# Security Checklist for AI-Integrated Applications

## Infrastructure & Access

- [ ] Use HTTPS/TLS for all AI API traffic.
- [ ] Enforce authentication and rate limits on AI endpoints.
- [ ] Keep AI secrets/API keys in secure vaults (e.g., HashiCorp Vault, AWS Secrets Manager).

## Prompt & Response Handling

- [ ] Sanitize user input before forming prompts.
- [ ] Use system prompts (aka AI stored procedures) to limit AI behavior.
- [ ] Validate AI output before using it in your app.
- [ ] Log AI interactions for observability and security review.

## Data & Privacy

- [ ] Do not pass personally identifiable information (PII) to AI unless strictly necessary.
- [ ] Mask or redact sensitive content in user input/output.
- [ ] Add warnings or disclaimers for users where AI is used in decision-making.

## Testing & Hardening

- [ ] Perform prompt injection tests (simulate malicious prompts).
- [ ] Create a denylist and allowlist of prompt intents.
- [ ] Monitor for AI misuse or unexpected outputs.

## Policy

- [ ] Align AI use with your organizations security and data handling policies.
- [ ] Include an AI security review in your SDLC (Software Development Life Cycle).
- [ ] Document your prompt design, system boundaries, and threat model.