AI Security Posture Overview / ■■■■ Security Posture ■■■■■■■■■■■ /

Best-practice controls overview (not certification claims)

Disclaimer: This document is a practical template and does not constitute legal, compliance, or financial advice. | ■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■ ■■■■■■■■■■■■■■■■■■■■■■■/■■■■■■■

Scope / ■■■■■■: Controls you can implement for AI services and data pipelines.

Controls / ■■■■■■■:

- Identity & access: least privilege, MFA where possible
- Secrets: vault/secret manager, rotation, no secrets in code
- Data security: encryption in transit/at rest, access logs
- Network: segmentation, allow-lists for critical services
- App security: input validation, dependency scanning, SBOM if possible
- Observability: structured logs, metrics, tracing, audit trails
- Incident response: runbooks, roles, postmortems

Evidence checklist / ■■■■■■■■■■■■■■■■:

- Access reviews, change logs, incident records, backup/restore tests

AI Security Posture Overview / ■■■■ Security Posture ■■■■■■■■■ A

Best-practice controls overview (not certification claims)

Notes / ■■■■■■■■:

AI Security Posture Overview / ■■■■ Security Posture ■■■■■■■■■ A

Best-practice controls overview (not certification claims)

Notes / ■■■■■■■■:

AI Security Posture Overview / ■■■■ Security Posture ■■■■■■■■■ A

Best-practice controls overview (not certification claims)

Notes / ■■■■■■■■:

AI Security Posture Overview / ■■■■ Security Posture ■■■■■■■■■ A

Best-practice controls overview (not certification claims)

Notes / ■■■■■■■■:

AI Security Posture Overview / ■■■■ Security Posture ■■■■■■■■■■ A

Best-practice controls overview (not certification claims)

Notes / ■■■■■■■■: