BAHÇEŞEHİR ÜNİVERSİTESİ
SORUMLU YAPAY ZEKÂ UYGULAMA
USUL VE ESASLARI

BİRİNCİ BÖLÜM
Amaç, Kapsam ve Uygulama Eşiği

Amaç

MADDE 1 – (1) Bahçeşehir Üniversitesi, yapay zekâ teknolojilerinin eğitim-öğretim, araştırma, toplumsal katkı, idari hizmetler ve kurumsal yönetişim süreçlerinde insan kapasitesini destekleyen, hizmet kalitesini geliştiren ve toplumsal fayda üreten araçlar olarak kullanılmasını teşvik eder.

(2) Bu usul ve esasların amacı, Bahçeşehir Üniversitesi Yapay Zekâ Politikasında belirlenen insan merkezli, etik, güvenilir, adil, kapsayıcı, güvenli ve sürdürülebilir yapay zekâ yaklaşımını kurumsal uygulamalara aktarmaktır.

(3) Bu Usul ve Esaslar;

a) Yapay zekâ uygulamalarının hangi durumlarda kurumsal değerlendirmeye tabi olacağını,

b) Uygulamaların risk seviyelerinin nasıl belirleneceğini,

c) Risk seviyesiyle orantılı olarak hangi kontrol, inceleme ve onay süreçlerinin uygulanacağını,

ç) Yapay zekâ uygulamalarının yaşam döngüsü boyunca nasıl izleneceğini,

d) Hangi durumlarda uygulamaların yeniden değerlendirileceğini, durdurulacağını veya sonlandırılacağını,

e) İlgili politika, prosedür, rehber, değerlendirme aracı ve kurumsal kayıtların birbirleriyle ilişkisini belirler.

Kapsam

MADDE 2 – (1) Bu Usul ve Esaslar,

a) Üniversite tarafından geliştirilen, temin edilen, yapılandırılan, test edilen veya kurumsal kullanıma sunulan yapay zekâ sistemlerini,

b) Üniversite adına yürütülen eğitim-öğretim, araştırma, toplumsal katkı, idari, operasyonel ve yönetsel faaliyetlerde kullanılan yapay zekâ uygulamalarını,

c) Yapay zekâ bileşeni içeren üçüncü taraf yazılım, platform ve hizmetleri,

ç) Üretken yapay zekâ araçlarını, sohbet asistanlarını, karar destek sistemlerini, tahmin ve sınıflandırma modellerini, öğrenme analitiği uygulamalarını ve yapay zekâ destekli otomasyonları,

d) Üniversitenin bilgi sistemleri, kurumsal veri kaynakları veya dijital hizmetleriyle bağlantı kuran yapay zekâ uygulamalarını,

e) Üniversite adına yapay zekâ uygulaması geliştiren veya hizmet sunan iç ve dış paydaşları,

kapsar.

(2) Bu usul ve esaslar Bahçeşehir Üniversitesi Yapay Zekâ Politikası ilkelerinin kurumsal karar ve kontrol mekanizmalarına nasıl dönüştürüleceğini göstermekte olup, kapsam dışında kalan aşağıdaki hususlar ilgili tamamlayıcı belgelerde ele alınır.

a) Yapay Zekâ Yönlendirme Komitesinin oluşum ve çalışma düzeni,

b) Öğrenci ve personelin ayrıntılı kullanım kuralları,

c) Belirli bir ürün veya platforma erişim koşulları,

ç) Kişisel verilerin işlenmesine ilişkin ayrıntılı süreçler,

d) Yapay Zekâ risk değerlendirme formundaki soru ve puanlama yöntemleri,

e) Dönemsel ve yıllık gözden geçirme tarihlerinin ayrıntıları.

Kurumsal değerlendirmeyi gerektiren durumlar

MADDE 3 – (1) Bir yapay zekâ uygulaması aşağıdaki durumlardan en az birini taşıyorsa bu usul ve esaslar kapsamında kurumsal değerlendirmeye tabi tutulur:

a) Üniversite tarafından satın alınacak, lisanslanacak veya kurumsal kullanıma sunulacak olması,

b) Öğrenci, personel, araştırmacı, mezun veya dış paydaşlara hizmet vermesi,

c) Kurumsal veri, kişisel veri veya kamuya açık olmayan bilgi kullanması,

ç) Üniversitenin bilgi sistemlerine veya kurumsal veri kaynaklarına bağlanması,

d) Akademik, idari, mali veya yönetsel bir karar sürecini desteklemesi,

e) Bir kişinin akademik durumu, hizmete erişimi, çalışma hayatı veya hakları üzerinde etkili olabilmesi,

f) Üniversite adına içerik, öneri, değerlendirme, bildirim veya işlem üretmesi,

g) Geniş bir kullanıcı grubuna veya kamuya açık biçimde sunulması,

ğ) Kurumsal kaynak, bütçe, altyapı veya insan kaynağı gerektirmesi,

h) Üniversitenin hukuki, etik, güvenlik veya itibari sorumluluğunu etkileyebilmesi.

Kapsam dışındaki kullanımlar

MADDE 4 – (1) Kişilerin tamamen şahsi amaçlarla kullandığı; üniversite verisi, kurumsal kimlik, görev yetkisi, üniversite hesabı veya kurumsal kaynakla bağlantısı bulunmayan uygulamalar kurumsal başvuru ve onay sürecine tabi değildir.

(2) Bununla birlikte kullanıcıların kişisel verilerin korunması, akademik dürüstlük, fikrî ve sınai mülkiyet, bilgi güvenliği ve diğer ilgili düzenlemelerden doğan yükümlülükleri devam eder.

(3) Düşük riskli günlük kullanım örneklerinin tamamı için ayrı bir kurumsal proje değerlendirmesi yapılması gerekmez. Ancak bu kullanımlarda da onaylı araç kullanımı, veri güvenliği, çıktı doğrulama ve insan sorumluluğu esasları geçerlidir.

İKİNCİ BÖLÜM
Sorumlu Yapay Zekâ Kontrol Alanları

Sorumlu yapay zekâ kontrol alanları

MADDE 5 – (1) Bahçeşehir Üniversitesi Yapay Zekâ Politikasında belirlenen ilkeler, kurumsal uygulamalarda aşağıdaki kontrol alanları üzerinden işletilir.

Politika alanı	Uygulamadaki temel kontrol
İnsan merkezlilik	İnsan denetimi, müdahale ve nihai insan sorumluluğu
Etik ve sorumlu kullanım	Meşru amaç, gereklilik, ölçülülük ve beklenen faydanın tanımlanması
Şeffaflık ve açıklanabilirlik	Kullanıcı bilgilendirmesi, yapay zekâ etkileşiminin açıklanması ve karar gerekçesinin izlenebilirliği
Hesap verebilirlik	Uygulama sahibi, veri sahibi, teknik sorumlu ve karar sahibinin belirlenmesi
Adalet, eşitlik ve kapsayıcılık	Önyargı, ayrımcılık, erişilebilirlik ve farklı kullanıcı grupları üzerindeki etkinin değerlendirilmesi
Veri güvenliği ve mahremiyet	Veri minimizasyonu, yetkilendirme ve Veri Koruma Prosedürüne uygunluk
Akademik dürüstlük ve bilimsel etik	İnsan katkısı, kaynak doğrulama, beyan ve bilimsel sorumluluk
Kalite güvencesi	Performans ölçümü, kullanıcı geri bildirimi ve sürekli iyileştirme
Sürdürülebilirlik ve toplumsal katkı	Kaynak kullanımı, kurumsal fayda ve toplumsal etkinin değerlendirilmesi

Meşru amaç, gereklilik ve ölçülülük

MADDE 6 – (1) Her yapay zekâ uygulaması için açık, belirli ve kurumsal amaçlarla uyumlu bir kullanım amacı tanımlanır.

(2) Yapay zekâ kullanımı bir amaç olarak değil, belirlenmiş bir ihtiyacın karşılanmasına yönelik araç olarak değerlendirilir. Aynı sonucun daha az veri işleyen, daha düşük riskli veya daha kolay denetlenebilir bir yöntemle elde edilip edilemeyeceği dikkate alınır.

(3) Bir sistemin teknik olarak kullanılabilir olması, kullanımının kurumsal olarak gerekli veya uygun olduğu anlamına gelmez.

İnsan denetimi ve sorumluluğu

MADDE 7 – (1) Yapay zekâ destekli süreçlerde akademik, bilimsel, hukuki, idari ve yönetsel nihai sorumluluk insanlardadır.

