

Vulnerability Disclosure Policy

Overview

TLJ Group is committed to protecting the security and privacy of our customers, users, products, services, and systems.

We recognise that security researchers, customers, partners, and members of the public may identify potential vulnerabilities in our products or services. This policy explains how potential vulnerabilities should be reported to us, how we will handle reports, and how we will work with reporters in a fair, professional, and coordinated way.

This policy follows the principles of coordinated vulnerability disclosure and is intended to support timely investigation, remediation, and communication of security vulnerabilities.

Scope

This policy applies to reports concerning potential security vulnerabilities in TLJ Group products, services, and systems.

The following are **out of scope** unless explicitly agreed with us in advance:

- Systems, products, or services not owned, operated, or maintained by TLJ Group
- Third-party websites, services, libraries, or platforms, except where they directly affect an in-scope product or service
- Physical attacks against premises, staff, offices, staff devices, or equipment
- Social engineering, phishing, or impersonation of our staff, customers, suppliers, or partners
- Denial-of-service, load, stress, or destructive testing
- Attempts to access, modify, delete, copy, or exfiltrate data that does not belong to you
- Attempts to gain persistence, pivot to other systems, or escalate access beyond what is required to demonstrate the issue
- Use of malware, ransomware, worms, or automated destructive tools
- Vulnerabilities that only affect unsupported, end-of-life, or heavily modified products unless they create a risk to supported products or services
- Vulnerabilities requiring compromised, rooted, jailbroken, or previously unauthorised devices unless clearly relevant to the security of our product

Policy

How to report a vulnerability

Vulnerabilities should be reported through our website contact form:

<https://tljgroup.com/contact/form>

Report a vulnerability

When submitting a vulnerability report, please select the category: **Vulnerability Disclosure**

If this category is not available, please select the closest available category and include **“Vulnerability Disclosure”** in the subject line or message title.

Please include as much of the following information as possible:

- A description of the suspected vulnerability
- The affected product, service, model, firmware version, software version, or system
- Steps to reproduce the issue
- Any proof-of-concept details, screenshots, logs, sample requests, or relevant technical evidence
- The potential impact of the vulnerability
- Whether you believe the issue is being actively exploited
- Whether any personal data, customer data, or confidential information may have been exposed
- Your name or preferred alias and contact details
- Whether you would like public acknowledgement if an advisory is published

Please do not include personal data, customer data, confidential information, or data obtained without authorisation unless it is strictly necessary to demonstrate the vulnerability. If you accidentally access such data, stop testing immediately and notify us through the contact form.

Once the contact form is submitted, our team will review it under our vulnerability disclosure process. Security-related submissions will be handled confidentially and routed to the appropriate internal team for triage and investigation.

Where possible, we recommend that reporters retain a copy of their submission for their own records.

Reporter conduct

We ask reporters to act responsibly and in good faith.

Reporters must:

- Only test against systems, products, and services that are in scope
- Avoid privacy violations, data destruction, service disruption, and degradation of user experience
- Avoid accessing, modifying, copying, deleting, or sharing data that does not belong to them
- Stop testing and notify us immediately if they encounter personal data, confidential data, or unauthorised access
- Avoid denial-of-service, social engineering, phishing, physical security attacks, or attacks against employees, customers, suppliers, or partners
- Not publicly disclose details of the vulnerability until we have had a reasonable opportunity to investigate and, where appropriate, remediate the issue
- Comply with all applicable laws and regulations

Where a reporter acts in good faith, follows this policy, and avoids harm to [Company Name], our users, customers, suppliers, and third parties, we will aim to work with them constructively and professionally.

What you can expect from us

When we receive a vulnerability report, we will aim to:

1. Review and triage the submission.
2. Investigate whether the issue is valid and reproducible.
3. Assess severity, impact, affected products, and remediation options.
4. Develop and deploy a mitigation or fix where appropriate.
5. Publish a security advisory where appropriate.
6. Recognise the reporter's contribution where agreed.
7. Carry out a post-incident review where appropriate.

We will handle vulnerability reports confidentially and share details only with those who need access to investigate, validate, mitigate, or coordinate the vulnerability.

Compliance

This policy will be officially monitored for compliance by the HSQE Director and may include random and scheduled inspections.

Non-compliance

All policies require the participation of staff to be successful. Anyone found to have violated this policy may be subject to disciplinary action.

This policy has been approved & authorised by:

Name: Claire Martin
Position: HSQE Director
Date: 15th September 2025

Review Date: September 2026

Signature:

A handwritten signature in black ink, appearing to read 'Martin', is placed within a light grey rectangular box.