Information security policy

Version 2 · Approved 18 November 2026 · Next review 18 November 2027
Owned by the Founder & CEO · Approved by the Founder & CEO
Latest version: https://gdpr.complydog.com/documents/policies/information-security

Why we have this policy

ComplyDog looks after its own information and the information customers trust us with. This policy sets out how we keep it safe: seen only by the right people, kept accurate, and there when it's needed.

Who and what it covers

Everyone who works for us or on our behalf: staff, contractors and suppliers who can reach our information. It covers the ComplyDog compliance platform, its Trust Centers and customer support, the information in it, and the systems we use to run it, including Google Workspace, GitHub, DigitalOcean, Vercel, Cloudflare and Outseta.

What we commit to

- We look for risks to our information at least once a year, and whenever something important changes, and decide what to do about each one.
- We give people only the access their work needs, and switch on two-step sign-in wherever it's offered.
- We keep systems up to date, back up important information, and check that we can restore it.
- We check suppliers' security before we rely on them.
- We report security incidents straight away, deal with them quickly and learn from them.
- We follow the laws, regulations and contracts that apply to us.
- Everyone takes security training when they join and once a year after that.
- We set yearly security goals and check how we're doing against them.

Who does what

- The Founder & CEO approves this policy and makes sure security gets the time and money it needs.
- The Founder & CEO leads security day to day: risks, incidents and the topic policies.
- The Founder & CEO owns this policy and looks at it again at least every 12 months.
- Everyone follows this policy and reports anything that looks wrong straight away.

The topic policies

The more detailed topic policies we've adopted, such as access control and incident response, sit under this one. If one of them disagrees with this policy, this policy applies until the other is fixed.

If the policy isn't followed

We take breaches of this policy seriously. Depending on what happened, the outcome can be extra training, losing access, or disciplinary action. When we review this policy, we also check it's being followed: we look at the records it asks for and fix any gaps we find. If something in this policy can't be followed, the Founder & CEO can agree an exception. It's written down with the reason, what we do instead and an end date.