PepperSprint Security Policy

Last Updated: 1 July 2026

Table of Content

1 Our Commitment to Security

At PepperSprint, protecting our clients' information, systems, and intellectual property is a core business responsibility. Security is integrated into our operations, software development lifecycle, and service delivery practices to help safeguard the confidentiality, integrity, and availability of information.

We continually review and improve our security practices to address evolving threats and industry best practices.

2 Security Principles

Our security program is guided by the following principles:

- Protect client data and confidential information.
- Apply security throughout the software development lifecycle.
- Minimise security risks through preventive controls.
- Limit access to information based on business need.
- Continuously improve our security practices.
- Promote security awareness across our organisation.

3 Information Security

PepperSprint implements appropriate administrative, technical, and organisational measures designed to protect information from unauthorised access, disclosure, alteration, or destruction.

Examples of these measures include:

- Role-based access controls.
- Strong authentication practices.
- Secure password management.
- Multi-factor authentication where supported.
- Secure remote working practices.
- Encryption of data in transit using industry-standard protocols.
- Endpoint protection and device security.
- Regular software updates and security patching.
- Controlled access to development environments.
- Secure backup procedures where applicable.

4 Secure Software Development

Security is considered throughout our software development process.

Depending on the engagement, our development practices may include:

- Secure coding standards.
- Peer code reviews.
- Version control using managed repositories.
- Dependency and package management.
- Identification and remediation of known vulnerabilities.
- Testing before production deployment.
- Controlled release and deployment procedures.
- Separation of development, testing, and production environments where practical.

Security activities are proportionate to the nature and risk profile of each project.

5 Access Management

Access to systems, repositories, infrastructure, and client environments is granted only to authorised personnel who require access to perform their responsibilities.

PepperSprint seeks to ensure that:

- user accounts are individually assigned;
- access rights follow the principle of least privilege;
- access is reviewed periodically where appropriate; and
- access is revoked when no longer required.

6 Data Protection

Where PepperSprint processes personal data, we do so in accordance with applicable privacy and data protection laws and our published GDPR Commitment and Privacy Policy.

We seek to minimise the collection and retention of personal data and implement safeguards appropriate to the nature of the information being processed.

7 Third-Party Services

Our services may utilise reputable third-party providers, including cloud hosting platforms, source code repositories, collaboration tools, AI platforms, and communication services.

While we carefully select our providers, each third-party service remains responsible for the security of its own infrastructure and services under its respective terms and policies.

8 Business Continuity

PepperSprint maintains operational practices intended to support service continuity and minimise disruption.

Depending on the engagement, these practices may include:

- secure source code repositories;
- documented deployment procedures;
- controlled backups;
- knowledge sharing within project teams; and
- recovery planning appropriate to the services provided.

9 Security Awareness

We recognise that information security depends not only on technology but also on people.

Personnel are expected to:

- maintain confidentiality;
- follow internal security procedures;
- use approved systems and tools;
- report suspected security incidents promptly; and
- handle client information responsibly.

10 Incident Management

PepperSprint maintains procedures for identifying, investigating, and responding to security incidents.

Where a security incident materially affects client information or contracted services, we will take reasonable steps to:

- investigate the incident;
- mitigate further impact;
- notify affected clients where appropriate and legally required;
- implement corrective measures; and
- review lessons learned to strengthen our security practices.

11 Client Responsibilities

Security is a shared responsibility.

Clients are expected to:

- maintain appropriate security for their own systems;
- protect account credentials;
- promptly report suspected security issues;
- provide secure access to project environments;
- maintain appropriate backup and disaster recovery arrangements unless otherwise agreed.

12 Responsible Disclosure

PepperSprint appreciates reports from security researchers and members of the community who identify potential security vulnerabilities.

If you believe you have identified a security issue affecting our systems or services, please report it responsibly by contacting:

security@peppersprint.com

We ask that you:

- act in good faith;
- avoid disrupting our services;
- refrain from accessing or modifying data that does not belong to you;
- provide sufficient information to reproduce the issue; and
- allow us reasonable time to investigate before publicly disclosing the vulnerability.

13 Compliance

PepperSprint strives to operate in accordance with applicable legal, contractual, and regulatory requirements relevant to the services we provide.

Where appropriate, client-specific security requirements may be addressed through contractual agreements, Statements of Work, or Data Processing Agreements.

14 Continuous Improvement

Cybersecurity is an ongoing process.

We periodically review our policies, development practices, operational procedures, and security controls to improve our resilience against emerging threats and support the evolving needs of our clients.

15 Contact

For questions regarding this Security Policy or to report a security concern, please contact:

PepperSprint

Email: **security@peppersprint.com**

For additional information, please refer to our:

- Privacy Policy
- GDPR Commitment
- Responsible Disclosure Policy
- Terms & Conditions
- Data Processing Agreement (available upon request)