Vulnerability Disclosure Policy

Last updated: 31 Jan 2025

Legl is committed to maintaining the security of our systems and protecting the privacy and trust of our customers. We welcome responsible disclosure of security vulnerabilities that could affect our services, and we aim to resolve valid issues promptly.

This Vulnerability Disclosure Policy describes how to report vulnerabilities to us, what you can expect in response, and what we expect from researchers. Please read it fully before reporting a vulnerability and act in accordance with it at all times.

Reporting a vulnerability

If you believe you have discovered a security vulnerability in a Legl system or service, please report it to us via one of the following methods. We prefer submission via our dedicated security email for direct handling.

- **Email:** security@legl.com
- **Submit via OpenBugBounty:** https://www.openbugbounty.org/submit/

When reporting, please include:

- The domain, page, or IP address where the vulnerability was observed.
- A clear and concise description of the issue (e.g., "Reflected XSS in onboarding form", "Insecure Direct Object Reference allowing access to other users' data").
- Detailed, step-by-step instructions or a clear proof-of-concept to reproduce the vulnerability reliably.
- Any relevant technical information, such as request/response samples, screenshots, or video recordings.
- An assessment of the potential impact of the vulnerability.
- Your contact details (optional, but recommended if you would like updates on your submission or recognition).

What you can expect

After you submit a report in accordance with this policy, we will:

- Acknowledge receipt of your report within 7 working days.
- Initiate an investigation and aim to provide an initial assessment of validity within 14 working days.
- Prioritise the remediation of valid vulnerabilities based on their severity, potential impact, and complexity of the fix.
- Keep you informed of our progress in investigating and remediating the vulnerability. We will aim to provide updates at least once every 10 working days for critical issues, and no less than once every 30 days for others.

- Notify you once the reported issue has been remediated.
- Recognise your contribution for keeping our customers safe and secure.

If your submission is valid, represents a previously unknown vulnerability, and you have requested credit, we may recognise your contribution for keeping our customers safe and secure.

If you wish to publicly disclose the issue, we require that you coordinate the timing and content of the disclosure with us *after* the issue has been fully resolved.

Scope

This policy applies to security vulnerabilities found in:

- All publicly accessible web applications and services hosted under the legl.com domain.
- Our primary customer-facing web applications.
- Our public marketing websites.

If you are unsure whether a specific system or service is in scope, please contact us at security@legl.com before conducting any testing.

Out of scope vulnerabilities and activities

The following types of vulnerabilities and activities are considered out of scope and should not be reported or attempted:

- Missing security headers (e.g., CSP, HSTS) unless their absence directly leads to a demonstrable vulnerability.
- Outdated TLS configurations or weak cipher suites that do not result in a practical, exploitable vulnerability.
- Reports of spam or social engineering techniques (e.g., phishing).
- Physical security testing.
- Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks.
- Automated scanning results without a clear, manually verified proof-of-concept for each reported issue.
- Vulnerabilities requiring a user to have significant privileges (e.g., administrator access) unless a privilege escalation is demonstrated.
- Disclosure of information that is already publicly known.
- Vulnerabilities in third-party services or platforms not managed directly by Legl. Please report these directly to the respective third party.
- Any activity that could degrade the performance or availability of our services.

Guidance for Researchers

When conducting security research, you must:

- Comply with all applicable laws and regulations.
- Stop testing immediately and report it if you encounter any personal data, confidential information, or other sensitive data. Do not access, modify, or retain this data.
- Always act in good faith and avoid causing privacy violations, service disruptions, or data loss.
- Comply with all applicable data protection and privacy laws.
- Securely delete any data retrieved during your testing as soon as it is no longer required to demonstrate the vulnerability, or within **14 days** of the vulnerability being resolved, whichever is sooner.
- Limit the amount of data accessed to the minimum necessary to demonstrate the vulnerability.

You must not:

- Access, modify, or delete data you do not own or have explicit permission to access.
- Attempt to move laterally within our network or escalate access beyond the initial vulnerability.
- Use high-intensity, automated tools that could impact system performance.
- Attempt or report denial-of-service (DoS) attacks.
- Attempt social engineering, phishing, or gain physical access to Legl facilities or equipment.
- Disclose vulnerability information to anyone other than Legl without our prior written consent, especially before the vulnerability is fixed.
- Demand compensation in exchange for vulnerability disclosure.

Legal

This policy supports responsible vulnerability research and aims to be compatible with UK and international good practice.

If you make a good faith effort to abide by this policy during your security research, Legl will consider your actions authorised and will not pursue legal action against you. This includes testing systems within scope, reporting vulnerabilities without public disclosure, and refraining from harming Legl or its data.

Nothing in this policy grants you permission to act in an unlawful manner, nor does it create any contractual rights or legally binding agreement between you and Legl. Legl reserves all of its legal rights in the event of any non-compliance or malicious activity.

Thank you for helping to keep Legl secure.