FRAUDFINDER LTD
71-75 Shelton St
London
WC2H 9JQ
United Kingdom

Email: alexander@fraudfinderai.com

Fraudfinder Vulnerability Remediation Policy & Timelines

1. Purpose and Commitment

To ensure that all identified vulnerabilities, whether reported internally, by clients, via third-party tools, or external researcher, are triaged, prioritised, and remediated in line with their severity and potential impact.

---

2. Scope

Fraudfinder uses the **CVSS v3.1 (Common Vulnerability Scoring System)** as baseline, along with contextual risk factors like exposure, exploitability, and business impact.

Severity Level	Definition	Examples
Critical	Exploitable vulnerability with significant risk to data integrity, availability, or client trust	Remote code execution, unauthenticated access to PII
High	Major security gap that could be exploited under specific conditions	Privilege escalation, insecure file handling
Medium	Exploitable under limited or internal circumstances	XSS, insecure API responses with rate limits
Low	Unlikely to be exploited; no material risk	Missing HTTP headers, outdated libraries

---

3. Remediations Timeline (SLA)

Severity	Time to Triage	Time to Remediate	Time to Verify & Close
Critical	4 business hours	24–48 hours (max)	24 hours post-fix

High	1 business day	5 business days	2 days post-fix
Medium	3 business days	14 business days	3 days post-fix
Low	5 business days	Next scheduled sprint	As part of regression testing

Delays beyond SLA must be documented, approved by the Head of Tech, and reviewed during monthly security standups.

---

4. Remediation Workflow

1. **Detection & Reporting**
    - Internal scans (e.g., GitHub Dependabot)
    - Pen test or client-reported
    - External researcher via **security@fraudfinder.ai**
2. **Triage (within SLA)**
    - Assign severity based on CVSS + context
    - Log in security backlog (e.g., Jira or Notion Security Board)
    - Assign Dev owner
3. **Remediation**
    - Code fix, dependency patch, infra update, or config change
    - Code reviewed and tested
    - For client-impacting fixes: deploy through emergency patch pipeline
4. **Verification & Closure**
    - Retest and validate fix
    - Update status in vulnerability register
    - Notify reporter (if external)

- Update affected clients (Enterprise only or if SLA breach occurred)

---

5. Monitoring & Reporting

- Monthly vulnerability report reviewed by **Head of Tech + Security Lead**
- Quarterly review of:
    - SLA compliance %
    - Open vulnerability age
    - Recurring root causes

---

6. Exceptions & Risk Acceptance

If a vulnerability **cannot be patched within SLA**:

- It must be documented in the **Risk Register**
- Include justification, compensating controls, and target timeline
- Requires **explicit sign-off from the Head of Tech**

---

7. Review & Audit

- This policy is reviewed **every 6 months**

Approved by:
Andrew Kenyon, Head of Tech

Effective Date: 06 July, 2025
Next Review Date: 05 July, 2026