(2) İnsan denetiminden sorumlu kişi;

a) Sistemin kullanım amacını ve sınırlarını bilmeli,

b) Çıktıyı değerlendirebilecek yeterliliğe sahip olmalı,

c) Çıktıyı reddetme veya değiştirme yetkisini kullanabilmeli,

ç) Gerektiğinde süreci durdurabilmeli,

d) Karar ve sonuçların sorumluluğunu üstlenebilmelidir.

(3) İnsan denetimi yalnızca yapay zekâ çıktısının biçimsel olarak onaylanması şeklinde yürütülemez.

Şeffaflık

MADDE 8 – (1) Kullanıcılar, yapay zekâ destekli bir sistemle etkileşimde oldukları konusunda açık ve anlaşılır biçimde bilgilendirilir. Uygun olduğu ölçüde kullanıcıya;

a) Sistemin amacı,

b) Bilgilerin dayandığı kaynaklar,

c) Sistemin önemli sınırlılıkları,

ç) Sistemin resmî karar veya görüş üretip üretmediği,

d) İnsan desteğine nasıl ulaşılacağı,

e) Kişisel veya gizli veri paylaşılmaması gerektiği

açıklanır.

Kişisel verilerin korunması, veri güvenliği ve mahremiyet

MADDE 9 – (1) Yapay zekâ uygulamalarında kişisel verilerin işlenmesi; 6698 sayılı Kişisel Verilerin Korunması Kanunu, Bahçeşehir Üniversitesi Kişisel Verilerin Korunması ve Veri Mahremiyeti Politikası ile Üniversitenin ilgili bilgi güvenliği ve veri yönetimi düzenlemelerine uygun olarak yürütülür.

(2) Yapay zekâ uygulamalarında kullanılan kişisel veriler aşağıdaki ilkelere uygun olarak işlenir:

a) Hukuka ve dürüstlük kurallarına uygun,

b) Doğru ve gerektiğinde güncel,

c) Belirli, açık ve meşru amaçlarla bağlantılı,

ç) İşleme amacıyla sınırlı ve ölçülü,

d) Yalnızca gerekli süre boyunca muhafaza edilecek

(3) Kişisel veri işleyen bir yapay zekâ uygulaması kullanıma alınmadan önce, uygulamanın risk seviyesiyle orantılı olarak aşağıdaki kriterler değerlendirilir.

a) Veri işleme amacı,

b) İşlenen veri kategorileri ve ilgili kişi grupları,

c) Veri işlemenin hukuki sebebi,

ç) Verinin kaynağı,

d) Erişim ve yetkilendirme yapısı,

e) Saklama ve silme koşulları,

f) Yurt içi veya yurt dışı aktarım durumu,

g) Hizmet sağlayıcı ve üçüncü taraf ilişkileri,

ğ) Uygulanacak teknik ve idari tedbirler

(4) Kişisel veriler ile gizli veya sınırlı erişime tabi kurumsal verilerin gizliliğini, bütünlüğünü ve erişilebilirliğini korumaya yönelik uygun teknik ve idari tedbirler uygulanır. Verilere erişim, görev ve ihtiyaçla sınırlı tutulur.

(5) Yapay zekâ aracının veya hizmet sağlayıcısının verileri saklama, aktarma, yeniden kullanma, model geliştirme veya alt hizmet sağlayıcılara iletme koşulları, uygulamanın kurumsal kullanımından önce ilgili değerlendirme sürecinde incelenir.

(6) Kişisel verilerin işlenmesine, aktarılmasına, saklanmasına, silinmesine, ihlal yönetimine ve üçüncü taraf hizmet sağlayıcılara ilişkin operasyonel ayrıntılar, Bahçeşehir Üniversitesi Kişisel Verilerin Korunması ve Veri Mahremiyeti Politikası ile ilgili veri koruma prosedürleri kapsamında yürütülür.

Adalet, eşitlik, kapsayıcılık ve erişilebilirlik

MADDE 10 – (1) Yapay zekâ uygulamalarının farklı kültürel, sosyal, ekonomik, dilsel ve demografik özelliklere sahip kişi ve gruplar üzerindeki muhtemel etkileri, uygulamanın niteliği ve risk seviyesiyle orantılı olarak değerlendirilir.

(2) Yapay zekâ uygulamalarının belirli kişi veya gruplar bakımından sistematik hata, ayrımcılık, dışlama, haksız avantaj veya dezavantaj doğurmaması için uygun önleyici ve düzeltici kontroller uygulanır.

(3) Yapay zekâ uygulamalarının tasarımında ve kullanımında aşağıdaki kriterler dikkate alınır.

a) Engellilik ve erişilebilirlik ihtiyaçları,

b) Dil farklılıkları,

c) Dijital araç ve hizmetlere erişim farklılıkları,

ç) Kullanıcıların teknik yeterlilik düzeyleri

(4) Yapay zekâ destekli bir faaliyet, kişilerin gizlilik, erişilebilirlik veya fırsat eşitliği bakımından dezavantajlı hâle gelmesine yol açıyorsa uygun insan destekli veya yapay zekâ kullanılmayan alternatif süreçler değerlendirilir.

Doğruluk, güvenilirlik ve teknik sağlamlık

MADDE 11 – (1) Yapay zekâ sistemlerinin çıktıları doğrudan doğru, eksiksiz veya güncel kabul edilmez. Çıktılar, kullanım amacının ve risk seviyesinin gerektirdiği ölçüde insan değerlendirmesi, kaynak kontrolü veya diğer doğrulama yöntemleriyle incelenir.

(2) Üniversiteye ilişkin bilgi sunan yapay zekâ uygulamalarında, yetkili birimlerce doğrulanmış ve güncelliği izlenen kaynakların kullanılması esastır.

(3) Yapay zekâ uygulamaları, amaçlanan kullanım koşullarını temsil eden örnekler üzerinden uygun olduğu ölçüde test edilir. Testlerde en az aşağıdaki riskler dikkate alınır.

a) Yanlış veya yanıltıcı çıktı,

b) Eksik veya güncelliğini yitirmiş bilgi,

c) Uydurma bilgi ve kaynak üretimi,

ç) Önyargılı veya tutarsız sonuçlar,

d) Yetkisiz erişim veya işlem,

e) Kötüye kullanım,

f) Sistem veya entegrasyon hatası

(4) Kurumsal sistemlerde kayıt oluşturabilen, değiştirebilen, silebilen veya üçüncü taraflara işlem iletebilen yapay zekâ uygulamalarında yetkiler görevle sınırlandırılır; gerekli işlemler insan onayına bağlanır ve yapılan işlemler uygun ölçüde kayıt altına alınır.

(5) Yapay zekâ uygulamalarında hata veya hizmet kesintisi oluşması hâlinde insan destekli sürece geçiş, işlemin durdurulması veya önceki güvenli duruma dönüş yöntemleri risk seviyesiyle orantılı olarak belirlenir.

Akademik dürüstlük, bilimsel sorumluluk ve fikrî haklar

MADDE 12 – (1) Yapay zekâ kullanımı; öğrencinin, akademisyenin, araştırmacının veya personelin özgün katkısını, mesleki değerlendirmesini ve akademik ya da bilimsel sorumluluğunu ortadan kaldırmaz.

(2) Yapay zekâ aracılığıyla uydurma veri, kaynak, atıf, bulgu, kanıt, kimlik veya resmî kayıt üretilemez ve kullanılamaz.

(3) Yapay zekâ tarafından üretilen analiz, öneri, metin, kod veya diğer çıktılar gerekli doğrulama ve insan değerlendirmesi yapılmadan akademik, bilimsel, idari veya resmî çıktı olarak kullanılamaz.

(4) Yapay zekâ kullanımının açıklanmasına, kaynak gösterilmesine, öğrencilerin özgün katkısına ve derslerde kullanım sınırlarına ilişkin ayrıntılar Öğrenci Yapay Zekâ Kullanım Rehberi ile Personel Yapay Zekâ Kullanım Rehberinde düzenlenir.

(5) Yapay zekâ sistemlerine girilen veya bu sistemlerden elde edilen materyaller bakımından aşağıdaki hususlar gözetilir.

a) Üniversitenin, kullanıcının veya üçüncü kişilerin fikrî ve sınai mülkiyet hakları

b) Lisans ve kullanım koşulları,

c) Gizlilik yükümlülükleri,

ç) Araştırma, yayın veya sözleşme sınırlamaları

Kalite güvencesi, kurumsal fayda ve sürdürülebilirlik

MADDE 13 – (1) Yapay zekâ uygulamaları, Üniversitenin kalite güvencesi ve sürekli iyileştirme yaklaşımı doğrultusunda izlenir ve değerlendirilir.

