



SECURITY & TRUST BRIEF

How we handle your code, your data and your accounts.

The standard practices behind every NorthPulse engagement, written for founders, engineering leads and the security reviewers who sign off on new vendors.

01

YOUR CODE
STAYS YOURS

02

LEAST-
PRIVILEGE
ACCESS

03

DEVICES &
DATA

04

AI AGENT
POLICY

05

INCIDENT
RESPONSE

06

COMPANY &
CONTRACTS

OVERVIEW

At a glance

NorthPulse is an AI-first engineering studio: agents draft, and senior engineers steer, review and approve everything that reaches your systems. This brief sets out the practices we follow on every engagement, with no tiers and no opt-ins.

01 • OWNERSHIP

Your code stays yours
Work happens in repositories you own. IP assigns to you on payment. We keep no copies after the engagement ends.

02 • ACCESS

We ask for access, never ownership
Least privilege, SSO and MFA everywhere, monthly reviews, and same-day removal when an engineer rolls off.

03 • DEVICES & DATA

Encrypted machines, no production data
Full-disk encryption, automatic updates and screen lock on every device. We work with synthetic or sampled data.

04 • AI AGENTS

Disclosed tools, human-approved output
You know which tools and models we use before kickoff. Nothing AI-written merges without senior review.

05 • INCIDENTS

24-hour notice, 5-day write-up
Suspected incidents reach your named contact within 24 hours, with a written summary within five business days.

06 • COMPANY

A US contracting entity
Lucid Outsourcing LLC dba NorthPulse, Nevada. W-9, good-standing certificate and mutual NDA on request.

In this brief

01	Your code stays yours	Ownership, IP, repositories
02	Access	Least privilege, SSO/MFA, the access lifecycle
03	Devices and data	Endpoint controls, data handling, what we don't take on
04	AI agent policy	Disclosure, your restrictions, human review
05	Incident response	Notification timeline and what you receive
06	Company and contracts	Entity, documents, insurance, NDA
07	What we don't have yet	SOC 2 and other honest gaps
08	Quick answers and next steps	For your vendor questionnaire

SECTION 01

Your code stays yours

Ownership is settled before any work starts, in writing, and never depends on our goodwill. You hold the repositories, the accounts and the off switch.

OUR COMMITMENTS

- 1.1 **All work happens in repositories you own**, under accounts you control. You can revoke our access in one click, at any time, without asking us first.
- 1.2 **We never fork, mirror or keep copies of client code** after an engagement ends.
- 1.3 **IP in everything we write assigns to you on payment**, and the contract says so explicitly.

WHAT THIS MEANS IN PRACTICE

- Branches, pull requests, issues and history live in your organization, not ours. There is no NorthPulse copy to fall out of sync or to leak.
- Your team can see every change as it happens, in the tools you already use.
- If you part ways with us, nothing needs to be handed back. Revoking our access is the whole offboarding step on your side.

WHAT YOU CONTROL

- Who on our team has access, and to which repositories.
- Branch protection, required reviews and merge rights.
- When access ends: immediately, at your discretion.

The short version: we ask for access. We never ask for ownership of your code, your accounts or your infrastructure.

SECTION 02

Access

Engineers get exactly what their current work requires, through strong authentication, and lose it the day they no longer need it.

OUR COMMITMENTS

2.1

Least privilege by default. Engineers get the repositories and environments they need for their tickets and nothing else.

