Access control 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/access-control

Why we have this policy

Only the right people should be able to see or change our systems and the customer data in them. This policy explains how ComplyDog gives, checks and removes access.

Who it applies to

Everyone who works for us or on our behalf: staff, contractors and suppliers. It covers ComplyDog, Google Workspace, GitHub, DigitalOcean, Vercel, Cloudflare, Outseta and Stripe.

The rules

- People get only the access their role needs, and nothing by default.
- Every person has their own account. Where a service allows only one login, it's kept in the password manager and only named people use it.
- Two-step sign-in is switched on for every system that offers it.
- Admin access is limited to 3 named people and checked every 3 months.
- Admins use their admin rights only for admin work, not for everyday tasks.
- Passwords are long, unique to each system and kept in a password manager.

Joining, moving and leaving

- New access is asked for in writing (a message or ticket is enough) and approved by the Founder & CEO.
- When someone changes role, access they no longer need is removed.
- When someone leaves, their access is removed on their last day, and company devices and data are returned.

Who is responsible

The Founder & CEO owns this policy and looks at it again at least every 12 months. The Founder & CEO approved it. 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.