(2) Bir yapay zekâ uygulamasının başarısı yalnızca kullanıcı, mesaj, işlem, içerik veya teknik kaynak tüketimi üzerinden ölçülmez. Değerlendirmede uygun olduğu ölçüde aşağıdaki kriterler birlikte dikkate alınır.

a) Öğrenme ve öğretme desteği,

b) Araştırma ve bilimsel üretim,

c) Hizmet kalitesi,

ç) Süreç verimliliği,

d) Kullanıcı deneyimi,

e) Hata ve risklerin azaltılması,

f) Kaynak kullanımı,

g) Maliyet ve toplam sahip olma maliyeti,

ğ) Bakım ve güncelleme ihtiyacı,

h) Toplumsal ve kurumsal fayda

(3) Kurumsal fayda üretmeyen, gerekli güncelliği sağlanamayan, kaynak kullanımıyla orantılı çıktı oluşturmayan veya kabul edilebilir risk düzeyini aşan uygulamalar yeniden değerlendirilir.

(4) Yapay zekâ sistemlerinin sosyal, ekonomik ve çevresel etkileri uygulamanın ölçeğiyle orantılı olarak değerlendirilir. Gereksiz veri işleme ve kullanım amacıyla orantısız teknik kaynak tüketiminden kaçınılır.

ÜÇÜNCÜ BÖLÜM
Risk Sınıflandırması

Risk sınıflandırmasına ilişkin genel esaslar

MADDE 14 – (1) Yapay zekâ uygulamaları; kullanım amacı, etkilenen kişi ve gruplar, kullanılan veri, sistemin özerklik düzeyi ve muhtemel sonuçları dikkate alınarak aşağıdaki risk seviyelerinden birine dâhil edilir:

a) Seviye 1 – Düşük risk,

b) Seviye 2 – Kontrollü risk,

c) Seviye 3 – Yüksek risk,

ç) Seviye 4 – Kabul edilemez kullanım.

(2) Risk seviyesi, kullanılan aracın veya teknolojinin ticari adına göre değil, somut kullanım senaryosuna göre belirlenir. Aynı araç, farklı kullanım amaçlarında farklı risk seviyelerinde değerlendirilebilir.

(3) Uygulamanın birden fazla risk seviyesine ilişkin özellik taşıması hâlinde daha yüksek risk seviyesi esas alınır.

(4) Risk sınıflandırması ve alınacak tedbirlerin ayrıntılı kaydı Yapay Zekâ Risk Değerlendirme Şablonu üzerinden yürütülür.

Seviye 1 – Düşük risk

MADDE 15 – (1) Düşük riskli kullanımlar genel olarak aşağıda belirtilen uygulamalardır.

a) Kamuya açık veya kişisel veri içermeyen bilgilerle çalışan,

b) Kişiler hakkında karar vermeyen,

c) Kurumsal sistemlerde işlem yapmayan,

ç) Hatası önemli akademik, hukuki, mali veya idari sonuç doğurmayan,

d) Çıktısı kullanıcı tarafından kolaylıkla kontrol edilebilen

(2) Düşük riskli kullanım örnekleri arasında aşağıdaki örnekler yer alabilir.

a) Fikir geliştirme,

b) İlk taslak oluşturma,

c) Kamuya açık bir metni özetleme,

ç) Dil ve anlatım iyileştirmesi,

d) Kişisel veri içermeyen örnek veriyle kod geliştirme,

e) Görsel veya sunum taslağı hazırlama

(3) Düşük riskli günlük kullanımlar için ayrı bir tam risk değerlendirmesi aranmaz. Bununla birlikte çıktı doğrulama, veri güvenliği, insan sorumluluğu ve ilgili kullanıcı rehberlerindeki kurallar uygulanır.

Seviye 2 – Kontrollü risk

MADDE 16 – (1) Kontrollü riskli uygulamalar genel olarak aşağıda verilen türdeki uygulamalardır.

a) Belirli bir ders, birim veya kullanıcı grubuna hizmet veren,

b) Kurumsal içerik veya sınırlı veri kaynağı kullanan,

c) Öğrenci, personel veya dış paydaşlarla doğrudan etkileşime giren,

ç) Yanlış çıktısı sınırlı ancak anlamlı bir hizmet veya öğrenme etkisi doğurabilen,

d) Üniversitenin onaylı bilgi kaynaklarına dayalı cevap veya öneri üreten.

(2) Kontrollü riskli uygulamalara aşağıdaki örnek gösterilebilir.

a) Ders veya öğrenme faaliyetine özgü ders asistanları uygulamaları,

b) Birim içi doküman arama ve soru-cevap asistanları,

c) Kişiler hakkında karar vermeyen öğrenci hizmetleri asistanları,

ç) Araştırma veya kodlama destek sistemleri,

d) Sınırlı kullanıcı grubuna yönelik idari asistanlar

(3) Kontrollü riskli uygulamalarda en az aşağıdaki kriterler aranır.

a) Uygulama sahibinin belirlenmesi,

b) Ön risk değerlendirmesi,

c) Veri ve kaynak kapsamının tanımlanması,

ç) Kullanıcı bilgilendirmesi,

d) Erişim sınırlarının belirlenmesi,

e) Kontrollü test veya pilot,

f) İzleme ve gözden geçirme yöntemi

Seviye 3 – Yüksek risk

MADDE 17 – (1) Aşağıdaki özelliklerden birini veya birkaçını taşıyan yapay zekâ uygulamaları yüksek riskli olarak değerlendirilir:

a) Özel nitelikli kişisel veri veya hassas veri işlemesi,

b) Kişisel verileri geniş ölçekte veya sistematik biçimde işlemesi,

c) Kişiler hakkında profil, tahmin, sınıflandırma veya risk değerlendirmesi oluşturması,

ç) Öğrencilerin akademik ilerlemesini, notunu, bursunu, disiplin durumunu veya hizmetlere erişimini etkileyebilmesi,

d) Personelin işe alınması, görevlendirilmesi, performansı, terfi veya çalışma ilişkisini etkileyebilmesi,

e) Sağlık, psikolojik danışmanlık veya özel destek ihtiyaçlarına ilişkin veri kullanması,

f) Öğrenci başarısızlığı, terk, davranış veya destek ihtiyacı tahmini yapması,

g) Biyometrik veri veya kimlik doğrulama işlevi kullanması,

ğ) Kurumsal bilgi sistemlerinde kayıt oluşturma, değiştirme, silme veya işlem yapma yetkisinin bulunması,

h) Hatalı çıktının kişilerin hakları veya Üniversitenin hukuki, mali ya da itibari durumu üzerinde önemli etki doğurabilmesi,

ı) Sistem çıktısının bağımsız olarak doğrulanmasının veya açıklanmasının güç olması.

(2) Yüksek riskli uygulamalarda en az aşağıdaki kriterler aranır.

a) Tam yapay zekâ risk değerlendirmesi,

b) Gerekli kişisel veri koruma ve bilgi güvenliği incelemeleri,

c) İlgili etik, hukuki, teknik, pedagojik veya akademik görüşler,

ç) Belgelenmiş insan denetimi,

d) Kontrollü pilot,

e) Kullanıcı bilgilendirmesi,

f) İtiraz ve insan tarafından yeniden değerlendirme yolu,

g) Yapay Zekâ Yönlendirme Komitesi değerlendirmesi

(3) Yüksek riskli uygulamalar, gerekli değerlendirme ve kurumsal onaylar tamamlanmadan üretim ortamında kullanıma alınamaz.

Seviye 4 – Kabul edilemez kullanım

MADDE 18 – (1) Bahçeşehir Üniversitesi kapsamında aşağıdaki kullanımlara izin verilmez:

a) Not, kabul, burs, disiplin, işe alım, performans, terfi veya iş ilişkisinin sona ermesi gibi kişileri önemli ölçüde etkileyen nihai kararların tamamen yapay zekâ sistemine bırakılması,

b) Kişiler hakkında genel güvenilirlik, değer, uygunluk veya davranış puanı oluşturulması,

c) Eğitim veya çalışma ortamlarında kişilerin duygu, kişilik veya hassas özelliklerinin izinsiz biçimde çıkarılması ve karar süreçlerinde kullanılması,

ç) Yetkisiz biyometrik izleme veya kitlesel gözetim yapılması,

d) Kişilerin yaşı, engellilik durumu, bilgi eksikliği veya diğer kırılganlıklarından yararlanılarak davranışlarının yönlendirilmesi,

e) Kişisel, gizli veya kamuya açık olmayan kurumsal verilerin gerekli değerlendirme ve yetkilendirme yapılmadan yapay zekâ sistemleriyle işlenmesi,

f) Yapay zekâ aracılığıyla veri, kaynak, atıf, delil, kimlik veya resmî kayıt uydurulması,

g) Güvenlik kontrollerini veya erişim yetkilerini aşmak amacıyla yapay zekâ kullanılması,

ğ) İnsan denetiminin yalnızca görünüşte bulunduğu ve yapay zekâ çıktısının sorgulanmadan uygulandığı karar süreçleri.

