SoruMind QA Yol Haritası

Projemizin temelinde, LGS gibi **eğitim verileri** yer alacağı için bilgi güvenliğini en başından garanti altına almak **bizim ortak sorumluluğumuzdur**. Bu nedenle, ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS) standartlarını kılavuz alarak bir yol haritası çıkardım.

---

1. Kapsam ve Risk Yönetimi

Bu aşama, halihazırda yaptığımız analiz çalışmalarını güvenlik perspektifiyle derinleştiriyor.

- **Kapsam Belirleme:** BGYS'nin sadece yapay zekâ modelini değil; **veri toplama, anonimleştirme, güvenli depolama ve sonuçların kullanıcıya sunulması** gibi tüm süreçleri kapsayacak şekilde sınırlarını netleştirdik.
- **Varlıkların Belirlenmesi:** Korunması gereken en kritik varlıklarımızı listeledim. Bunlar:
    - **Veri Varlıkları:** Topladığımız LGS/eğitim verileri, öğrenci performans metrikleri ve oluşturduğumuz **tahmin modelleri**.
    - **Yazılım Varlıkları:** Yapay zekâ kodumuz, test araçlarımız ve kuracağımız loglama sistemi.
- **Risk Değerlendirmesi:** Bir QA gözüyle, bu varlıklara yönelik olası tehditleri (veri sızıntısı, modelin çalınması, algoritma manipülasyonu) belirledim.

---

2. Uygulanması Gereken Kritik Kontroller (Ek-A)

ISO 27001'in Ek-A bölümündeki kontrolleri inceleyerek, projemizin başlangıç aşamasında **kod yazılmadan** uygulamamız gereken temel güvenlik adımlarını belirledim:

A. Organizasyonel Güvenlik ve Politika

- **Bilgi Güvenliği Politikası:** Bu politika, verilerin nerede saklanacağı ve kimlerin erişebileceği gibi temel kuralları içerecek.
- **Görevlerin Ayrılığı: Test rolümüzün bağımsızlığı**, güvenlik ve kaliteyi sağlama açısından kritik önem taşıyor.

B. İnsan Kaynakları ve Erişim Kontrolü

- **Farkındalık ve Eğitim:** Ekip üyelerimizi, özellikle eğitim verilerinin **gizliliği** ve KVKK/GDPR benzeri uyum gereklilikleri konusunda bilgilendireceğim.

C. Geliştirme ve Test Süreci Güvenliği

- **Güvenli Kodlama Prensipleri:** Geliştiricilerimiz için temel **güvenli kodlama standartlarını** (örneğin giriş doğrulama ve veri filtreleme) belirleyerek, yazılım zafiyetlerini daha oluşmadan önlemeyi hedefliyorum.

3. QA Rolünün Güvenliğe Kritik Katkısı

Benim QA Engineer olarak görevim, ISO 27001 süreçlerinin sadece kural olarak kalmamasını, **uygulanmasını** sağlamaktır.

- **Test Planına Güvenlik Ekleme:** Hazırlayacağımız test planı sadece uygulamanın beklendiği gibi çalışıp çalışmadığını değil, aynı zamanda belirlenen **güvenlik kontrollerine** uyup uymadığını da denetleyecek (örneğin yetkisiz erişim denemeleri, veri bütünlüğü testleri).
- **Loglama Sisteminin Kontrolü:** Kurulacak loglama sisteminin, sadece fonksiyonel hataları değil, aynı zamanda **tüm güvenlik olaylarını** (başarısız girişler, yetki değişiklikleri) da doğru bir şekilde kayıt altına aldığını **test edeceğim**.
- **BGYS Performans Ölçümü:** Projemizdeki güvenlik ihlali sayısı ve tespit edilen zayıf yön sayısı gibi metrikleri izleyerek BGYS'nin ne kadar etkili çalıştığını ölçmeye katkıda bulunacağım.

Bu adımlar, projemizin temelden güvenli, sürdürülebilir ve kurumsal standartlara uygun bir yapıya sahip olmasını amaçlamaktadır.