



Vulnerability Disclosure Policy

External security researcher reporting process

Effective date	1 October 2026
Policy owner	Tec Reports Group
Security contact	service@bennettbrooks.co.uk
Website	www.tecreportsgroup.co

Purpose

This policy tells external security researchers how to safely report suspected software, hardware or service vulnerabilities to Tec Reports Group and explains how we will handle those reports.

Tec Reports Group appreciates responsible security research that helps us identify and address potential weaknesses while protecting our customers, systems and services.

1. Our Commitment

At **Tec Reports Group**, we take the security of our systems, software, hardware, services and information seriously.

We recognise that security researchers and other members of the public may identify vulnerabilities that we have not yet discovered. We therefore welcome responsible reports of potential security vulnerabilities affecting our systems, applications, services or hardware.

This Vulnerability Disclosure Policy explains how external security researchers can safely report vulnerabilities to us and what they can expect from Tec Reports Group during investigation and remediation.

2. Reporting a Vulnerability

If you believe you have identified a security vulnerability affecting Tec Reports Group, please report it to us as soon as reasonably possible.

Security contact: service@bennettbrooks.co.uk

Suggested subject line: CONFIDENTIAL – Vulnerability Report

Please do not report suspected security vulnerabilities through general customer-service channels or social media.

Where possible, include:

- A clear description of the vulnerability.
- The affected website, application, software, hardware or service.
- The relevant URL, product name, model or version.
- Steps required to reproduce the vulnerability.
- Proof-of-concept information, screenshots or other supporting evidence.
- The potential security impact.
- Any relevant CVE, CWE or CVSS information, if known.
- Details of testing already undertaken.
- Your contact details so our security team can communicate with you.

Please avoid including unnecessary personal, confidential or commercially sensitive information in your report.

3. Safe and Responsible Security Testing

Researchers are expected to conduct testing responsibly and take reasonable steps to prevent disruption, damage or unauthorised access to information.

Researchers should:

- Only test systems and services owned or operated by Tec Reports Group that are within the scope of this policy.
- Avoid accessing, modifying, deleting or downloading information belonging to other individuals.
- Avoid actions that could interrupt or degrade our services.
- Avoid denial-of-service or distributed denial-of-service testing.

- Avoid social engineering, phishing or physical security testing unless expressly authorised in writing.
- Avoid installing persistent software, malware or backdoors.
- Avoid attempting to maintain access after demonstrating a vulnerability.
- Stop testing if sensitive personal, customer or commercially confidential information is encountered.
- Notify Tec Reports Group immediately if sensitive information is unintentionally accessed.
- Delete information obtained unintentionally when it is no longer required to demonstrate the vulnerability, where appropriate and legally permissible.

4. Scope

This policy applies to security vulnerabilities affecting Tec Reports Group systems, applications, software, hardware and services that are owned or operated by Tec Reports Group.

Examples of potentially in-scope areas include:

- www.tecreportsgroup.co
- Tec Reports Group web applications and customer-facing portals.
- Tec Reports Group APIs.
- Tec Reports Group-developed applications and software.
- Authentication and access-control mechanisms.
- Vulnerabilities that could result in unauthorised access to Tec Reports Group systems or information.
- Tec Reports Group-owned hardware or technology.

Third-party systems: Systems, applications, services or infrastructure owned and operated by third parties are not automatically included, even where Tec Reports Group uses or links to those services. Researchers must not test third-party infrastructure without appropriate authorisation from the relevant owner.

5. Out-of-Scope Activities

Unless expressly authorised in writing by Tec Reports Group, researchers must not undertake:

- Denial-of-service or distributed denial-of-service attacks.
- Stress or load testing capable of affecting service availability.
- Social engineering or phishing attacks against employees or customers.
- Physical security testing.
- Destructive testing.
- Attacks against third-party systems.
- Deliberate access to, modification or deletion of customer information.
- Mass automated scanning that creates significant system load.
- Spam or mass messaging.
- Installation of malware or persistent access mechanisms.
- Any activity that could negatively affect availability, integrity or confidentiality.

6. Responsible Disclosure

Tec Reports Group asks security researchers to allow reasonable time to investigate and, where appropriate, remediate a reported vulnerability before publicly disclosing technical details.

Once a vulnerability has been reported, we will work with the researcher where appropriate to determine a reasonable disclosure timeframe.

Researchers should not publicly disclose vulnerability details, exploit code or proof-of-concept material, customer or employee information, credentials, security keys, confidential business information, or information that could enable further exploitation while the issue is being investigated.