(2) Kabul edilemez nitelikteki bir teknolojinin yalnızca araştırma amacıyla incelenmesi; gerçek kişiler üzerinde kullanılmaması, uygun veri kullanılması ve gerekli etik, hukuki ve güvenlik onaylarının alınması koşuluyla ayrıca değerlendirilir.

DÖRDÜNCÜ BÖLÜM
Yapay Zekâ Uygulama Yaşam Döngüsü

İhtiyacın ve sahipliğin belirlenmesi

MADDE 19 – (1) Kurumsal bir yapay zekâ uygulaması için aşağıdaki hususlar belirlenir.

a) Çözülmek istenen ihtiyaç,

b) Kullanım amacı,

c) Hedef kullanıcı grubu,

ç) Beklenen kurumsal fayda,

d) Uygulama sahibi,

e) Başarı ölçütleri

(2) Aynı ihtiyacın daha düşük riskli, daha az veri işleyen veya daha kolay denetlenebilir bir yöntemle karşılanıp karşılanamayacağı değerlendirilir.

Ön bildirim ve risk sınıflandırması

MADDE 20 – (1) Üniversite tarafından satın alınması, geliştirilmesi, kurumsal kullanıma sunulması veya sistemlere entegre edilmesi planlanan kontrollü ve yüksek riskli uygulamalar Yapay Zekâ Yetkinlik Birimine bildirilir.

(2) Kullanım amacı, veri kapsamı, sistemin özerklik düzeyi, hedef kullanıcılar ve muhtemel etkiler üzerinden ön inceleme ve risk sınıflandırması yapılır.

(3) Kontrollü ve yüksek riskli uygulamalar değerlendirme aşamasından itibaren kurumsal yapay zekâ envanterine kaydedilir.

Değerlendirme ve karar

MADDE 21 – (1) Uygulamanın niteliğine ve risk seviyesine göre aşağıdaki süreçler uygulanır.

a) Yapay Zekâ Risk Değerlendirme Şablonu,

b) Veri koruma ve bilgi güvenliği değerlendirmesi,

c) Etik veya akademik değerlendirme,

ç) Pedagojik ve ölçme-değerlendirme incelemesi,

d) Fikrî ve sınai mülkiyet incelemesi,

e) Tedarikçi, sözleşme ve erişim değerlendirmesi

(2) Değerlendirme sonucunda aşağıdaki kararlardan biri verilir:

a) Kullanıma uygun,

b) Belirli koşullarla kullanıma uygun,

c) Pilot uygulamaya uygun,

ç) Ek bilgi veya revizyon gerekli,

d) Geçici olarak uygun değil,

e) Kullanıma uygun değil.

(3) Kararda uygulama sahibi, kullanım kapsamı, gerekli kontroller, veri ve kullanıcı sınırları, izleme yöntemi ve gözden geçirme tarihi belirtilir.

Pilot ve kullanıma alma

MADDE 22 – (1) Kontrollü ve yüksek riskli uygulamalar, mümkün olduğu ölçüde sınırlı kullanıcı, veri ve işlev kapsamında pilot olarak uygulanır.

(2) Pilot sürecinde teknik performansın yanı sıra doğruluk, yanıltıcı çıktı, önyargı, kullanıcı deneyimi, insan müdahalesi, veri kullanımı, güvenlik ve beklenmeyen etkiler izlenir.

(3) Bir uygulama ancak aşağıdaki kriterleri sağlıyorsa kurumsal kullanıma alınabilir.

a) Sorumluları belirlenmiş,

b) Risk seviyesi tespit edilmiş,

c) Gerekli değerlendirme ve onayları tamamlanmış,

ç) Veri ve erişim sınırları tanımlanmış,

d) İnsan denetimi kurulmuş,

e) Kullanıcı bilgilendirmesi hazırlanmış,

f) İzleme ve durdurma yöntemi belirlenmiş

İzleme ve önemli değişiklikler

MADDE 23 – (1) Kullanıma alınan yapay zekâ uygulamaları, risk seviyeleriyle orantılı olarak izlenir.

(2) Aşağıdaki değişikliklerden birinin gerçekleşmesi hâlinde uygulamanın risk sınıflandırması ve önceki onayı yeniden değerlendirilir:

a) Kullanım amacının değişmesi,

b) Yeni kullanıcı grubuna açılması,

c) Yeni veya daha hassas veri kaynağı eklenmesi,

ç) Modelin veya hizmet sağlayıcının değişmesi,

d) Kurumsal sistem entegrasyonu yapılması,

e) Sisteme yeni işlem veya karar yetkisi verilmesi,

f) Kullanım ölçeğinin önemli ölçüde artması,

g) Güvenlik, performans veya sözleşme koşullarının önemli ölçüde değişmesi.

Durdurma ve sonlandırma

MADDE 24 – (1) Bir yapay zekâ uygulaması aşağıdaki durumlardan bir veya daha fazlasına sahip olması hâlinde geçici olarak durdurulabilir, yeniden yapılandırılabilir veya sonlandırılabilir.

a) Kabul edilemez risk oluşturması,

b) Amacını karşılamaması,

c) Sürekli hatalı veya ayrımcı sonuç üretmesi,

ç) Veri güvenliği veya gizlilik ihlaline yol açması,

d) Gerekli güncelliğin sağlanamaması,

e) Kurumsal faydasının kaynak kullanımını karşılamaması,

f) Hizmet sağlayıcı veya sözleşme koşullarının uygunluğunu kaybetmesi

(2) Sonlandırma sürecinde veri, kullanıcı erişimi, sistem entegrasyonları, kayıtlar, içerik sahipliği ve üçüncü taraf hizmet ilişkileri kontrollü biçimde kapatılır.

BEŞİNCİ BÖLÜM
Asgari Kontroller ve Karar Yapısı

Risk seviyesine göre asgari kontroller

MADDE 25 – (1) Aşağıdaki tabloda yer alan kontroller asgari niteliktedir. Uygulamanın niteliğine, kullanılan veriye ve ilgili mevzuata göre ek kontrol veya onay süreçleri uygulanabilir.

Kontrol	Düşük risk	Kontrollü risk	Yüksek risk
Kullanım amacının belirlenmesi	Gerekli	Gerekli	Gerekli
Uygulama sahibinin belirlenmesi	Kullanıcı veya birim sorumluluğu	Zorunlu	Zorunlu
Kurumsal envanter kaydı	Gerektiğinde	Zorunlu	Zorunlu
Ön risk incelemesi	Genel kullanım kuralları	Zorunlu	Zorunlu
Tam risk değerlendirmesi	Aranmaz	Gerektiğinde	Zorunlu
Kişisel verilerin korunması, veri güvenliği ve mahremiyet	Veri işleniyorsa yeniden sınıflandırılır	Kullanıma göre	Zorunlu
Bilgi güvenliği incelemesi	Entegrasyon varsa	Kullanıma göre	Zorunlu
Kullanıcı bilgilendirmesi	Gerektiğinde	Zorunlu	Zorunlu
İnsan denetimi	Kullanıcı kontrolü	Açıkça tanımlanır	Belgelenir
Pilot uygulama	İsteğe bağlı	Kural olarak gerekli	Zorunlu
Uzman birim görüşü	Gerektiğinde	Kullanıma göre	Zorunlu
Komite değerlendirmesi	Aranmaz	Gerektiğinde	Zorunlu
Periyodik gözden geçirme	Genel takvim	En az dönemsel	Riskle orantılı olarak daha sık
İtiraz ve yeniden değerlendirme yolu	Kural olarak aranmaz	Etkiye göre	Zorunlu
Sonlandırma yöntemi	Gerektiğinde	Gerekli	Zorunlu

Uygulama sahibi
MADDE 26 – (1) Her kontrollü veya yüksek riskli uygulama için bir uygulama sahibi belirlenir.

(2) Uygulama sahibi aşağıdaki hususları sağlamakla sorumludur.

a) Kullanım amacı ve kapsamını tanımlamak,
b) Risk değerlendirmesi için gerekli bilgileri sağlamak,
c) Onaylanan kontrol ve sınırlamaları uygulamak,
ç) İnsan denetimini sağlamak,
d) Kullanım ve performansı izlemek,
e) Önemli değişiklik, hata veya olayları bildirmek

Yapay Zekâ Yetkinlik Birimi
MADDE 27 – (1) Yapay Zekâ Yetkinlik Birimi;

a) Başvuru ve ön inceleme sürecini koordine eder,
b) Risk sınıflandırmasına destek olur,
c) İlgili uzman görüşlerinin alınmasını sağlar,
ç) Kurumsal yapay zekâ envanterini tutar,
d) Risk değerlendirme ve gözden geçirme kayıtlarını izler,
e) Yüksek riskli veya stratejik uygulamaları Komite gündemine hazırlar.

