

	SÜLEYMAN DEMİREL ÜNİVERSİTESİ Bilgi İşlem Daire Başkanlığı Yapay Zekâ Politikası	Doküman No	PLT-035
		İlk Yayın Tarihi	03.6.2025
		Revizyon Tarihi	03.6.2025
		Revizyon No	000
		Sayfa No	1 / 3

1. AMAÇ

Süleyman Demirel Üniversitesi Bilgi İşlem Daire Başkanlığı, yapay zekâ teknolojilerinin eğitim, araştırma ve idari süreçlerde etik, sorumlu ve şeffaf bir şekilde kullanılmasını teşvik eder. Bu politika, yapay zekâ kullanımına ilişkin temel ilkeleri belirlemek amacıyla başta öğrencilerimiz ve çalışanlarımız olmak üzere tüm paydaşlarımız için temel bir rehber sunmak üzere hazırlanmıştır.

2. KAPSAM

Bu politika; yapay zekâ teknolojilerinin kullanımına ilişkin tüm faaliyetlerini kapsar.

3. SORUMLULUK

Bu politikanın uygulanmasından, değerlendirilmesinden ve güncellenmesinden Bilgi İşlem Daire Başkanlığı sorumludur.

4. UYGULAMA

4.1. Temel İlkeler

4.1.1. Etik Kullanım

- Yapay zekâ, etik kurallara uygun biçimde ve toplumsal sorumluluk anlayışı çerçevesinde kullanılmalıdır.
- Yapay zekâ kullanımı, uluslararası, ulusal ve kurumsal ilkeler gözetilerek etik, güvenli ve sorumlu şekilde gerçekleştirilmelidir.
- Akademik çalışmalarda ve idari faaliyetlerde yapay zekâ kullanımı dürüstlük ilkelerine uyumlu olarak gerçekleştirilmelidir.

4.1.2. Şeffaflık

- Yapay zekânın kullanıldığı her süreçte şeffaf olunmalıdır.
- Yapay zekâ araçlarıyla üretilen içeriklerde, hangi aşamalarda ve nasıl kullanıldığı, verilerin nasıl toplandığı açıkça belirtilerek ifade edilmelidir.
- Bir çalışmanın oluşturulmasında yapay zekânın katkısı varsa, bu katkı uygun şekilde referans gösterilmelidir.
- Kurum içi uygulamalara entegre edilen yapay zekâ bileşenlerinin karar alma süreçleri, mümkün olduğunca şeffaf ve açıklanabilir olmalıdır. Özellikle kritik kararlar alan yapay zekâ sistemlerinde, kararın nasıl verildiğine dair izlenebilirlik sağlanmalıdır.
- Kurum içi uygulamalarda kullanılan yapay zekâ sistemlerinin performansından, hatalarından ve olası yanlışlıklarından kaynaklanabilecek sonuçlardan ilgili birimler ve proje sahipleri sorumlu olacaktır.

Hazırlayan	Kontrol	Onay
Sürekli İşçi - Merve GÜNEŞ	Şube Müdürü - Zekâi KÜNAR	Doktor Öğretim Üyesi - Veli ÇAPALI

	SÜLEYMAN DEMİREL ÜNİVERSİTESİ Bilgi İşlem Daire Başkanlığı Yapay Zekâ Politikası	Doküman No	PLT-035
		İlk Yayın Tarihi	03.6.2025
		Revizyon Tarihi	03.6.2025
		Revizyon No	000
		Sayfa No	2 / 3

4.1.3. Hesap Verebilirlik

- Yapay zekâ kullanımı sonucu elde edilen çıktıların ve karşılaşılan sonuçların sorumluluğunun tamamı kullanıcıya aittir.

4.1.4. Mahremiyet ve Gizlilik

- Kişisel verilerin gizliliği ve güvenliği korunmalıdır.
- Kişisel ve hassas veriler; yapay zekâ teknolojilerinde kullanılmadan önce anonimleştirilmeli, mahremiyet ve gizlilik ilkelerine uygun işlenmelidir.
- Kişisel bilgilerin gizliliğini ihlal edebilecek platformlar ve araçlar tercih edilmemelidir.
- Kurumsal verilerin yapay zekâ araçlarında kullanımı için ilgililerden onay alınmalıdır. Gizlilik içeren hiçbir belge veya bilgi kesinlikle açık (ChatGPT, DeepSeek vb.) ya da kapalı (kuruma özgü) büyük veya küçük dil modeli (LLM veya SLM) ve/veya makine öğrenmesi içeren yapay zekâ araçlarına yüklenmemelidir.
- Kurum içi geliştirilen uygulamaların ürettiği veya işlediği veriler, yapay zekâ araçlarıyla analiz edilirken veya kullanılırken Kişisel Verilerin Korunması Kanunu (KVKK) ve kurumun veri gizliliği politikalarına tam uyum sağlanmalıdır. Özellikle hassas ve kişisel verilerin anonimleştirilmesi veya psödonimleştirilmesi (takma ad kullanılması) zorunludur.
- Kurum içi uygulamalardan elde edilen verilerin, harici yapay zekâ modellerinin eğitimi için kullanılması durumunda, veri sahiplerinden gerekli izinlerin alınması ve verilerin anonimliğinin güvence altına alınması esastır

4.1.5. İnsan Denetimi

- Yapay zekâ destekli süreçlerde, nihai kararı kullanıcı vermelidir.

