Security questionnaire (completed)

Completed by: Elena Voss, Head of Trust, NovaBridge, Inc. **Date:** 2026-09-02 **Product:** NovaBridge Relay **Structured copy:** `3_Build_Source_Data/questionnaire.csv`

Questionnaires are **claims**. They are not independent tests. Read the narratives, then compare them to the other artifacts in this packet.

ID	Topic	Response	Narrative
Q-01	Independent penetration testing at least annually	Yes	Testing is performed annually by an independent firm. Latest report is attached to this packet.
Q-02	Multi-factor authentication required for privileged / administrative access	Yes	Privileged Relay operators must use MFA. Local-account MFA is supported.
Q-03	Encryption at rest for customer ticket content	Yes	AES-256 at rest in NimbusCloud-managed storage.
Q-04	Encryption in transit (TLS 1.2+)	Yes	TLS 1.2 or higher for browser and API traffic.
Q-05	Customer data deleted within 30 days of contract termination	Yes	Deletion workflow completes within 30 days of written termination notice.
Q-06	Subprocessors reviewed at least annually	Yes	Trust team reviews subprocessors at least annually and publishes an updated list.
Q-07	All product modules included in the current SOC 2 report	Partial	Core Relay ticketing and knowledge base are in scope. Optional modules are documented separately if a customer enables them.
Q-08	Customer ticket content is not used to train or improve models	Yes	NovaBridge does not use customer content to train models.
Q-09	SAML / OIDC single sign-on available at customer go-live	Partial	SSO is on the enterprise roadmap. Named local accounts are supported for initial launch. MFA can be required on those accounts.
Q-10	Security incident notification to customers within 72 hours of confirmation	Yes	Trust team notifies affected customers within 72 hours of confirming a security incident.
Q-11	Customer right to audit security controls	Partial	Audit rights are as specified in the MSA. On-site access to production systems is limited.
Q-12	Primary production hosting in the United States	Yes	Production Relay for this contract is hosted in NimbusCloud us-east-1.
Q-13	Backups encrypted	Yes	Daily backups are encrypted with the same class of keys as primary storage.

ID	Topic	Response	Narrative
Q-14	Application audit logs retained at least 12 months	Yes	Admin and authentication logs retained 12 months.
Q-15	Background checks for employees with production access	Yes	U.S. employees with production access complete a background check before access is granted.
Q-16	PCI DSS because the product stores cardholder data	N/A	Relay does not store payment card data. Harborline billing remains in a separate system.
Q-17	Mobile application security tested in the last 12 months	Yes	The NovaBridge mobile companion was included in recent application security work.
Q-18	Customer may disable optional AI summarization	Yes	NovaBrief can be left off. It is not required for ticketing or knowledge base.

PCI is marked N/A. Harborline's stated use does not put cardholder data in Relay.