



SECURITY & ACCESS POLICY

Non-negotiable rules for working inside **your** systems.

How we handle your repository, servers, credentials and data on every engagement.
Sent before we ask for access, so you can hold us to it from day one.

01

Least privilege

Read-only access for the Assessment. A deploy key or a dedicated user for delivery. Never the owner's personal credentials. Access is revoked at handover and you confirm it.

02

Secrets

No .env files, keys or passwords in chat, email or tickets. Shared only through your secret manager or a one-time link. Never committed to a repository.

03

Your data

Production data is not copied to laptops. Staging uses anonymised or subset data wherever possible. No client data leaves client-controlled infrastructure.

04

Devices & accounts

Full-disk encryption, screen lock and a password manager on every engineer's machine. MFA on GitHub, AWS and email. Company accounts only, never personal ones.

05

Change control

All work through branches and pull requests, reviewed by a senior engineer. Production deploys happen only in the agreed window, with the rollback plan written first.

06

Backups

A verified restore before any change is made. We never rely on a backup we have not restored ourselves, and we run the drill before the first commit.

07

Confidentiality

A mutual NDA is offered by default with every order form. Your name, code and business details are used publicly only with your written permission.

08

Incidents

Any suspected exposure is reported to you in writing within 24 hours: what happened, when, the impact, and the fix. No waiting, no minimising.

09

Audit trail

An access log of who had what, from when to when, is kept for every engagement and included in your handover pack alongside the documentation.

What this means **for you**



You keep control

Repository and servers stay yours. We work inside them; we never move them.



You own everything

Code, documentation and configuration we produce belong to you, even if you leave.



Nothing is hidden

Weekly written status, a named senior lead, and a written report if anything goes wrong.

