

Checklist for Securing AI-to-App Communication

Inbound to AI

- ☐ Validate incoming prompts on the server side before forwarding to AI.
- ☐ Limit user-generated prompt length and complexity.
- ☐ Implement guardrails to block unsafe or malformed prompts.

Outbound from AI

- ☐ Check for hallucinations or unexpected responses.
- ☐ Wrap all AI responses in a content validation layer before UI display or database insertion.
- ☐ Quarantine and alert on anomalous AI outputs (e.g., customer data leaks).