Towelrads
VULNERABILITY DISCLOSURE POLICY

Effective Date: 25/06/2026
Last Updated: 25/06/2026

1. Purpose
Towelrads.com Ltd (Towelrads) is committed to maintaining the security of our products, systems, and services. We welcome reports from security researchers, customers, and members of the public who believe they have identified a security vulnerability. This Vulnerability Disclosure Policy describes how to report vulnerabilities to us and how we will respond to such reports.

2. Scope
This policy applies to vulnerabilities affecting products manufactured, developed, or supplied by Towelrads. If you are unsure whether a vulnerability falls within scope, please contact us using the reporting details below.

3. Reporting a Vulnerability
Security vulnerabilities should be reported to PSTI@towelrads.com and where possible, reports should include and be encrypted:

- A description of the vulnerability
- The affected product, software version, or service
- Steps required to reproduce the issue
- Proof-of-concept code or screenshots (if applicable)
- The potential security impact
- Your contact details for follow-up questions

4. Our Commitments
Upon receiving a vulnerability report, we will:

- **Acknowledge Receipt** - We will acknowledge receipt of a vulnerability report within **5 working days**.
- **Assess the Report** - We will review the information provided and determine whether the reported issue constitutes a security vulnerability.
- **Provide Status Updates** - We will provide updates regarding the progress of our investigation and remediation efforts where appropriate.
- **Remediate Valid Vulnerabilities** - Where a reported vulnerability is confirmed, we will seek to remediate it within a timeframe proportionate to the severity, complexity, and potential impact of the issue.
- **Coordinate Disclosure** - We support coordinated vulnerability disclosure and will work with reporters regarding public disclosure timelines where appropriate.

5. What We Ask of Security Researchers

When conducting security research, we ask that you:

- Act in good faith and avoid privacy violations, destruction of data, interruption of services, or exploitation of vulnerabilities beyond what is necessary to demonstrate their existence.
- Do not access, modify, or delete data belonging to others.
- Do not disclose vulnerability details publicly until we have had a reasonable opportunity to investigate and remediate the issue.
- Comply with all applicable laws and regulations.
- Avoid social engineering, phishing, physical attacks, denial-of-service attacks, spam, or other activities that may negatively affect our users, systems, or services.

6. Safe Harbour

Provided that researchers act in good faith, comply with this policy, and make reasonable efforts to avoid harm to users, customers, employees, and our services, Towelrads will not initiate legal action against researchers solely for reporting vulnerabilities under this policy. This statement does not authorise activities that are unlawful or that cause harm, service disruption, privacy violations, or unauthorised access to data.

7. Information Handling

Information submitted under this policy will be used for the purpose of investigating and remediating security vulnerabilities. Personal information submitted as part of a vulnerability report will be handled in accordance with our Privacy Policy and applicable data protection laws.

8. Security Update Support Periods

In accordance with applicable UK product security requirements, Towelrads publishes the minimum period during which security updates will be provided for each relevant connectable product.

Current support periods are available at https://towelrads.com/security-support-periods

Support periods include will include both the minimum duration for which security updates will be provided; and the applicable support end date.

9. Policy Updates

We may update this Vulnerability Disclosure Policy from time to time. The latest version will be published on our website.