(2) Yapay Zekâ Yetkinlik Birimi, başka kurul, komisyon veya birimin görev alanına giren konularda tek başına nihai onay vermez.

Uzman birimler
MADDE 28 – (1) Uygulamanın niteliğine göre ilgili akademik ve idari birimler aşağıdaki alanlarda değerlendirme yapar ve görüş sunar.

a) Kişisel verilerin korunması,
b) Bilgi güvenliği ve teknik mimari,
c) Hukuki uygunluk ve sözleşmeler,
ç) Etik ve akademik dürüstlük,
d) Eğitim ve ölçme-değerlendirme,
e) Fikrî ve sınai mülkiyet,
f) Satın alma, erişim ve lisanslama,
g) Erişilebilirlik

Yapay Zekâ Yönlendirme Komitesi
MADDE 29 – (1) Yapay Zekâ Yönlendirme Komitesi;

a) Yüksek riskli uygulamaları,
b) Birden fazla birimi veya geniş kullanıcı kitlesini etkileyen uygulamaları,
c) Stratejik nitelikteki kurumsal yatırımları,
ç) Önemli etik, hukuki, güvenlik veya itibari risk taşıyan uygulamaları,
d) Risk seviyesi veya devam kararı konusunda görüş ayrılığı bulunan uygulamaları değerlendirir.

(2) Komitenin oluşumu, görevleri, çalışma düzeni ve karar süreçleri Bahçeşehir Üniversitesi Yapay Zekâ Yönlendirme Komitesi Çalışma Usul ve Esaslarında düzenlenir.

Yetkili kurul ve makamlar
MADDE 30 – (1) İlgili mevzuat veya Üniversite düzenlemeleri uyarınca Senato, Rektörlük, etik kurul, disiplin organı, satın alma makamı veya başka bir yetkili kurulun kararı gerekiyorsa bu Usul ve Esaslar kapsamında yapılan değerlendirme söz konusu kararın yerine geçmez.

ALTINCI BÖLÜM
İlgili Belgeler ve Kayıtlar

Tamamlayıcı belgeler

MADDE 31 – (1) Bu Usul ve Esaslar aşağıdaki belgelerle birlikte uygulanır:

Belge	Düzenlediği alan
Bahçeşehir Üniversitesi Yapay Zekâ Politikası	Üst düzey kurumsal yaklaşım ve ilkeler
Bahçeşehir Üniversitesi Kişisel Verilerin Korunması ve Veri Mahremiyeti Politikası	Üst düzey kurumsal yaklaşım ve ilkeler
Yapay Zekâ Yönlendirme Komitesi Çalışma Usul ve Esasları	Yönetişim, görev ve karar yapısı
Öğrenci Yapay Zekâ Kullanım Rehberi	Öğrencilerin kullanım ve akademik dürüstlük kuralları
Personel Yapay Zekâ Kullanım Rehberi	Akademik ve idari personelin kullanım sorumlulukları
Yapay Zekâ Veri Koruma Prosedürü	YZ uygulamalarındaki operasyonel veri koruma süreçleri
Yapay Zekâ Risk Değerlendirme Şablonu	Uygulama bazlı risk, kontrol ve onay kaydı
Yapay Zekâ Gözden Geçirme Takvimi	Aylık, dönemlik ve yıllık izleme faaliyetleri

Kurumsal kayıtlar

MADDE 32 – (1) Kontrollü ve yüksek riskli uygulamalar için risk seviyesiyle orantılı olarak aşağıdaki kayıtlar tutulur:

a) Uygulamanın adı ve amacı,
b) Uygulama sahibi,
c) Hedef kullanıcı grubu,
ç) Risk seviyesi,
d) Kullanılan veri ve kaynak türleri,
e) İnsan denetimi yöntemi,
f) Yapılan değerlendirmeler ve alınan görüşler,
g) Onay veya karar,
ğ) Pilot sonuçları,
h) Kullanım ve performans göstergeleri,
ı) Önemli değişiklikler,
i) Olay ve düzeltici faaliyetler,
j) Gözden geçirme tarihi,
k) Devam, revizyon, durdurma veya sonlandırma durumu.

YEDİNCİ BÖLÜM
İzleme ve Son Hükümler

İzleme ve gözden geçirme

MADDE 33 – (1) Bu Usul ve Esasların uygulanması aşağıdaki kaynaklar üzerinden izlenir.

a) Kurumsal yapay zekâ envanteri,
b) Risk değerlendirme kayıtları,
c) Uygulama ve proje raporları,
ç) Kullanıcı geri bildirimleri,
d) Hata, şikâyet ve olay kayıtları,
e) Eğitim ve yetkinlik verileri,
f) Kurumsal performans göstergeleri

(2) İzleme faaliyetlerinin dönemleri, sorumluları ve çıktıları Yapay Zekâ Gözden Geçirme Takviminde belirlenir.

(3) Bu Usul ve Esaslar; teknolojik gelişmeler, mevzuat değişiklikleri, uygulama deneyimleri, risk ve olay kayıtları, kullanıcı geri bildirimleri ile Yapay Zekâ Politikası ve Yol Haritasındaki değişiklikler dikkate alınarak en az yılda bir kez gözden geçirilir.

Diğer düzenlemelerle ilişki

MADDE 34 – (1) Bu Usul ve Esaslar, Üniversitenin akademik dürüstlük, bilimsel araştırma ve yayın etiği, kişisel verilerin korunması, bilgi güvenliği, fikrî ve sınai mülkiyet, eğitim-öğretim, öğrenci, personel, kalite güvencesi, satın alma ve kurumsal risk yönetimine ilişkin düzenlemeleriyle birlikte uygulanır.

(2) Bu Usul ve Esaslar, diğer kurul, komisyon, birim ve yetkili makamların mevcut görev, yetki ve sorumluluklarını ortadan kaldırmaz.

(3) Bu Usul ve Esaslar ile başka bir Üniversite düzenlemesi arasında yorum farklılığı oluşması hâlinde yürürlükteki mevzuat, Senato kararları ve üst düzenleme niteliğindeki Üniversite politikaları esas alınır.

Hüküm bulunmayan hâller

MADDE 35 – (1) Bu Usul ve Esaslarda hüküm bulunmayan hâllerde;

a) İlgili ulusal mevzuat,

b) Bahçeşehir Üniversitesi Yapay Zekâ Politikası,

c) Bahçeşehir Üniversitesi Kişisel Verilerin Korunması ve Veri Mahremiyeti Politikası,

ç) Üniversitenin ilgili politika, yönerge, usul ve esas, prosedür ve kararları,

d) Senato ve Üniversite Yönetim Kurulu kararları,

e) Rektörlük karar ve talimatları

uygulanır.

(2) Bu Usul ve Esasların uygulanmasında ortaya çıkan tereddütleri gidermeye Rektör yetkilidir.

Yürürlük

MADDE 36 – (1) Bu Usul ve Esaslar, Bahçeşehir Üniversitesi Senatosu tarafından kabul edildiği tarihte yürürlüğe girer.

Yürütme

MADDE 37 – (1) Bu Usul ve Esaslar hükümlerini Bahçeşehir Üniversitesi Rektörü yürütür.

BAHÇEŞEHİR UNIVERSITY
RESPONSIBLE ARTIFICIAL INTELLIGENCE IMPLEMENTATION PROCEDURES AND PRINCIPLES

PART ONE
Purpose, Scope and Threshold for Application

Purpose

ARTICLE 1 – (1) Bahçeşehir University encourages the use of artificial intelligence technologies as tools that support human capacity, improve service quality, and generate societal benefit in teaching and learning, research, societal contribution, administrative services, and institutional governance processes.

(2) The purpose of these Procedures and Principles is to translate the human-centred, ethical, trustworthy, fair, inclusive, secure, and sustainable artificial intelligence approach established in the Bahçeşehir University Artificial Intelligence Policy into institutional practice.

(3) These Procedures and Principles set out:

a) the circumstances in which artificial intelligence applications are subject to institutional assessment;

b) how the risk levels of applications are determined;

c) the controls, reviews, and approval processes to be applied in proportion to the level of risk;

d) how artificial intelligence applications are monitored throughout their life cycle;

e) the circumstances in which applications are reassessed, suspended, or terminated; and

f) the relationship among the relevant policies, procedures, guidelines, assessment tools, and institutional records.

