications/i/item/9789240084759
10. WHO (2026), Artificial intelligence-related health research: ethics review and oversight: https://www.who.int/publications/i/item/9789240124073

Not: Bu metin, 27 Ekim 2026 itibarıyla ulaşılabilen mevzuat ve kurumsal rehberler esas alınarak hazırlanmıştır. Üst normlarda değişiklik olması hâlinde ilgili mevzuat öncelikle uygulanır.