# ปลอดภัยตั้งแต่การออกแบบ

SECURE BY DESIGN — REVIEWED 2026-06-03

เงินของผู้ให้ทิป**ไม่เคยผ่านมือ Tipjai** เราเป็นเครื่องมือสร้าง QR และแจ้งเตือนเท่านั้น เอกสารนี้สรุปการควบคุมความปลอดภัยที่เราใช้จริง ไม่มีกระเป๋ารวมให้ตกเป็นเป้า

## CONTROLS การควบคุมที่ใช้จริง

01 **ไม่ถือเงิน (non-custodial)**
เงินวิ่งจากผู้ให้ทิปถึงครีเอเตอร์โดยตรง

02 **Row-Level Security ทุกตาราง**
ผู้ใช้เข้าถึงได้เฉพาะข้อมูลของตัวเอง

03 **ชำระเงินยืนยันได้ กันซ้ำ**
ตรวจลายเซ็น webhook + idempotent + กันสลิปซ้ำ

04 **จำกัดอัตราการเรียก**
ต่อ IP และต่อผู้ใช้ กันยิงถล่มและเผาโควต้า

05 **CSP + security headers**
HSTS, same-origin framing, ครบชุด

06 **ความลับไม่ถึงเบราว์เซอร์**
secret อยู่ฝั่งเซิร์ฟเวอร์ ไม่เก็บเลขบัตร/รหัสผ่าน

07 **กันสคริปต์ฝังในข้อความ**
escape + sanitize ก่อนแสดงผลและขึ้น overlay

08 **ล็อกอินไม่มีรหัสผ่าน**
อีเมลลิงก์, OTP, Google และ Discord

09 **ความเป็นส่วนตัวตาม PDPA**
เก็บเท่าที่จำเป็น เข้าถึง/แก้/ลบได้

## METHODOLOGY / วิธีตรวจสอบ

ตรวจสอบความปลอดภัยภายในแบบหลายมิติ ครอบคลุมการยืนยันตัวตน การชำระเงินและ webhook การฝังสคริปต์และ CSP การรั่วของความลับ การใช้งานในทางที่ผิด และ Row-Level Security ข้อค้นพบถูกแก้ไขครบและตรวจทานต่อเนื่อง

หมายเหตุตามจริง เป็นการตรวจสอบภายในที่เป็นระบบ ไม่ใช่การรับรองจากองค์กรภายนอก เราไม่กล่าวอ้างตราที่ไม่ได้รับจริง

**พบช่องโหว่? ช่วยรายงานเราได้**
รายงานแบบส่วนตัว เราไม่ดำเนินคดีกับผู้รายงานเจตนาดี และยินดีให้เครดิต

tipjai.com
/security