7. Our Response Process

Following receipt of a vulnerability report, Tec Reports Group will:

- **Acknowledge:** Acknowledge receipt where reasonably possible.
- **Assess:** Assess whether the report represents a genuine security vulnerability and identify affected systems.
- **Investigate:** Investigate and attempt to reproduce the reported issue.
- **Risk assess:** Consider impact, exploitability, access requirements, affected systems, users, controls and mitigations.
- **Remediate:** Determine and implement appropriate remediation or mitigation measures.
- **Communicate:** Provide the researcher with appropriate updates regarding investigation and remediation.
- **Close:** Confirm closure where appropriate and discuss coordinated disclosure if applicable.

8. Response Times

Tec Reports Group will endeavour to acknowledge vulnerability reports within **5 business days**.

Investigation and remediation times will depend on the severity, complexity and potential impact of the reported vulnerability.

Where a vulnerability presents a significant or immediate risk, it may be prioritised for urgent investigation and remediation.

9. Critical or High-Risk Vulnerabilities

If you believe a vulnerability could result in significant unauthorised access, exposure of sensitive information, compromise of systems or significant disruption to our services, clearly mark your report:

CRITICAL SECURITY VULNERABILITY

Please provide as much relevant technical information as possible. Researchers should avoid public disclosure while Tec Reports Group investigates the issue.

10. Good-Faith Security Research

Tec Reports Group recognises the value of responsible security research.

Where a researcher acts in good faith, follows this policy, limits testing to systems within scope, avoids unnecessary harm or disruption, does not intentionally access or misuse information beyond what is reasonably necessary to demonstrate the vulnerability, and reports the vulnerability promptly, Tec Reports Group will consider the research to have been conducted responsibly.

We will not seek legal action solely because a researcher has carried out authorised security research in accordance with this policy. This does not provide permission to test systems belonging to third parties and does not prevent Tec Reports Group from taking appropriate action where activities fall outside this policy or involve malicious, destructive, fraudulent or unlawful activity.

11. Personal and Confidential Information

Researchers must not intentionally access, collect, copy, retain or disclose personal or confidential information.

If such information is accidentally accessed during testing, the researcher should:

- Stop testing the affected area where reasonably possible.
- Avoid copying, downloading or distributing the information.
- Notify Tec Reports Group immediately.
- Securely delete unintentionally obtained information when it is no longer required to demonstrate the vulnerability, where appropriate and legally permissible.

12. Confidentiality

Tec Reports Group will treat vulnerability reports as confidential and restrict access to individuals who need the information to investigate, assess and remediate the reported issue.

Researchers are also requested to maintain confidentiality while Tec Reports Group investigates and addresses the vulnerability.

Nothing within this policy prevents either party from complying with legal, regulatory or law-enforcement requirements.

13. Public Disclosure

Tec Reports Group supports responsible and coordinated disclosure.

Where a vulnerability has been confirmed, Tec Reports Group will seek to work with the researcher regarding any proposed public disclosure.

Where appropriate, the parties may agree:

- A disclosure date.
- The technical information that can be published.

- Information that must be removed or redacted.
- Appropriate acknowledgement of the researcher.

Public disclosure must not contain customer information, personal information, credentials, security keys or other information that could create additional security risks.

14. Researcher Recognition

Where appropriate, and with the researcher's permission, Tec Reports Group may acknowledge security researchers who responsibly identify and report valid vulnerabilities.

Recognition does not imply that the researcher is an employee, contractor, agent or representative of Tec Reports Group.

Tec Reports Group does **not currently operate a bug bounty programme**. Unless separately agreed in writing, submitting a vulnerability report does not create an entitlement to financial compensation.

15. Reports That Are Not Security Vulnerabilities

A report may be determined not to represent a security vulnerability. Examples include:

- Issues with no meaningful security impact.
- General recommendations or best-practice suggestions without an identifiable vulnerability.
- Issues affecting third-party systems.
- Vulnerabilities outside the published scope.
- Issues that cannot be reproduced.
- Issues requiring highly unrealistic circumstances to exploit.

Where appropriate, Tec Reports Group will explain the outcome of our assessment.

16. Changes to This Policy

Tec Reports Group may update this Vulnerability Disclosure Policy from time to time.

The latest version of this policy will be published on **www.tecreportsgroup.co**. Researchers should review the current version before undertaking security research.

17. Contact Us

Tec Reports Group

Security Contact: Theodore Griffin

Email: service@bennettbrooks.co.uk

Website: www.tecreportsgroup.co

Registered Head Office

Griffin House
2 Rawdon Road
Moirā
Swadlincote
Derbyshire
DE12 6DQ

Telephone: 0333 091 3001

Thank you for helping Tec Reports Group keep its systems secure.

Responsible security research helps us strengthen our systems, protect our customers and maintain the security and integrity of the services we provide.