

KURUMSAL YZ KULLANIM REHBERİ

Yalnızca yasaklamakla yetinmeyin. Güvenli kullanım çerçevesi oluşturun.

Kurumsal yapay zekâ kullanım rehberi

Çalışan ve geliştiricilerin yapay zekâ (YZ) araçlarını iş hedefleri doğrultusunda, veri güvenliği ve kurumsal sorumluluk sınırları içinde kullanması için kısa ve uygulanabilir ilkeler.

KULLANICI**GELİŞTİRİCİ****GÜVENLİK & BT****SOFTBYT LABS ÜRÜN AİLESİ • KULLANIM REHBERİ**

KURUMSAL YZ KULLANIM REHBERİ

Beş temel ilke

Güvenli YZ kullanımı yalnızca teknoloji değil; doğru davranış, yetki ve doğrulama disiplindir.



KURUMSAL YZ KULLANIM REHBERİ

Günlük kullanım kontrol listesi

Günlük iş akışına uyarlanabilecek dört pratik kontrol.



İstem yazarken

Hassas veriyi ayıklayın; yalnız gerekli bağlamı verin; kurumun izin verdiği aracı kullanın.



Dosya paylaşıırken

Sınıflandırmayı kontrol edin; yalnız gerekli bölümü paylaşın; gizli anahtar ve kimlik bilgisi göndermeyin.



YZ ajanı çalıştırırken

Çalışma alanını daraltın; araç ve kaynak izinlerini sınırlayın; yapılan değişiklikleri gözden geçirin.



MCP / eklenti kullanırken

Yalnız onaylı sunucu ve eklentileri kullanın; gereksiz izinleri vermeyin; şüpheli talimatı durdurun.

KRİTİK UYARILAR

Parola / API anahtarı

Ham personel verisi

Müşteri sırrı

Yayımlanmamış ticari plan

KURUMSAL YZ KULLANIM REHBERİ

Kime ne düşüyor?

Politika, kullanıcı davranışı ve teknik kontrol birlikte çalıştığında sürdürülebilir güvenlik oluşur.

Çalışanlar

- Onaylı araçları kullanır.
- Minimum veri ilkesiyle hareket eder.
- YZ çıktısını doğrular ve şüpheli olayı bildirir.

Geliştiriciler

- Çalışma alanı ve araç izinlerini sınırlar.
- Kod ve dosya değişikliklerini incelemekten kabul etmez.
- Kurumsal sırları istem veya eklenti akışına taşımaz.

Güvenlik & BT

- YZ envanteri ve politika çerçevesini yönetir.
- Pilot ve eğitim programını yürütür.
- Olayları izler, ölçer ve kuralları günceller.

1

Keşfet

Kullanılan araçları ve kullanım biçimlerini görün.

2

Kuralı Belirle

Veri sınıfları ve kullanım senaryoları için sınırları tanımlayın.

3

Pilotla

Seçili ekiplerde kontrol ve eğitim modelini doğrulayın.

4

İyileştir

Olay, geri bildirim ve kullanım verisiyle politikayı güncelleyin.