Scope

ARTICLE 2 – (1) These Procedures and Principles cover:

a) artificial intelligence systems developed, procured, configured, tested, or made available for institutional use by the University;

b) artificial intelligence applications used in teaching and learning, research, societal contribution, administrative, operational, and managerial activities carried out on behalf of the University;

c) third-party software, platforms, and services that incorporate an artificial intelligence component;

d) generative artificial intelligence tools, conversational assistants, decision-support systems, prediction and classification models, learning analytics applications, and artificial intelligence-supported automation;

e) artificial intelligence applications connected to the University’s information systems, institutional data sources, or digital services; and

f) internal and external stakeholders that develop artificial intelligence applications or provide services on behalf of the University.

(2) These Procedures and Principles explain how the principles of the Bahçeşehir University Artificial Intelligence Policy are translated into institutional decision-making and control mechanisms. The following matters fall outside their scope and are addressed in the relevant supplementary documents:

a) the composition and working arrangements of the Artificial Intelligence Steering Committee;

b) detailed rules governing the use of artificial intelligence by students and staff;

c) conditions of access to a particular product or platform;

d) detailed procedures relating to the processing of personal data;

e) the questions and scoring methods included in the Artificial Intelligence Risk Assessment Form; and

f) the details of periodic and annual review dates.

Circumstances requiring institutional assessment

ARTICLE 3 – (1) An artificial intelligence application shall be subject to institutional assessment under these Procedures and Principles where it meets at least one of the following conditions:

a) it is to be purchased, licensed, or made available for institutional use by the University;

b) it provides services to students, staff, researchers, alumni, or external stakeholders;

c) it uses institutional data, personal data, or information that is not publicly available;

d) it connects to the University's information systems or institutional data sources;

e) it supports an academic, administrative, financial, or managerial decision-making process;

f) it may affect a person's academic status, access to services, employment, or rights;

g) it generates content, recommendations, assessments, notifications, or transactions on behalf of the University;

h) it is made available to a broad user group or to the public;

i) it requires institutional resources, budget, infrastructure, or human resources; or

j) it may affect the University's legal, ethical, security, or reputational responsibilities.

Uses outside the scope

ARTICLE 4 – (1) Applications used by individuals solely for personal purposes, without any connection to University data, institutional identity, official authority, a University account, or institutional resources, are not subject to the institutional application and approval process.

(2) Nevertheless, users remain subject to their obligations arising from personal data protection, academic integrity, intellectual and industrial property, information security, and other applicable regulations.

(3) A separate institutional project assessment is not required for every example of low-risk routine use. Approved-tool requirements, data security, output verification, and human responsibility nevertheless remain applicable to such uses.

PART TWO
Responsible Artificial Intelligence Control Areas

Responsible artificial intelligence control areas

ARTICLE 5 – (1) The principles established in the Bahçeşehir University Artificial Intelligence Policy are implemented in institutional applications through the following control areas:

Policy area	Core control in practice
Human-centred approach	Human oversight, intervention, and ultimate human responsibility
Ethical and responsible use	Definition of a legitimate purpose, necessity, proportionality, and expected benefit
Transparency and explainability	User information, disclosure of artificial intelligence interaction, and traceability of the basis for decisions
Accountability	Designation of the application owner, data owner, technical lead, and decision owner
Fairness, equality, and inclusiveness	Assessment of bias, discrimination, accessibility, and impacts on different user groups
Data security and privacy	Data minimisation, authorisation, and compliance with the Data Protection Procedure
Academic integrity and scientific ethics	Human contribution, source verification, disclosure, and scientific responsibility
Quality assurance	Performance measurement, user feedback, and continuous improvement
Sustainability and societal contribution	Assessment of resource use, institutional benefit, and societal impact

Legitimate purpose, necessity, and proportionality

ARTICLE 6 – (1) A clear and specific purpose aligned with institutional objectives shall be defined for every artificial intelligence application.

(2) Artificial intelligence shall be regarded not as an end in itself but as a tool for meeting an identified need. Consideration shall be given to whether the same outcome can be achieved through a method that processes less data, involves lower risk, or is easier to oversee.

(3) The technical availability of a system does not, in itself, mean that its institutional use is necessary or appropriate.

Human oversight and responsibility

ARTICLE 7 – (1) Ultimate academic, scientific, legal, administrative, and managerial responsibility in artificial intelligence-supported processes rests with human beings.

(2) The person responsible for human oversight shall:

a) understand the purpose and limitations of the system;

b) possess the competence required to assess its output;

c) be able to exercise the authority to reject or modify its output;

d) be able to stop the process where necessary; and

e) assume responsibility for the decisions and outcomes.

(3) Human oversight shall not be limited to the formal approval of artificial intelligence output.

Transparency

ARTICLE 8 – (1) Users shall be informed clearly and understandably when they are interacting with an artificial intelligence-supported system. To the extent appropriate, users shall be informed of:

a) the purpose of the system;

b) the sources on which the information is based;

c) the material limitations of the system;

d) whether the system produces an official decision or opinion;

e) how human support may be accessed; and

f) the requirement not to disclose personal or confidential data.

Personal data protection, data security, and privacy

ARTICLE 9 – (1) The processing of personal data in artificial intelligence applications shall be carried out in accordance with Law No. 6698 on the Protection of Personal Data, the Bahçeşehir University Personal Data Protection and Data Privacy Policy, and the University's relevant information security and data governance regulations.

(2) Personal data used in artificial intelligence applications shall be processed:

a) lawfully and fairly;

b) accurately and, where necessary, kept up to date;

c) for specified, explicit, and legitimate purposes;

d) in a manner that is relevant, limited, and proportionate to the purpose of processing; and

e) retained only for the period required.

(3) Before an artificial intelligence application that processes personal data is placed into use, the following matters shall be assessed in proportion to the application's level of risk:

a) the purpose of processing;

b) the categories of data processed and the groups of data subjects concerned;

c) the legal basis for processing;

d) the source of the data;

e) the access and authorisation structure;

f) retention and deletion conditions;

g) whether data is transferred domestically or internationally;

h) relationships with service providers and other third parties; and

i) the technical and administrative measures to be implemented.

(4) Appropriate technical and administrative measures shall be implemented to protect the confidentiality, integrity, and availability of personal data and confidential or restricted-access institutional data. Access to such data shall be limited according to role and need.

(5) The conditions under which the artificial intelligence tool or service provider retains, transfers, reuses, or uses data for model development, or discloses data to sub-processors, shall be examined through the relevant assessment process before institutional use.

(6) Operational details relating to the processing, transfer, retention, and deletion of personal data, the management of breaches, and third-party service providers shall be governed by the Bahçeşehir University Personal Data Protection and Data Privacy Policy and the relevant data protection procedures.

Fairness, equality, inclusiveness, and accessibility

ARTICLE 10 – (1) The potential effects of artificial intelligence applications on persons and groups with different cultural, social, economic, linguistic, and demographic characteristics shall be assessed in proportion to the nature and level of risk of the application.

(2) Appropriate preventive and corrective controls shall be implemented to ensure that artificial intelligence applications do not create systematic error, discrimination, exclusion, unfair advantage, or disadvantage for particular persons or groups.

(3) The following matters shall be taken into consideration in the design and use of artificial intelligence applications:

a) disability-related and accessibility needs;

b) linguistic differences;

c) differences in access to digital tools and services; and

d) users' levels of technical competence.

(4) Where an artificial intelligence-supported activity places persons at a disadvantage in relation to privacy, accessibility, or equality of opportunity, appropriate human-supported or non-artificial-intelligence alternatives shall be considered.

Accuracy, reliability, and technical robustness

ARTICLE 11 – (1) The outputs of artificial intelligence systems shall not be presumed to be accurate, complete, or current. Outputs shall be reviewed through human assessment, source verification, or other validation methods to the extent required by the purpose and level of risk of the use.

(2) Artificial intelligence applications that provide information about the University shall use sources verified by authorised units and subject to ongoing currency checks.

(3) Artificial intelligence applications shall, where appropriate, be tested using examples representative of the intended conditions of use. Testing shall take into account at least the following risks:

a) incorrect or misleading output;

b) incomplete or outdated information;

c) fabricated information or sources;

d) biased or inconsistent results;

e) unauthorised access or transactions;

f) misuse; and

g) system or integration failure.

(4) For artificial intelligence applications capable of creating, changing, or deleting records in institutional systems, or of transmitting transactions to third parties, permissions shall be limited by role; relevant actions shall be subject to human approval; and transactions shall be recorded to an appropriate extent.