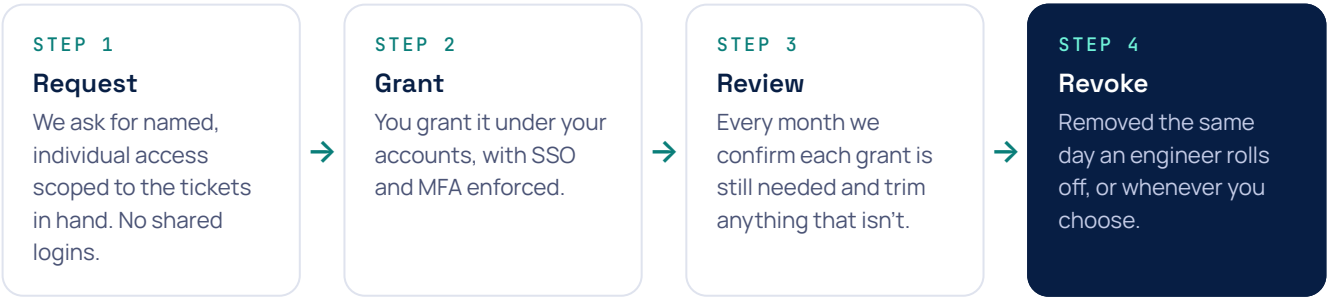
2.2

Single sign-on and multi-factor authentication on every tool we use.

2.3

Access is reviewed monthly and removed the day an engineer rolls off your engagement.

The access lifecycle



PRODUCTION AND ENVIRONMENTS

Access to production systems is not a default. Where an engagement needs it, it is scoped to the specific environment and task, granted by you and covered by the same monthly review.

ASK US FOR

- The current list of who on our team has access to what, at any time.
- Immediate removal of any grant you no longer want.

SECTION 03

Devices and data

The machines our engineers use are hardened, and your sensitive data stays out of them. Where we can't protect a class of data properly, we say so and don't take the work.

OUR COMMITMENTS

3.1

Full-disk encryption, automatic updates and screen lock on every machine used for client work.

3.2

No production data on engineer machines. We work with synthetic or sampled data unless you provide a controlled environment.

3.3

No protected health information. We do not currently sign Business Associate Agreements, so we don't take work that involves PHI.

Endpoint baseline

CONTROL	STANDARD ON EVERY MACHINE
Encryption at rest	Full-disk encryption enabled. A lost or stolen laptop does not expose code or credentials.
Patching	Automatic operating system and security updates.
Physical access	Automatic screen lock when unattended.
Authentication	SSO and MFA on every work tool (see Section 02).

How we work with your data

DEFAULT

Development and testing use synthetic data or a sample you approve. Real customer records never need to leave your systems for us to do our job.

WHEN REAL DATA IS UNAVOIDABLE

You provide a controlled environment (for example, a hosted workspace or a locked-down staging system) and the data stays there. It is not copied to engineer machines.

SECTION 04

AI agent policy

AI agents are how we deliver faster. They are also the question security reviewers ask about first. Here is exactly how we use them, and the controls you keep.

OUR COMMITMENTS

4.1

Full disclosure before kickoff. We use AI coding agents on every engagement, and we tell you which tools and models, and under which terms: API tiers with no training on your data, and enterprise agreements where available.

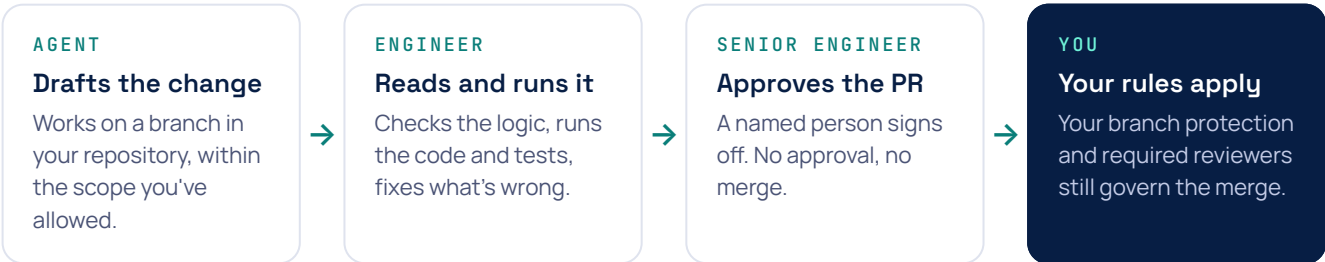
4.2

You set the limits. You can restrict or exclude AI tooling for specific repositories or data classes, in writing, at any time.

4.3

AI output never merges unreviewed. A senior engineer reads, runs and approves every pull request.

From agent draft to your main branch



THE DISCLOSURE YOU RECEIVE BEFORE KICKOFF

- Each AI tool we plan to use on your work.
- The underlying model and its provider.
- The terms it runs under, including confirmation that your code is not used to train the model.

