DERROS

LEGAL

LEGAL · FOR CLIENTS AND RESEARCHERS

Security

How we protect Trellis, and how to tell us about a problem.

LAST UPDATED

18 September 2026

derros.com/legal/security

IN THIS DOCUMENT

01

How Trellis is deployed

Trellis is built as a multi-tenant platform. In our hosted service, clients share the same application and infrastructure, and each client's data is kept in its own workspace, separated at application level so that users see only the workspaces they belong to.

Trellis is also available as a dedicated single-tenant instance, which runs only your organisation's workspace, or on premise, installed on your own infrastructure. On premise, you control the hosting, network, access and backups, so the hosting and infrastructure measures below apply to our hosted service and dedicated instances.

02

Hosting and infrastructure

- Trellis runs in Hetzner's ISO/IEC 27001:2022 certified data centre in Helsinki, so client data is stored inside the European Union.
- The live Trellis service has no public inbound port. It is reachable only through an encrypted Cloudflare tunnel, and Cloudflare's network filters malicious traffic and bots before requests reach our servers.
- All traffic to the live service is encrypted with HTTPS.
- The server sits behind a Hetzner network firewall that blocks all inbound connections from the internet, and it runs its own host firewall as well.
- The database, cache and search services are not reachable from the internet.
- We keep a record of every inbound connection our firewalls allow and the reason for it, and we review the rules at least once a year.
- Server operating system security updates are installed automatically.
- Server access is restricted to named Derros employees and development partners, using SSH keys over a private, encrypted network. Password logins to the server are switched off.

- The database is backed up every six hours and before every release. Backups are encrypted before they leave the server and are stored in the EU.

We review our choice of data centre and security providers regularly, and we can and will move to a different provider when that gives Trellis stronger security. Any move follows the sub-processor process in section 7 of our Data Processing Agreement.

03

Secure development

- Trellis's code is kept in a private source code repository. Every change is reviewed for correctness and security before it is merged.
- Every change runs through automated tests before it is released, and the full suite, more than 250,000 test assertions, runs every day.
- Automated guard tests check our access-control rules, so a change that breaks one fails before it can ship.
- We keep a written record of the access rules for every page and endpoint in the application.
- Passwords, API keys and other secrets are never hard-coded. Each environment keeps them in its own encrypted vault, and they reach the application as environment configuration when it runs.
- Development and production run as separate environments, with their own databases and document storage.
- Releases are deployed automatically over a private network. A database backup is taken first, and the release stops if the backup fails.

04

Application security

- Each client's data sits in its own workspace, and users see only the workspaces they belong to.
- Two-factor authentication is available to every user, using an authenticator app or a passkey, with backup codes for recovery. It is required for Derros staff and development partners.
- Passwords must be at least 12 characters long, with no maximum, and common or previously breached passwords are rejected.
- Repeated failed sign-in attempts are slowed down and then blocked, to protect accounts against password guessing.
- Passwords are stored as salted hashes using a modern algorithm.
- Forms and actions are protected against cross-site request forgery, and session cookies are marked secure and HTTP-only.
- Selected sensitive fields are encrypted in the database, and uploaded documents are held in storage that is encrypted at rest.
- Errors are reported to our monitoring service so we can fix faults quickly. It is set up not to collect IP addresses or account details.

Clients can find the security measures we commit to contractually in section 9 of our Data Processing Agreement, and details of where data is hosted in our Privacy & Data Protection notice.

05

How we run Derros

The controls below cover every device, account and cloud service used for Derros work, including when our staff work from home. They follow the five controls of the Cyber Essentials scheme.

SECURE CONFIGURATION

- Software and services we do not need are removed or disabled, and default passwords are changed before a device or service is used.
- Files downloaded from the internet cannot run automatically.
- Laptops and phones lock automatically when not in use and need a PIN, password or biometric to unlock.

SECURITY UPDATES

- We use only software that is still supported by its supplier with security updates.
- Updates that fix high-risk or critical vulnerabilities are installed within 14 days of release. That covers operating systems, applications, firewall and router firmware, the server's containers and the software packages Trellis is built from.
- Automatic updates are switched on wherever they are available.

ACCOUNTS AND ACCESS

- Accounts are created only after an approval step, each person has their own login, and people get only the access their role needs.
- Administrator rights are granted through a formal process, kept on separate accounts from everyday work, recorded in a register, and reviewed regularly.
- Multi-factor authentication is switched on for every user and administrator of every cloud service we use.
- When someone leaves, their accounts are removed or disabled promptly.
- If we suspect a password or account has been compromised, we change the password and revoke its sessions straight away, then investigate.

MALWARE PROTECTION

- Every laptop and desktop runs anti-malware software that updates itself, scans files when they are opened, and warns before a malicious website loads.
- Phones and tablets install apps only from their official app stores.

RESPONSIBILITY

A named member of the Derros team is responsible for IT and security, keeps a list of the devices and cloud services we use, and makes sure these controls are followed.

06

Standards and regulation

Derros has not had a SOC 2 audit, but we aim to meet the standard it sets. We design our security, availability and confidentiality controls against the SOC 2 Trust Services Criteria and hold ourselves to them.

Derros aims to maintain Cyber Essentials or Cyber Essentials Plus certification, the UK government-backed cyber security scheme, and to renew it every year.

