GIẢI PHÁP BẢO MẬT DỮ LIỆU KHI GỬI VÀ NHẬN ĐỐI VỚI MÔ HÌNH AI

## 1. Mã hóa dữ liệu đầu vào (trước khi gửi đến API Model AI)

* Mục tiêu: Ngăn chặn dữ liệu nhạy cảm bị lộ nếu request bị đánh cắp trước khi tới Model AI.
* Giải pháp:
* Áp dụng tokenization hoặc masking (ẩn các thông tin nhạy cảm như số CMND, email, mã khách hàng).
* Chỉ áp dụng mã hóa bất đối xứng (RSA/AES) đối với những nội dung cần lưu trữ an toàn, **không dùng thể mã hóa toàn bộ nội dung gửi đến Model AI**, vì mô hình không thể hiểu nội dung đã mã hóa.
* Với những thông tin không thể mã hóa (vì cần mô hình hiểu rõ), nên rút gọn và chuyển thành mã hóa theo ngữ nghĩa (semantic code).
* Chỉ truyền tải những thông tin thực sự cần thiết cho quá trình phân tích của AI, tránh gửi toàn bộ dữ liệu thô hoặc không liên quan.
* Phân quyền dữ liệu hỏi đáp với AI (quyền hỏi dữ liệu nội bộ và quyền hỏi dữ liệu ngoài internet).
* Phân quyền dữ liệu truy cập dữ liệu trong hệ thống theo vai trò của người dùng.

## 2. Sử dụng HTTPS/TLS để bảo vệ dữ liệu truyền tải

* Mục tiêu: Đảm bảo toàn bộ luồng request/response với Model AI được mã hóa mạng.
* Giải pháp:
* Đảm bảo mọi request đến domain của Model AI sử dụng giao thức HTTPS với TLS 1.2+.
* Nếu dùng proxy, cần xác minh proxy hỗ trợ HTTPS và không can thiệp nội dung.

## 3. Mã hóa dữ liệu đầu ra (kết quả từ Model AI trả về)

* Mục tiêu: Nếu phản hồi có thông tin nội bộ, cần được mã hóa trước khi lưu.
* Giải pháp:
* Sử dụng AES-256 để mã hóa nội dung trả về trước khi ghi vào DB.
* Kết hợp giải mã chỉ tại UI (client-side decrypt nếu bảo mật đủ).
* Tích hợp giải pháp Data Loss Prevention (DLP) để lọc đầu ra nếu cần.

## 4. Quản lý khóa và bảo mật khóa mã hóa

* Mục tiêu: Tránh rò rỉ các khóa mã hóa (key) trong code hoặc cấu hình.
* Giải pháp:
* Mã hóa APIKey khi lưu ở Database
* Không lưu khóa trong mã nguồn, Git, cấu hình appsettings.
* Giao tiếp mã hóa thông qua thư viện hỗ trợ chính thức như Microsoft.AspNetCore.DataProtection.

## 5. Thiết lập giới hạn quyền truy cập và token bảo mật

* Mục tiêu: Bảo vệ API Key của Model AI và giới hạn truy cập API.
* Giải pháp:
* Lưu API Key trong biến môi trường hoặc secret manager, không hardcode.
* Dùng Role-Based Access Control (RBAC) để giới hạn người dùng được gọi API.