

Information Security Policy

Policy statement

Two Hat Software Ltd protects the confidentiality, integrity and availability of its own information and of the information clients trust us with. We apply security controls proportionate to the risk, and we follow recognised good practice, including the controls in the UK government's Cyber Essentials scheme.

Scope

This policy applies to all information, devices, accounts and systems used for company business. It covers the company's director, any employees we may take on, and any substitutes and subcontractors.

Devices

- All laptops and mobile devices used for company work have full-disk encryption, a screen lock with a short timeout, and a strong passcode.
- Operating systems, browsers and software are kept up to date, with security updates applied promptly.
- Devices run anti-malware protection and have a firewall enabled.
- Lost or stolen devices are reported straight away, and wiped remotely where possible.

Accounts and access

- Every account uses a unique, strong password stored in a password manager.
- Multi-factor authentication is turned on wherever it is available, and always for email, code hosting, cloud platforms and client systems.
- Access is limited to what each task needs. Administrator and cloud root accounts are used only for tasks that require them.
- Access to client systems is removed or handed back when an engagement ends.

Client information

- We follow each client's security policies and access procedures when working on their systems.

- Client credentials and secrets are kept in a password manager or the client's own secrets store. They are never kept in source code, chat messages or plain text files.
- Client data is stored only on encrypted devices and approved services. It is not put on removable media unless the client has agreed and the media is encrypted.
- Client information is not discussed or displayed where it can be overheard or overlooked.

Secure development

- Source code is held in version control on a platform protected by multi-factor authentication.
- Changes are reviewed, and automated tests and checks run before release where the project supports it.
- Dependencies are kept up to date and checked for known vulnerabilities.
- Secrets are injected at runtime from a secure store. They are never committed to repositories.
- Cloud infrastructure is defined as code where practical, follows the principle of least privilege, and has logging turned on.

Email and phishing

We treat unexpected links, attachments and requests for payment or credentials with caution, and check them through a separate channel before acting on them.

Backups

Company information is held in cloud services with built-in resilience, and important data is backed up. We test that backups can be restored.

Incidents

Any suspected security incident is reported to the director straight away. We will:

1. contain the incident and assess its impact
2. tell affected clients promptly, as our contracts require
3. report any personal data breach as our Data Protection Policy sets out
4. record what happened and what we have changed to prevent it happening again

Disposal

When devices and storage media reach the end of their life, they are securely wiped or destroyed. Paper containing confidential information is shredded.

Remote working

Work is mostly done remotely. We use secure, password-protected networks, and avoid untrusted public networks for client work unless the connection is otherwise protected.

Responsibility and review

The director, George Dennington, is responsible for information security. This policy is reviewed at least once a year, and after any significant incident. It took effect on 3 October 2026.

Two Hat Software Ltd is registered in England and Wales, company number 17490460.

Registered office: Apartment 6, 89 Parade, Leamington Spa, England, CV32 4NL.

© 2026 Two Hat Software Ltd