Vulnerability Management Policy

1. Purpose

This policy establishes Subcontext's approach to identifying, assessing, and remediating security vulnerabilities. It makes sure weaknesses in our code, dependencies, container images and infrastructure are found early, judged consistently and fixed within set timescales.

2. Scope

This policy applies to:

- The Subcontext application code, including the web application, REST API, MCP server, embeddable widgets and the iOS, Android and Mac apps
- Third-party libraries and packages the platform uses
- Production container images
- AWS infrastructure and its configuration
- Devices used by personnel to access Subcontext systems, as set out in the Information Security Policy

3. Definitions

Term	Meaning
Vulnerability	A weakness that could be exploited to compromise confidentiality, integrity or availability
Remediation	Removing a vulnerability, by fixing code, updating a dependency or changing configuration
Compensating control	A measure that reduces the risk of a vulnerability that cannot yet be fixed, such as a firewall rule or disabling a feature
Remediation target	The maximum time from a vulnerability being confirmed to it being remediated

4. Roles and Responsibilities

Role	Responsibility
Security Officer	Owns this policy, triages findings, sets severity, approves exceptions and tracks remediation
Engineers	Act on findings in the code they work on, keep dependencies current and do not release code that fails the security checks
Founding team	Approves emergency releases where needed and accepts residual risk that exceeds the targets

5. Vulnerability Identification

- **Dependency scanning:** automated scanning of application dependencies for known vulnerabilities (Bundler Audit for Ruby, npm audit for JavaScript)
- **Static analysis:** automated security scanning of application code (Brakeman)
- **Infrastructure monitoring:** AWS security advisories and configuration compliance checks
- **Automated dependency updates:** Dependabot raises weekly updates for Ruby gems and GitHub Actions
- **JavaScript dependency audit:** `importmap audit` checks the browser JavaScript packages for known vulnerabilities
- **Container image scanning:** every production image is scanned for vulnerabilities when pushed to Amazon ECR
- **Web application firewall:** AWS WAF managed rule sets (common exploits, SQL injection, known bad inputs, IP reputation) protect the platform's public endpoint
- **External reports:** responsible disclosure from external security researchers

Bundler Audit, `importmap audit` and Brakeman run as part of the full check suite before every release, and Brakeman fails on any warning. A release must not go ahead while any of these checks is failing. Findings can also arise from penetration tests, incident reviews, supplier advisories and customer reports.

6. Risk Assessment and Prioritisation

Severity	Description	Remediation Target
Critical	Actively exploited or trivially exploitable, high impact	Within 24 hours
High	Exploitable with known techniques, significant impact	Within 7 days
Medium	Requires specific conditions to exploit, moderate impact	Within 30 days
Low	Difficult to exploit, limited impact	Within 90 days

Severity is set by the Security Officer, starting from any published score for the issue and then adjusted for how Subcontext actually uses the affected component. Factors include whether the vulnerable code is reachable, whether exploitation needs authentication, what data would be exposed (taking account of the Data Classification Policy), and whether a compensating control is already in place.

6.1 Worked examples

- A library vulnerability rated high by its publisher, in a function Subcontext never calls, may be rated Low, with the reasoning recorded, and updated in the next routine dependency update.
- A flaw that would let a signed-in user read another organisation's data is rated Critical even if exploiting it needs some effort, because of the impact.
- A vulnerability in a container base image affecting a package not used at runtime is normally rated Medium or Low, and fixed by rebuilding the image.

7. Remediation

- Vulnerabilities are remediated by applying patches, updating dependencies, or implementing compensating controls
- Critical and high-severity vulnerabilities may require emergency releases outside the normal change management process
- Remediation is verified through re-scanning or manual testing

Every confirmed vulnerability rated Medium or above is recorded with its severity, owner, target date and status until it is closed. Fixes are released through the Change Management Policy, using the emergency route where the target requires it. Where a fix is not yet available, a compensating control is put in place and the vulnerability stays open until fully remediated. A vulnerability that is being actively exploited is also handled as an incident under the Incident Response Plan.

8. Exceptions and Risk Acceptance

If a vulnerability cannot be remediated within its target (for example because no fix exists or the fix would break a critical function), the owner must request an exception. The request states the reason, the compensating controls in place and a new target date. Exceptions are approved by the Security Officer, and for Critical and High vulnerabilities also by a director. Approved exceptions are recorded in the risk register and reviewed at least monthly until closed.

9. Penetration Testing

- External penetration testing is conducted at least annually, beginning in 2027
- Findings are triaged and remediated according to the severity targets above
- Once a test has been completed, its report is retained and available to customers upon request (subject to reasonable redaction)

Testing is also considered after significant changes to the platform's architecture or authentication. Retesting confirms that Critical and High findings are fixed.

10. Responsible Disclosure

Security researchers who discover vulnerabilities in the Subcontext platform should report them to hello@subcontext.com, as set out in full in our Vulnerability Disclosure Policy. We commit to:

- Acknowledging receipt within 2 business days
- Providing an initial assessment within 5 business days
- Working with the reporter to understand and resolve the issue
- Not pursuing legal action against researchers acting in good faith

Reported vulnerabilities are assessed and remediated under the same severity targets as any other finding.

11. Monitoring Compliance

The Security Officer reviews open vulnerabilities and any missed targets at least monthly, and reports the position to the founding team. Trends, such as repeated issues of the same kind, feed into secure coding guidance and the risk register.

12. Related Documents

- Information Security Policy
- Vulnerability Disclosure Policy
- Secure Development Policy
- Change Management Policy
- Incident Response Plan
- Data Classification Policy

13. Document Control

Item	Detail
Owner	Security Officer
Approved by	The directors of Subcontext Ltd
Review	At least annually, and after any significant change to tooling or infrastructure
Effective	October 2026

Subcontext Ltd, registered in England and Wales, Company No. 17019645. Registered office: 124 City Road, London, EC1V 2NX. The current version of this document is published at subcontext.com.