How I work inside your AWS account

I'm Vander Nunes, the engineer who does the work. **I work remotely in US business hours through Nuno Cloud LLC.** This page explains how I get access, what I do with it, and how you take it back.

01 Access you create, own and can remove

- You create my access in your account: a user in your IAM Identity Center, or an IAM role I assume. You own it and can disable it at any time without asking me.
- Least privilege. I start read-only. Anything more is scoped to a named, agreed task.
- MFA on every sign-in. Sessions expire on their own after 4 hours at most.
- Time-bound: access has an end date that matches the engagement.
- Kubernetes access through EKS access entries or your existing mapping, read-only by default.
- Everything I do is recorded in your CloudTrail under my own named identity. No shared or root accounts.

02 Your data stays in your environment

- I don't copy customer data, database contents, logs with personal data or secrets out of your accounts.
- Your data is yours. Analysis happens inside your account and tools. Billing data you choose to send me is used only for your work and deleted when the engagement ends.

03 No long-lived keys

- No IAM users with static access keys, for me or created by me.
- No credentials in email, chat, tickets or notes. Secrets stay in your secret store.
- Each client's credentials, keys and cloud configuration are kept separate on my machine, so access to one client can never be used in another client's account.

04 Changes through your Git and your approval

- Changes are infrastructure as code, in your repositories, as pull requests your team reviews and merges.
- My commits are signed with a key used only for your work.
- I never change anything in your environment on my own. Every change is discussed with you first and made only with your formal written authorization and consent.

05 My laptop and accounts

- Full-disk encryption on the laptop I work from.
- 1Password for every credential.
- YubiKey hardware security keys plus MFA on every account I use for your work: email, Git hosting, cloud.
- Automatic system and security updates, and the screen locks itself after 5 minutes.
- A separate browser profile per client.

06 People who work with me

- Today I do the work myself.
- If another engineer joins your project, I name them to you first. They sign the same confidentiality and security terms, get their own access that you approve, and never share mine.

07 Confidentiality

- I'll sign your NDA before you share anything, or send a mutual NDA.
- Your name, data and architecture stay confidential. I don't name clients or publish their results without written approval.

08 If something goes wrong

- If I suspect anything that could affect your systems or data, such as a lost device or a credential that may be exposed, I tell you as soon as I know, always within 24 hours, and help you rotate access.

09 Data agreement

- A data processing agreement (DPA) is available on request, or I can sign yours.

10 Offboarding checklist, when the work ends or whenever you ask

1. You disable my Identity Center user or delete the role; I confirm I can't sign in.
2. EKS access entries and any Kubernetes bindings for me are removed.
3. My access to your Git hosting, CI and tools is removed.
4. Any secret I saw during the work is listed so you can rotate it.
5. I delete local copies of your files and notes and confirm it in writing.
6. You get the handover: code in your repositories, runbooks and open items.
7. Optional: we check CloudTrail together for no activity after the end date.

COMPLIANCE I help clients build SOC 2 technical controls as code: access, logging and change management. Nuno itself does not hold a SOC 2 report or other certification. I'm happy to fill in your security questionnaire.

Vander Nunes · vander@nuno.io