

Security & Privacy Summary (High-level)

Procurement-safe summary aligned to common vendor questionnaires. Details and exhibits (where applicable) are exchanged after scope confirmation and a secure channel agreement.

Scope and boundary

Public intake is non-confidential routing-only. Do not submit credentials, secrets, private keys, or regulated personal data in public forms.

Sensitive artefacts move only after scope confirmation and secure channel agreement.

Last updated: December 22, 2025

Non-binding summary. Final commercial and contractual terms are set only in executed agreements.

Operating model (summary)

- **Minimization-first:** request the minimum necessary information for the defined deliverables.
- **Least-privilege:** scoped and revocable access paths; time-bounded where applicable.
- **Evidence-first delivery:** deliverables reference evidence pointers; gaps are recorded, not hidden.
- **Change control:** scope changes route via SOW amendment.

Security posture snapshot (baseline)

High-level baseline posture intended to answer common questionnaire items. Engagement-scoped exhibits (where applicable) are shared after scope confirmation.

- **Identity & access:** MFA enforced for internal access; least-privilege and need-to-know; administrative access restricted and reviewed.
- **Device security:** company-managed devices are encrypted; screen lock and secure configuration controls applied; timely patching for supported systems.
- **Data protection:** encryption in transit (TLS) for supported channels; confidential artefacts exchanged only via buyer-approved secure channels.
- **Logging:** access/activity logging maintained for operational and security review where applicable to the engagement.
- **Personnel:** confidentiality obligations; access is limited to assigned delivery staff; offboarding removes access promptly.
- **Vulnerability handling:** issues are tracked and remediated per risk; third-party dependencies are assessed where applicable to deliverables.

Typical information types (engagement-scoped)

| Information type | Typical source | Notes |
|------------------------|---|---|
| Governance artefacts | Policies, standards, decision records | Used to map claims to controls and evidence. |
| Configuration evidence | Exports, screenshots, audit/log extracts (as allowed) | Collected to support evidence pointers, not broad data collection. |
| Project/process inputs | Workflows, owner lists, approval routes | Supports board-ready decision options and MAP ownership. |
| User/content data | Not required by default | If required, handled only after scope + secure channel agreement and documented in SOW/DPA. |
| Credentials/secrets | Not accepted via public channels | Secure access patterns are buyer-controlled and revocable. |

Data handling baseline (summary)

Default posture is minimization-first and buyer-controlled access. Any processing of personal data is engagement-scoped and documented in the applicable agreement(s) (e.g., SOW/DPA) when required.

- **Buyer-controlled workspace preferred:** buyer-provided SharePoint/Teams, secure file transfer, or equivalent.
- **No production credentials via public channels:** credentials and secrets are not accepted in public intake; secure access patterns are coordinated after kickoff when needed.
- **Limit copies and duration:** artefacts are shared only as required for the agreed deliverables; retention and deletion follow SOW/DPA and buyer policy where applicable.
- **Segregation:** engagement artefacts are logically separated by client and scope.
- **Export-first preference:** read-only exports and evidence pointers are preferred over broad system access.

Secure sharing and access (typical patterns)

- **Buyer-provided secure workspace preferred** (e.g., buyer-controlled SharePoint/Teams, secure file transfer, or equivalent).
- **Revocable access:** buyer retains control of accounts and can revoke at any time.
- **Scope-limited artefact movement:** only artefacts required for agreed deliverables are shared.
- **Confidential context** can route via NDA after kickoff when needed by policy.

Security operations (summary)

- **Engagement-scoped exhibits:** security details align to engagement type and data sensitivity and are provided after scope confirmation.
- **Incident path:** defined per enterprise engagement (SOW/DPA-scoped) including notification and coordination points when applicable.
- **Coordination:** where required, Noetfield aligns to buyer incident-response workflows and designated security contacts.
- **Sub-processors:** disclosed in SOW/DPA when applicable; additional details provided on request.

Privacy boundaries (summary)

- **Purpose limitation:** information is used only for the contracted scope and deliverables.
- **Retention and deletion:** set per engagement in SOW/DPA where applicable (buyer policy prevails).
- **Public routing remains non-confidential:** do not send secrets/credentials/regulated personal data via public forms.

Not accepted via public forms

- Credentials, access tokens, private keys, or secrets.
- Customer identifiers, regulated personal data, or sensitive personal data.
- Confidential legal documents or privileged communications (use secure channel after scope).

Request enterprise exhibits: email procurement@noetfield.com with the RID and requested items (e.g., DPA review, security exhibit list, sub-processor list).