(5) In the event of an error or service interruption, methods for transition to a human-supported process, suspension of the transaction, or restoration to the previous safe state shall be defined in proportion to the level of risk.

Academic integrity, scientific responsibility, and intellectual property rights

ARTICLE 12 – (1) The use of artificial intelligence does not remove the original contribution, professional judgement, or academic or scientific responsibility of the student, academic, researcher, or member of staff.

(2) Artificial intelligence shall not be used to fabricate or use data, sources, citations, findings, evidence, identities, or official records.

(3) Analyses, recommendations, text, code, or other outputs generated by artificial intelligence shall not be used as academic, scientific, administrative, or official output without the required verification and human assessment.

(4) Detailed requirements relating to disclosure of artificial intelligence use, attribution, students' original contribution, and limitations on use in courses are set out in the Student Artificial Intelligence Use Guidelines and the Staff Artificial Intelligence Use Guidelines.

(5) The following matters shall be observed in relation to materials entered into or obtained from artificial intelligence systems:

a) the intellectual and industrial property rights of the University, the user, or third parties;

b) licensing and terms of use;

c) confidentiality obligations; and

d) research, publication, or contractual restrictions.

Quality assurance, institutional benefit, and sustainability

ARTICLE 13 – (1) Artificial intelligence applications shall be monitored and evaluated in line with the University's quality assurance and continuous improvement approach.

(2) The success of an artificial intelligence application shall not be measured solely by the number of users, messages, transactions, items of content, or technical resources consumed. Where appropriate, the following criteria shall be considered together:

a) support for learning and teaching;

b) research and scientific output;

c) service quality;

d) process efficiency;

e) user experience;

f) reduction of errors and risks;

g) resource use;

h) cost and total cost of ownership;

i) maintenance and updating requirements; and

j) societal and institutional benefit.

(3) Applications that do not generate institutional benefit, cannot be kept sufficiently current, do not produce outputs proportionate to their use of resources, or exceed the acceptable level of risk shall be reassessed.

(4) The social, economic, and environmental impacts of artificial intelligence systems shall be assessed in proportion to the scale of the application. Unnecessary data processing and technical resource consumption disproportionate to the purpose of use shall be avoided.

PART THREE
Risk Classification

General principles of risk classification

ARTICLE 14 – (1) Artificial intelligence applications shall be assigned to one of the following risk levels, taking into account the purpose of use, affected persons and groups, the data used, the degree of system autonomy, and potential consequences:

a) Level 1 – Low Risk;

b) Level 2 – Controlled Risk;

c) Level 3 – High Risk; and

d) Level 4 – Unacceptable Use.

(2) The risk level shall be determined on the basis of the specific use case, rather than the commercial name of the tool or technology used. The same tool may be assigned different risk levels for different purposes of use.

(3) Where an application possesses characteristics associated with more than one risk level, the higher risk level shall apply.

(4) The detailed record of risk classification and the measures to be taken shall be maintained through the Artificial Intelligence Risk Assessment Template.

Level 1 – Low Risk

ARTICLE 15 – (1) Low-risk uses generally include applications that:

a) work with publicly available information or information that does not contain personal data;

b) do not make decisions about individuals;

c) do not perform transactions in institutional systems;

d) would not, if erroneous, produce significant academic, legal, financial, or administrative consequences; and

e) produce output that can readily be checked by the user.

(2) Examples of low-risk use may include:

a) idea generation;

b) preparation of an initial draft;

c) summarisation of publicly available text;

d) language and style improvement;

e) code development using sample data that contains no personal data; and

f) preparation of a visual or presentation draft.

(3) A separate full risk assessment is not required for low-risk routine use. Output verification, data security, human responsibility, and the rules in the applicable user guidelines nevertheless apply.

Level 2 – Controlled Risk

ARTICLE 16 – (1) Controlled-risk applications generally include applications that:

a) serve a particular course, unit, or user group;

b) use institutional content or a limited data source;

c) interact directly with students, staff, or external stakeholders;

d) may, if erroneous, have a limited but meaningful effect on a service or learning process; and

e) produce answers or recommendations based on University-approved information sources.

(2) Examples of controlled-risk applications may include:

a) course- or learning-activity-specific teaching assistant applications;

b) unit-level document search and question-and-answer assistants;

c) student-service assistants that do not make decisions about individuals;

d) research or coding support systems; and

e) administrative assistants intended for a limited user group.

(3) Controlled-risk applications shall meet at least the following requirements:

a) designation of an application owner;

b) a preliminary risk assessment;

c) definition of the scope of data and sources;

d) user information;

e) definition of access restrictions;

f) controlled testing or a pilot; and

g) a monitoring and review method.

Level 3 – High Risk

ARTICLE 17 – (1) Artificial intelligence applications shall be classified as high risk where they possess one or more of the following characteristics:

a) processing special categories of personal data or other sensitive data;

b) processing personal data on a large scale or systematically;

c) creating profiles, predictions, classifications, or risk assessments concerning individuals;

d) being capable of affecting students' academic progression, grades, scholarships, disciplinary status, or access to services;

e) being capable of affecting the recruitment, assignment, performance, promotion, or employment relationship of staff;

f) using data relating to health, psychological counselling, or special support needs;

g) predicting student failure, withdrawal, behaviour, or support needs;

h) using biometric data or identity-verification functionality;

i) having the authority to create, modify, delete, or process records in institutional information systems;

j) being capable, if erroneous, of materially affecting the rights of individuals or the University's legal, financial, or reputational position; or

k) producing outputs that are difficult to verify independently or explain.

(2) High-risk applications shall meet at least the following requirements:

a) a full artificial intelligence risk assessment;

b) the required personal data protection and information security reviews;

c) relevant ethical, legal, technical, pedagogical, or academic opinions;

d) documented human oversight;

e) a controlled pilot;

f) user information;

g) a route for appeal and reassessment by a human; and

h) assessment by the Artificial Intelligence Steering Committee.

(3) High-risk applications shall not be placed into production until the required assessments and institutional approvals have been completed.

Level 4 – Unacceptable Use

ARTICLE 18 – (1) The following uses are not permitted within Bahçeşehir University:

a) delegating entirely to an artificial intelligence system final decisions that materially affect individuals, including decisions on grades, admission, scholarships, discipline, recruitment, performance, promotion, or termination of employment;

b) creating general scores concerning the trustworthiness, value, suitability, or behaviour of individuals;

c) inferring, without authorisation, the emotions, personality, or sensitive characteristics of individuals in educational or working environments and using such inferences in decision-making;

d) unauthorised biometric monitoring or mass surveillance;

e) directing the behaviour of individuals by exploiting their age, disability, lack of information, or other vulnerabilities;

f) processing personal, confidential, or non-public institutional data through artificial intelligence systems without the required assessment and authorisation;

g) using artificial intelligence to fabricate data, sources, citations, evidence, identities, or official records;

h) using artificial intelligence to circumvent security controls or access permissions; and

i) decision-making processes in which human oversight is merely nominal and artificial intelligence output is applied without scrutiny.

(2) The examination of a technology involving an unacceptable use solely for research purposes may be assessed separately, provided that it is not used on real persons, appropriate data is used, and all required ethical, legal, and security approvals are obtained.

PART FOUR
Artificial Intelligence Application Life Cycle

Identification of need and ownership

ARTICLE 19 – (1) The following shall be determined for an institutional artificial intelligence application:

a) the need to be addressed;

b) the purpose of use;

c) the target user group;

d) the expected institutional benefit;

e) the application owner; and

f) success criteria.

(2) Consideration shall be given to whether the same need can be met through a lower-risk method that processes less data or is easier to oversee.

Preliminary notification and risk classification

ARTICLE 20 – (1) Controlled- and high-risk applications that are planned to be purchased, developed, made available for institutional use, or integrated into systems by the University shall be notified to the Artificial Intelligence Competency Unit.

(2) A preliminary review and risk classification shall be carried out on the basis of the purpose of use, data scope, degree of system autonomy, target users, and potential impacts.

(3) Controlled- and high-risk applications shall be entered into the institutional artificial intelligence inventory from the assessment stage onwards.

Assessment and decision

ARTICLE 21 – (1) Depending on the nature and risk level of the application, the following processes shall be applied:

a) the Artificial Intelligence Risk Assessment Template;

b) data protection and information security assessment;

c) ethical or academic assessment;

d) pedagogical and assessment review;

e) intellectual and industrial property review; and

f) supplier, contract, and access assessment.

(2) The assessment shall result in one of the following decisions:

a) suitable for use;

b) suitable for use subject to specified conditions;

c) suitable for a pilot;

d) additional information or revision required;

e) temporarily unsuitable; or

f) unsuitable for use.

