MCP integration

Review the permissions and controls behind each business-system action.

Identity / Permissions / Action

Project / owner _____ Review date _____

Contract And Identity

- [ ] Define specific read and write operations and their input schemas.
- [ ] Document the chosen MCP version, transport, and authentication arrangement.
- [ ] Establish user identity from authentication, not model-provided identifiers.
- [ ] Enforce record-level authorization on every operation.
- [ ] Keep credentials server-side and document rotation and revocation.

Reads

- [ ] Return only information needed for the permitted task.
- [ ] Treat retrieved text as untrusted data, not a source of new permissions.
- [ ] Test cross-account record requests and prompt-injection attempts.
- [ ] Define redaction and error messages that do not expose protected records.

Scope decisions

Illustrative planning resource, not a complete security assessment.

MCP integration

Acceptance testing and operational readiness.

Identity / Permissions / Action

Project / owner _____ Review date _____

Writes

- [ ] Bind approval to the exact operation, arguments, user, and relevant state.
- [ ] Do not accept a model-provided approved=true value as authorization.
- [ ] Validate permissions again when the write occurs.
- [ ] Implement application-level duplicate protection where required.
- [ ] Test a successful write with a lost response before retrying.
- [ ] Return the actual system outcome, including pending or unresolved results.

Operations

- [ ] Test expired access, downstream failures, invalid input, and timeouts.
- [ ] Log operation identity and outcome with sensitive information minimized.
- [ ] Document hosting, network controls, monitoring, and incident ownership.
- [ ] Record acceptance results and unresolved risks before production release.

Open items / owner / next action

MCP does not by itself enforce business permissions, approval, or exactly-once writes. This checklist is not a complete security assessment.