Universal AI Agent Platform DOC-ID: UAA-VI-2026-V3

Cẩm nang Giải pháp, Kiến trúc Bảo mật & Hướng dẫn Cấu hình Universal AI Agent

Không sửa đổi hệ thống cũ — Kết nối trực tiếp CSDL doanh nghiệp an toàn chuẩn MCP chỉ từ 3 ngày

APPI / Zero Data Retention

MCP Read-Only Protocol

01. TÓM TẮT GIẢI PHÁP & HIỆU QUẢ ĐẦU TƯ (ROI)

Universal AI Agent kết nối trực tiếp ở chế độ Chỉ đọc (Read-Only) với CSDL hiện có (SQL Server, PostgreSQL, MySQL, SQLite), giúp tự động hóa tư vấn bán hàng 24/7 kèm thẻ sản phẩm trực quan và phân tích dữ liệu điều hành tức thì trên một nền tảng duy nhất.

Tỷ lệ tự động xử lý hội thoại

80%

Hợp nhất Web Widget + Facebook Messenger

Thời gian nhân viên soạn phản hồi

-70%

AI Copilot gợi ý sẵn câu trả lời nháp

Thời gian kết nối kiểm chứng PoC

Từ 3 ngày

Chi phí khởi tạo 0đ • Không sửa API cũ

02. SƠ ĐỒ KIẾN TRÚC KẾT NỐI & BẢO VỆ 2 TẦNG

FLOW 01 Đa kênh & Xác thực

Khách hàng / Quản lý

Đặt câu hỏi tự nhiên qua Web Widget (đọc Cookie tự động) hoặc FB Messenger.

FLOW 02 Lá chắn 1 • Phản tư

Regex Gate + LangGraph

Chặn từ khóa nguy hiểm, tra Từ điển Nghiệp vụ & tự sửa lỗi SQL (Reflection).

FLOW 03 Lá chắn 2 • RLS

SQL AST & Cô lập RLS

Cây cú pháp AST chỉ cho phép lệnh SELECT; gắn khóa phân quyền theo vai trò.

FLOW 04 TLS 1.3 Trực tiếp

CSDL Doanh nghiệp

Truy vấn Read-Only trực tiếp, không sao chép dữ liệu ra ngoài (Zero Retention).

SECURITY 01 **Lá chắn CSDL 2 Tầng & Kết nối 100% Read-Only**

Kết hợp bộ lọc Regex tốc độ cao và trình phân tích cú pháp SQL AST nhằm chặn 100% các lệnh làm thay đổi dữ liệu (INSERT, UPDATE, DELETE, DROP) trước khi chạm tới CSDL.

SECURITY 02 **Phân quyền Dòng (RLS), Đồng bộ Vai trò & Zero Retention**

Tự động đồng bộ bảng phân quyền (role_table) và khóa User Scoping để cô lập dữ liệu và điều chỉnh văn phong theo vai trò. Không dùng dữ liệu doanh nghiệp để huấn luyện AI.

ENGINE 03 **Vòng lặp Tự sửa lỗi (LangGraph) & Thẻ UI Sinh động**

AI tự kiểm tra chéo câu lệnh SQL và kết quả truy vấn để chống ảo giác (hallucination), tự động hiển thị thẻ sản phẩm kèm hình ảnh, tồn kho và bảng tổng hợp KPI.

STUDIO 04 **4 Engine AI Auto-Detect & Từ điển Nghiệp vụ**

Tự động phát hiện bảng nối ảnh (Image JOIN), Vai trò, User Scoping và Quyền truy cập bảng chỉ với 1 cú nhấp chuột, kết hợp Từ điển Nghiệp vụ và màn hình Live Preview.

03. HƯỚNG DẪN GIAO DIỆN QUẢN TRỊ KHÔNG CẦN CODE (3 MÀN HÌNH)

Nhân sự nghiệp vụ hoặc IT đều có thể dễ dàng thiết lập và vận hành qua 3 màn hình trực quan:

SCREEN 01 **Wizard Kết nối CSDL & AI Gợi ý Bảng dữ liệu** — Kết nối Read-Only OK (18ms)

- Chọn loại CSDL (PostgreSQL / SQL Server / MySQL / SQLite) và kiểm tra kết nối
- AI tự động đánh dấu gợi ý các bảng nghiệp vụ chính (products, orders...)
- Tích chọn ẩn các bảng hoặc cột nhạy cảm (mật khẩu, giá vốn) chỉ với 1 chạm

```
Bảng dữ liệu: ☑ products ☑ orders ☐ admin_secrets (Đã ẩn)
```

SCREEN 02 **4 Nút AI Auto-Detect & Từ điển Nghiệp vụ** — Đã tự động cấu hình AI

- 1 chạm để AI tự phát hiện cột nối ảnh (Image JOIN), bảng Role và khóa User RLS
- Định nghĩa tên cột viết tắt sang ngôn ngữ kinh doanh (Từ điển Nghiệp vụ)
- Thiết lập giọng điệu phản hồi (Persona) riêng cho Quản lý và CSKH

```
Từ điển: orders.total_amt → "Tổng doanh thu (Đã gồm VAT)"
```

SCREEN 03 **Kiểm thử Live Playground & Nhúng 1 Dòng Mã** — Sẵn sàng vận hành

- Chat thử nghiệm ngay trên Dashboard để kiểm tra SQL và thẻ sản phẩm
- Bật tính năng tự động đọc Cookie khách hàng hoặc Form thu thập thông tin
- Copy 1 dòng thẻ <script> dán vào website để kích hoạt trong 30 giây

```
<script src="https://.../widget.js" data-id="ag_jp01" async></script>
```

04. THÔNG SỐ KỸ THUẬT & MÔI TRƯỜNG HỖ TRỢ

Hệ CSDL hỗ trợ	Microsoft SQL Server / PostgreSQL / MySQL / SQLite (Kết nối 100% Read-Only)
Giao thức & Hạ tầng	Chuẩn Model Context Protocol (MCP) / Hỗ trợ Cloud (AWS, Azure, GCP) & On-Premise VPN
Kênh giao tiếp & Hộp thư	Web Widget (nhúng 1 dòng script) + Facebook Messenger (Hộp thư hợp nhất Unified Inbox)
Xác thực & Form trước Chat	Tự động đọc Token khách hàng từ Cookie / LocalStorage & Form thu thập thông tin tùy chỉnh
Bảo mật & Pháp lý	Tuân thủ chuẩn APPI Nhật Bản / Khung ISO/IEC 27001 (ISMS) / Mã hóa TLS 1.3 & AES-256 / Nhật ký kiểm toán

05. LỘ TRÌNH TRIỂN KHAI KIỂM CHỨNG POC MIỄN PHÍ

STEP 01 — Ngày 1

Xác định phạm vi (30p)

Thống nhất loại CSDL và bài toán tư vấn/phân tích cần tự động hóa (Hỗ trợ ký NDA).

STEP 02 — Ngày 2

Wizard nối DB (0.5 ngày)

Kết nối tài khoản Read-Only, AI gợi ý bảng và đồng bộ Từ điển Nghiệp vụ chuẩn MCP.

STEP 03 — Ngày 3+

Cấu hình & Live Preview

Kiểm thử Persona, quy tắc nghiệp vụ, thẻ Image JOIN và phân quyền RLS trên dữ liệu thật.

STEP 04 — 30 giây

Nhúng 1 dòng mã & Vận hành

Dán 1 dòng <script> lên website để kích hoạt cùng tính năng Handoff & AI Copilot.

06. THÔNG TIN PHÁP NHÂN PHÁT TRIỂN & VẬN HÀNH

Đơn vị vận hành	BK HIGHTECH Co., LTD
Năm thành lập	2022
Đồng sáng lập	TS. Đặng Hoài Phương, Nguyễn Tân, Nguyễn Dung
Cố vấn R&D	TS. Đặng Thiên Bình (Hợp tác nghiên cứu ứng dụng cùng Trường Đại học Bách Khoa - Đại học Đà Nẵng / DUT)
Trụ sở chính	K96/17 Hải Hồ, Quận Hải Châu, TP. Đà Nẵng, Việt Nam
Liên hệ & Website	+84 816 946 355 / contact@bkhightech.vn / https://bkhightech.vn

© 2026 BK HIGHTECH Co., LTD. All rights reserved. — Universal AI Agent Platform (DOC-ID: UAA-VI-2026-V3)