Apples AI Security One-Pager

Status note: Apples is applying to the OpenAI Partner Network and Anthropic partner ecosystem. Apples is not currently representing itself as an approved OpenAI or Anthropic partner.

Principles

- Least-privilege access for connected accounts and APIs
- Data minimization by workflow scope
- Human approval for high-impact actions
- No public exposure of credentials, private files, or raw infrastructure details

AI controls

- AI can draft, classify, summarize, extract, and recommend
- Outbound messaging, payments, customer commitments, and sensitive changes require approved controls
- AI voice or chat experiences include disclosure where applicable

Operational controls

- Logs for automated runs and failed actions
- Rollback path for production deployments
- Monitoring for workflow errors and integration failures
- Customer-specific access separated by workspace

Review boundary

Security controls are tailored per implementation based on data access, compliance risk, and connected systems.