The EU Cyber Resilience Act does not apply to hosted Trellis, because it is software as a service rather than an installed product. On-premise installations are software we supply, so one supplied into the EU may fall within the Act, and we will meet its requirements where they apply. The NIS2 Directive does not apply, given Derros's size and location.

07

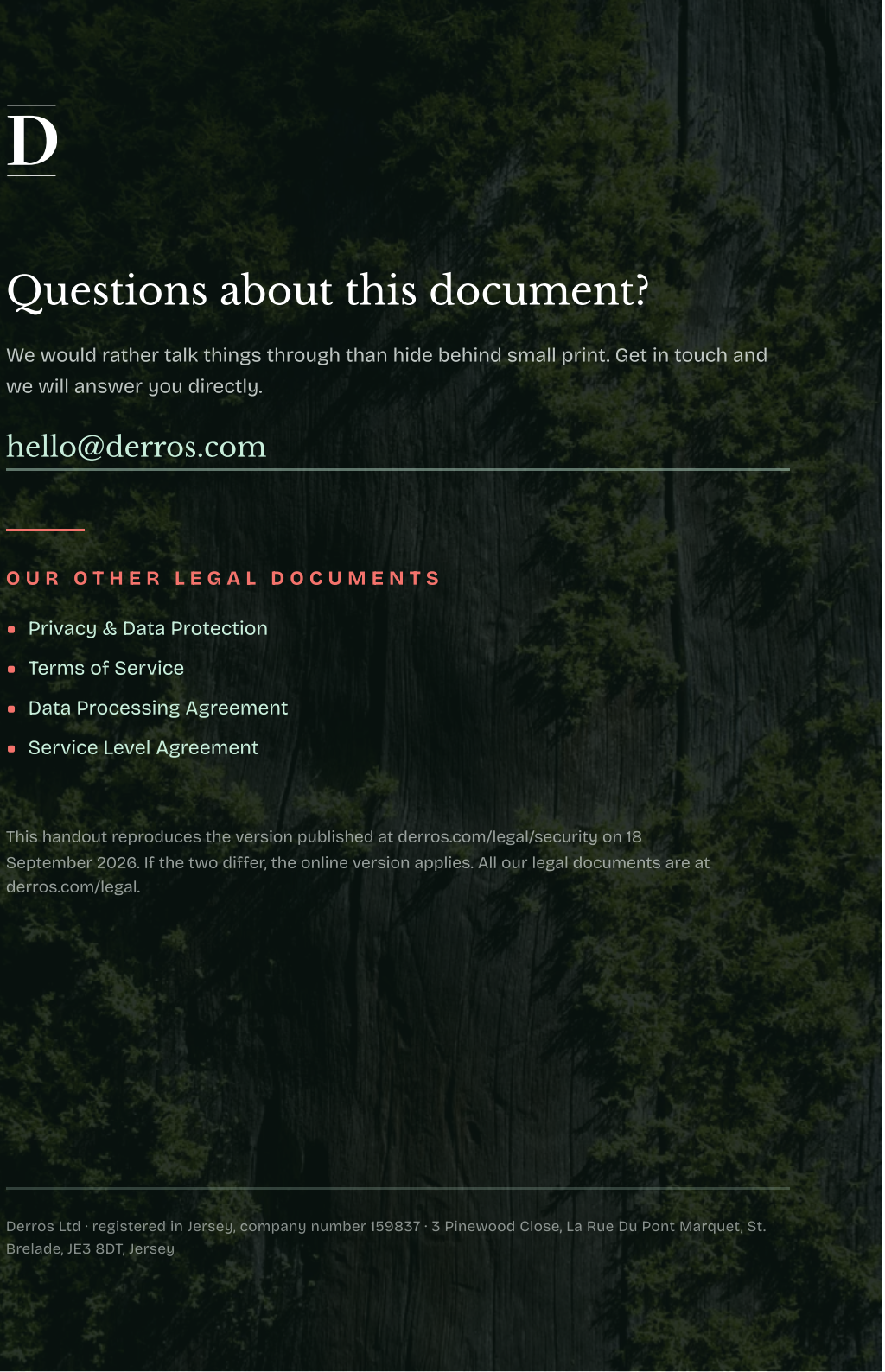
Reporting a vulnerability

If you think you have found a security vulnerability in Trellis or on derros.com, please email hello@derros.com. Tell us what you found, where, and the steps to reproduce it. We aim to acknowledge reports within five working days and will keep you updated while we fix the problem.

We will not take legal action against anyone who researches and reports in good faith and within these limits:

- only access or change data that belongs to you, and stop as soon as you reach anyone else's;
- do not disrupt the service, for example with denial-of-service attacks or automated scanning at volume;
- do not use social engineering, phishing or physical attacks against our staff or suppliers; and
- give us a reasonable time to fix the problem before you tell anyone else about it.

We do not run a paid bug bounty, but we are grateful for every report and happy to credit you once a fix is out.



D

Questions about this document?

We would rather talk things through than hide behind small print. Get in touch and we will answer you directly.

hello@derros.com

OUR OTHER LEGAL DOCUMENTS

- Privacy & Data Protection
- Terms of Service
- Data Processing Agreement
- Service Level Agreement

This handout reproduces the version published at derros.com/legal/security on 18 September 2026. If the two differ, the online version applies. All our legal documents are at derros.com/legal.

Derros Ltd · registered in Jersey, company number 159837 · 3 Pinewood Close, La Rue Du Pont Marquet, St. Brelade, JE3 8DT, Jersey