LLM Security Guidelines - Enterprise AI Systems

Security Framework Overview

Enterprise AI applications require comprehensive security measures to protect sensitive data and ensure compliance with regulatory requirements. This document outlines security best practices for LLM-based systems.

Data Protection
• Encrypt all data in transit and at rest
• Implement proper access controls and authentication
• Use Azure Key Vault for credential management
• Regular security audits and penetration testing

Model Security
• Input validation and sanitization
• Prompt injection prevention
• Output filtering and content moderation
• Model version control and integrity verification

Compliance Requirements
• SOC 2 Type II certification
• GDPR compliance for EU data
• HIPAA compliance for healthcare data
• Regular compliance assessments and reporting