RESTRICTIONS YOU CAN SET, IN WRITING

- Exclude AI tooling from specific repositories.
- Exclude specific data classes (for example, customer records or secrets).
- Tighten or lift restrictions at any point in the engagement.

SECTION 05

Incident response

If something goes wrong, you hear it from us first, quickly, with facts rather than reassurance, and then in writing.

OUR COMMITMENTS

- 5.1 24-hour notification.** Any suspected security incident involving your systems is reported to your named contact within 24 hours of discovery, with what we know and what we are doing.
- 5.2 Written post-incident summary** within five business days.

The timeline

**T + 0****Discovery**

We identify a suspected incident touching your systems, accounts or code. "Suspected" is the trigger: we don't wait for certainty before telling you.

**Within 24 hours****You are notified**

Your named contact hears what we know so far, what we have already done to contain it, and what happens next.

**Ongoing****Working with your team**

We keep your contact updated and follow your lead on anything inside your environment, including revoking or rotating our own access.

**Within 5 business days****Written summary**

A post-incident summary of what happened, what was affected, what was done and what changes as a result.

At kickoff, name your contact. Tell us who should receive security notifications (and a backup) so the 24-hour clock reaches the right person.

SECTION 06

Company and contracts

You contract with a registered US company, and the paperwork your vendor-onboarding process needs is ready before you ask.

ITEM	DETAIL
Contracting entity	Lucid Outsourcing LLC dba NorthPulse, a Nevada, USA limited liability company.
Tax and registration	W-9 and certificate of good standing available on request. EIN and DUNS number provided during vendor setup.
Insurance	Professional liability (technology E&O) and cyber liability. Certificates naming your company available on request.
Confidentiality	Mutual NDA available, signed before any access is granted.
Intellectual property	All IP in work we deliver assigns to you on payment, written into the contract (see Section 01).
Security questionnaires	Answered within three business days, in your format.

Documents you can request today

TAX

Form W-9

For your accounts payable and vendor master.

STANDING

Certificate of good standing

Issued by the State of Nevada.

INSURANCE

Certificates of insurance

Technology E&O and cyber, naming your company.

LEGAL

Mutual NDA

Our template or yours, signed before any access.

SECTION 07

What we don't have yet

A security brief that only lists strengths isn't much use to a reviewer. These are the limits you should know about before you choose us.

No SOC 2 report. We follow the controls in this brief and will pursue SOC 2 Type I when client requirements call for it. If you need a SOC 2 report today, we're not the right vendor yet.

No Business Associate Agreements. We don't currently sign BAAs, so we don't take on work involving protected health information.

What we offer instead

Answer your questionnaire

Send us your security questionnaire in whatever format your team uses. We return it within three business days.

NDA before access

A mutual NDA is signed before anyone on our team touches your systems, so your reviewer can share what they need to.

SECTION 08

Quick answers and next steps

The questions that come up most often in vendor reviews, answered in a line each.

QUESTION	ANSWER
Who owns the code you write?	You do. IP assigns to you on payment, in the contract.
Do you keep copies of our code?	No. We never fork, mirror or keep copies after the engagement ends.
Is our code used to train AI models?	No. We use API tiers with no training on your data, and enterprise agreements where available.
Can we turn AI tooling off?	Yes, for specific repositories or data classes, in writing, at any time.
Does AI-written code merge automatically?	Never. A senior engineer reads, runs and approves every pull request.
Will you hold production data?	Not on engineer machines. Synthetic or sampled data, or your controlled environment.
How fast do you report incidents?	Within 24 hours of discovery, with a written summary within five business days.

Send us your security questionnaire.

We answer within three business days, in your format. Happy to sign a mutual NDA first.

SECURITY PAGE

northpulse.tech/security

GET IN TOUCH

northpulse.tech/contact

This brief describes NorthPulse’s standard practices as of October 2026 and is provided for information. Where it differs from a signed agreement, the agreement governs. NorthPulse is a trade name of Lucid Outsourcing LLC, Nevada, USA.