Security & Privacy Summary

Enterprise-facing, non-confidential overview for procurement and risk review

Document ID: NF-SEC-PRIV **Version:** 2.3 **Date:** 2025-12-21

Non-binding summary. Buyer-specific commitments are defined only in an executed agreement (NDA/SOW/MSA/DPA) and in buyer-approved delivery channels.

Engagement boundary

- **Public intake is non-confidential.** Do not submit secrets, credentials, or regulated personal data via public forms or email.
- **Secure channels after kickoff.** Evidence and artifacts are exchanged only via mutually approved secure channels.
- **Least privilege and traceability.** Prefer read-only access and buyer-generated exports; findings are tied to Evidence IDs and dates.

RID: Include a Request / Evidence ID in email subjects and file names (example: `RID-NF-2025-XXXX`).

Security posture snapshot (baseline)

Domain	Baseline posture
Identity & access	MFA enforced; administrative access restricted; least privilege used.
Devices	Encrypted endpoints; secure configuration; offboarding access removal.
Transport	Encrypted transport for approved channels; secure transfer for deliverables.
Vulnerability handling	Updates and remediation tracked based on risk and scope.
Logging	Security-relevant logs retained and reviewed in a scope-appropriate manner.

Questionnaire quick answers (high-level)

Topic	Answer
Customer content used to train models	No - not used for training by default.
Third-party AI tools	Scoped - documented and buyer-approved if required.
Encryption in transit	Yes - for approved channels.
Encryption at rest	Scoped - depends on storage pattern; buyer workspace preferred.
Subprocessors	Scoped - disclosed and bounded per engagement; buyer-approved where required.
Incident notification	Contract-defined - timelines and contacts set in executed agreement.

Data handling baseline

Default posture is minimization, buyer-controlled access patterns, and time-bounded handling.

Data handling principles

- **Minimize.** Process only what is necessary to deliver the scoped outputs.
- **Prefer buyer-controlled storage.** Buyer workspaces and exports are preferred over vendor-hosted storage.
- **Purpose and time bounds.** Use data only for scope; remove access and delete per agreement.

Storage and residency (default posture)

Buyer-controlled storage is preferred. If storage is required, region and retention window are agreed in writing; access is restricted; and encryption-at-rest is used.

AI / LLM boundary (procurement-safe)

- **No training on customer content by default.** Customer content is not used to train models.
- **Third-party AI tools.** Any use is documented and buyer-approved if required.
- **Sensitive content excluded.** Regulated personal data, secrets, credentials, and production dumps are excluded unless explicitly agreed.

Information not accepted via public intake

- Secrets, credentials, or private keys
- Regulated personal data (health, financial account numbers, government IDs)
- Unredacted production datasets or large exports without prior written approval

Data categories and access patterns (typical)

Category	Typical pattern
Configuration / policy exports	Buyer-generated exports (policy settings, audit logs, config snapshots).
Operational evidence	Screenshots/reports shared via secure channel with Evidence IDs and dates.
Identity signals	Aggregated summaries when possible; avoid raw identifiers unless scope requires.

Retention and deletion

Retention and deletion follow the executed agreement and buyer policy. Default posture is to delete engagement data after completion or after the agreed retention window.

Operational controls and buyer alignment

Secure delivery, third parties, and incident coordination in an enterprise engagement.

Secure channels and delivery

- **Buyer-controlled workspace (preferred):** buyer SharePoint/OneDrive, approved portals, or equivalent.
- **Secure file transfer:** SFTP or encrypted transfer approved by buyer.
- **Evidence labeling:** deliverables use Evidence IDs / RID for traceability.

Subprocessors and third parties

Subprocessors/hosting (if any) are scoped per engagement. A subprocessor list and hosting posture summary are available upon request and aligned to buyer approval requirements.

Incident response and notification

- **Coordination:** incident contacts defined at kickoff and reflected in the executed agreement.
- **Notification:** timelines are contract-defined; buyer policy prevails where specified.
- **Containment:** access revoked and channels rotated as needed; evidence preserved for analysis.

Control alignment (informal)

Controls are organized to map to common enterprise domains (ISO 27001-style / SOC2-style). A lightweight control mapping can be provided after scope confirmation.

Enterprise exhibits available upon request (post-scope)

- Security Exhibit (controls overview)
- Subprocessor / hosting posture summary
- DPA position and negotiation notes
- Vendor questionnaire short answers (extended)

Contacts

Purpose	Contact
Security / trust	`trust@noetfield.com`
Procurement / vendor review	`procurement@noetfield.com`
Legal / agreements	`legal@noetfield.com`
Operations	`ops@noetfield.com`

Publishing note: Forwardable and non-confidential. Detailed controls/evidence and buyer-specific commitments are provided only after scope confirmation and via secure channels.