(3) The decision shall identify the application owner, scope of use, required controls, data and user boundaries, monitoring method, and review date.

Pilot and deployment

ARTICLE 22 – (1) Controlled- and high-risk applications shall, to the extent possible, be piloted with a limited user group, data scope, and functionality.

(2) In addition to technical performance, the pilot shall monitor accuracy, misleading output, bias, user experience, human intervention, data use, security, and unintended effects.

(3) An application may be deployed for institutional use only where:

a) responsible persons have been designated;

b) the risk level has been determined;

c) the required assessments and approvals have been completed;

d) data and access boundaries have been defined;

e) human oversight has been established;

f) user information has been prepared; and

g) monitoring and suspension methods have been defined.

Monitoring and material changes

ARTICLE 23 – (1) Artificial intelligence applications placed into use shall be monitored in proportion to their risk levels.

(2) The risk classification and previous approval of an application shall be reassessed where any of the following changes occurs:

a) a change in the purpose of use;

b) extension to a new user group;

c) addition of a new or more sensitive data source;

d) a change of model or service provider;

e) integration with an institutional system;

f) granting the system new transactional or decision-making authority;

g) a material increase in the scale of use; or

h) a material change in security, performance, or contractual conditions.

Suspension and termination

ARTICLE 24 – (1) An artificial intelligence application may be temporarily suspended, restructured, or terminated where one or more of the following circumstances applies:

a) it creates an unacceptable risk;

b) it does not fulfil its intended purpose;

c) it persistently produces erroneous or discriminatory results;

d) it causes a data security or privacy breach;

e) it cannot be kept sufficiently current;

f) its institutional benefit does not justify its use of resources; or

g) the service provider or contractual conditions cease to be appropriate.

(2) During termination, data, user access, system integrations, records, content ownership, and third-party service relationships shall be closed in a controlled manner.

PART FIVE
Minimum Controls and Decision-Making Structure

Minimum controls by risk level

ARTICLE 25 – (1) The controls in the following table are minimum requirements. Additional controls or approval processes may be applied depending on the nature of the application, the data used, and applicable legislation.

Control	Low Risk	Controlled Risk	High Risk
Definition of purpose of use	Required	Required	Required
Designation of application owner	User or unit responsibility	Mandatory	Mandatory
Institutional inventory record	Where required	Mandatory	Mandatory
Preliminary risk review	General rules of use	Mandatory	Mandatory
Full risk assessment	Not required	Where required	Mandatory
Personal data protection, data security, and privacy	Reclassified if data is processed	According to the use case	Mandatory
Information security review	Where integrated	According to the use case	Mandatory

Control	Low Risk	Controlled Risk	High Risk
User information	Where required	Mandatory	Mandatory
Human oversight	User control	Clearly defined	Documented
Pilot	Optional	Required as a general rule	Mandatory
Opinion of specialist unit	Where required	According to the use case	Mandatory
Committee assessment	Not required	Where required	Mandatory
Periodic review	General calendar	At least once per term	More frequently in proportion to risk
Appeal and reassessment route	Not normally required	According to impact	Mandatory
Termination method	Where required	Required	Mandatory

Application owner

ARTICLE 26 – (1) An application owner shall be designated for every controlled- or high-risk application.

(2) The application owner is responsible for:

a) defining the purpose and scope of use;

b) providing the information required for risk assessment;

c) implementing the approved controls and limitations;

d) ensuring human oversight;

e) monitoring use and performance; and

f) reporting material changes, errors, or incidents.

Artificial Intelligence Competency Unit

ARTICLE 27 – (1) The Artificial Intelligence Competency Unit shall:

a) coordinate the application and preliminary review process;

b) support risk classification;

c) ensure that relevant specialist opinions are obtained;

d) maintain the institutional artificial intelligence inventory;

e) monitor risk assessment and review records; and

f) prepare high-risk or strategic applications for the agenda of the Committee.

(2) The Artificial Intelligence Competency Unit shall not, acting alone, grant final approval in matters falling within the remit of another board, committee, or unit.

Specialist units

ARTICLE 28 – (1) Depending on the nature of the application, relevant academic and administrative units shall conduct assessments and provide opinions in the following areas:

a) personal data protection;

b) information security and technical architecture;

c) legal compliance and contracts;

d) ethics and academic integrity;

e) education and assessment;

f) intellectual and industrial property;

g) procurement, access, and licensing; and

h) accessibility.

Artificial Intelligence Steering Committee

ARTICLE 29 – (1) The Artificial Intelligence Steering Committee shall assess:

a) high-risk applications;

b) applications that affect more than one unit or a broad user population;

c) strategic institutional investments;

d) applications involving material ethical, legal, security, or reputational risk; and

e) applications for which there is disagreement concerning the risk level or the decision to continue.

(2) The composition, duties, working arrangements, and decision-making processes of the Committee are governed by the Bahçeşehir University Artificial Intelligence Steering Committee Procedures and Principles.

Authorised boards and authorities

ARTICLE 30 – (1) Where the applicable legislation or University regulations require a decision by the Senate, Rectorate, an ethics board, a disciplinary body, a procurement authority, or another authorised board, an assessment conducted under these Procedures and Principles shall not replace that decision.

PART SIX
Related Documents and Records

Supplementary documents

ARTICLE 31 – (1) These Procedures and Principles shall be applied together with the following documents:

Document	Area governed
Bahçeşehir University Artificial Intelligence Policy	High-level institutional approach and principles
Bahçeşehir University Personal Data Protection and Data Privacy Policy	High-level institutional approach and principles
Artificial Intelligence Steering Committee Procedures and Principles	Governance, duties, and decision-making structure
Student Artificial Intelligence Use Guidelines	Rules governing student use and academic integrity
Staff Artificial Intelligence Use Guidelines	Responsibilities of academic and administrative staff
Artificial Intelligence Data Protection Procedure	Operational data-protection processes for artificial intelligence applications
Artificial Intelligence Risk Assessment Template	Application-specific record of risk, controls, and approval
Artificial Intelligence Review Calendar	Monthly, term-based, and annual monitoring activities

Institutional records

ARTICLE 32 – (1) The following records shall be maintained for controlled- and high-risk applications in proportion to their level of risk:

a) the name and purpose of the application;

b) the application owner;

c) the target user group;

d) the risk level;

e) the types of data and sources used;

f) the method of human oversight;

g) assessments conducted and opinions obtained;

h) the approval or decision;

i) pilot results;

j) use and performance indicators;

k) material changes;

l) incidents and corrective actions;

m) the review date; and

n) the status of continuation, revision, suspension, or termination.

PART SEVEN
Monitoring and Final Provisions

Monitoring and review

ARTICLE 33 – (1) The implementation of these Procedures and Principles shall be monitored through the following sources:

a) the institutional artificial intelligence inventory;

b) risk assessment records;

c) application and project reports;

d) user feedback;

e) error, complaint, and incident records;

f) training and competency data; and

g) institutional performance indicators.

(2) The frequency, responsible parties, and outputs of monitoring activities shall be specified in the Artificial Intelligence Review Calendar.

(3) These Procedures and Principles shall be reviewed at least annually, taking into account technological developments, changes in legislation, implementation experience, risk and incident records, user feedback, and changes to the Artificial Intelligence Policy and Roadmap.

Relationship with other regulations

ARTICLE 34 – (1) These Procedures and Principles shall be applied together with the University's regulations concerning academic integrity, research and publication ethics, personal data protection, information security, intellectual and industrial property, teaching and learning, students, staff, quality assurance, procurement, and institutional risk management.

(2) These Procedures and Principles do not remove the existing duties, powers, and responsibilities of other boards, committees, units, or authorised authorities.

(3) Where a difference of interpretation arises between these Procedures and Principles and another University regulation, applicable legislation, Senate decisions, and higher-level University policies shall prevail.

Matters not provided for

ARTICLE 35 – (1) In matters not provided for in these Procedures and Principles, the following shall apply:

a) applicable national legislation;

b) the Bahçeşehir University Artificial Intelligence Policy;

c) the Bahçeşehir University Personal Data Protection and Data Privacy Policy;

d) the University's relevant policies, directives, procedures and principles, operational procedures, and decisions;

e) decisions of the Senate and the University Executive Board; and

f) decisions and instructions of the Rectorate.

(2) The Rector is authorised to resolve any uncertainty arising in the implementation of these Procedures and Principles.

Entry into force

ARTICLE 36 – (1) These Procedures and Principles shall enter into force on the date of their adoption by the Bahçeşehir University Senate.

Execution

ARTICLE 37 – (1) The provisions of these Procedures and Principles shall be executed by the Rector of Bahçeşehir University.