4.1.6. Eğitim ve Farkındalık

- Kurum içi uygulama geliştiren personele, yapay zekânın güvenli ve etik kullanımı, veri gizliliği ve kurum politikaları hakkında düzenli eğitimler verilmelidir.

4.1.7. Fikri Mülkiyet ve Alıntı

- Yapay zekâ tarafından üretilen içeriklerin kullanımı uygun şekilde kaynak gösterilerek ilgili mevzuat uyarınca yapılmalıdır.
- Yapay zekâ araçları kullanılarak kurum içi uygulamalar için geliştirilen kod, içerik veya tasarımların fikri mülkiyet hakları kuruma ait olacaktır. Harici yapay zekâ araçlarının lisans koşulları bu prensibe aykırı olmamalıdır.

4.1.8. Yapay Zekâ Destekli Geliştirme Süreçleri

- Kurum içi uygulamaların geliştirme, test veya bakım süreçlerinde yapay zekâ araçlarından faydalanılıyorsa, bu araçların ürettiği kod veya çıktıların doğruluğu, güvenliği ve lisans uyumluluğu geliştirme ekipleri tarafından titizlikle kontrol edilmelidir.

Hazırlayan	Kontrol	Onay
Sürekli İşçi - Merve GÜNEŞ	Şube Müdürü - Zekâi KÜNAR	Doktor Öğretim Üyesi - Veli ÇAPALI

	SÜLEYMAN DEMİREL ÜNİVERSİTESİ Bilgi İşlem Daire Başkanlığı Yapay Zekâ Politikası	Doküman No	PLT-035
		İlk Yayın Tarihi	03.6.2025
		Revizyon Tarihi	03.6.2025
		Revizyon No	000
		Sayfa No	3 / 3

- Yapay zekâ araçları tarafından üretilen kod parçalarının veya algoritmaların, mevcut kurum içi sistemlerle entegrasyonu öncesinde kapsamlı güvenlik testlerinden geçirilmesi ve olası zafiyetlere karşı önlem alınması gerekmektedir.

4.1.9. Hassas Kimlik Bilgilerinin (API Anahtarları, Parolalar vb.) Güvenliği ve Yönetimi

- Kurum içi geliştirilen uygulamaların kaynak kodları içerisinde, API anahtarları, veritabanı bağlantı bilgileri, servis hesaplarına ait parolalar, erişim belirteçleri (access tokens) gibi hassas kimlik bilgileri kesinlikle açık metin (hardcoded) olarak saklanmamalıdır.
- Bu tür hassas bilgiler, kurum tarafından onaylanmış güvenli kimlik bilgisi yönetim sistemleri (secrets management tools), ortam değişkenleri (environment variables) veya güvenli yapılandırma dosyaları aracılığıyla yönetilmeli ve uygulamalara çalışma zamanında güvenli bir şekilde sağlanmalıdır.
- Kaynak kodlarının yapay zekâ araçlarına yüklenmesi veya bu araçlarla analiz edilmesi durumunda, öncelikle kod içerisinde hiçbir hassas kimlik bilgisinin bulunmadığından emin olunmalıdır. Kod analiz araçları veya yapay zekâ tabanlı güvenlik tarama araçları, bu tür bilgilerin sızmasını önlemek amacıyla düzenli olarak kullanılabilir.
- Geliştiriciler, API anahtarları ve diğer kimlik bilgilerini kullanırken en az ayrıcalık (least privilege) prensibine uymalı, yani bir anahtara sadece gerekli olan minimum yetkileri atamalıdır.
- Hassas bilgilere erişim sağlayan kod parçalarının veya yapılandırmaların kurum dışı yapay zekâ araçlarıyla paylaşılması kesinlikle yasaktır.

4.1.10. Yasal Uygunluk

- 6698 sayılı Kişisel Verilerin Korunması Kanunu, 2547 sayılı Yükseköğretim Kanunu, 5846 sayılı Fikir ve Sanat Eserleri Kanunu, Yükseköğretim Kurulunun yayınladığı Yükseköğretim Kurumları Bilimsel Araştırma ve Yayın Faaliyetlerinde Üretken Yapay Zekâ Kullanımına Dair Etik Rehber ve ilgili diğer mevzuata uyum esastır.

5. YAPTIRIM

Politika ihlallerinde uygulanacak yaptırımlar, **Disiplin Prosedürü** hükümlerine göre işletilir

Hazırlayan	Kontrol	Onay
Sürekli İşçi - Merve GÜNEŞ	Şube Müdürü - Zekâi KÜNAR	Doktor Öğretim Üyesi - Veli ÇAPALI