



TS3D-IS-20 Coordinated Vulnerability Disclosure Policy V1.0

Document title	Coordinated Vulnerability Disclosure Policy		
Reference No.	TS3D-IS-20	Version	1.0
Author	Richard Taylor - Senior IT Manager, Security & Compliance Marco Salino - Product Manager II, Hoops Exchange		
Reviewed by	Ross Mills - Senior Director of Engineering Thibault Tournier - Director of Engineering Frode Brandt - Director of Engineering William Gallego - Senior Director of Partner Success Jeff Wheeler - Senior Director of Operations Technology		
Authorised by	Jeff Wheeler - Senior Director of Operations Technology		
Effective Date	18 Sept 2026		

DOCUMENT CONTROL

Version	Date	Description	Author	Approved by
1.0	18/09/2026	New Issue	Richard Taylor	Jeff Wheeler

1. Introduction

1. Tech Soft 3D is committed to the security of its software products and the protection of its users. This Coordinated Vulnerability Disclosure Policy (CVD Policy) describes how security researchers, customers, and any other third party can report vulnerabilities affecting our products, and how Tech Soft 3D will handle such reports in a transparent, timely, and responsible manner.
2. This policy is issued in compliance with the EU Cyber Resilience Act (Regulation (EU) 2024/2847), Article 13 and Annex I Part II, which require manufacturers to establish and maintain a coordinated vulnerability disclosure policy.

2. Scope

1. This policy applies to all software products developed and maintained by Tech Soft 3D, including the HOOPS, SpinFire & Tetra4D product brands. It covers vulnerabilities reported by external security researchers, customers, partners, or any other third party.
2. This policy does not cover vulnerabilities in third-party software or services that are not under our direct control. Where applicable, we will forward reports to the relevant vendors.

3. Reporting a Vulnerability

1. If you believe you have identified a vulnerability affecting one of our products, please report it:
 - By creating a Support Ticket at [Tech Soft 3D Support Portal](#)
 - Or by email to support@techsoft3d.com
2. Reports should include sufficient information to allow the issue to be reproduced and investigated.

3. Where possible, please provide:

- product name and version
- a description of the vulnerability
- steps required to reproduce the issue
- proof-of-concept code, input data, or screenshots if available
- an assessment of the potential impact
- your contact details for follow-up questions.

4. Providing detailed information helps us investigate and resolve the issue more efficiently.

4. Our Commitments to Reporters

1. When you report a vulnerability to us in good faith, Tech Soft 3D commits to the following:

4.1. Acknowledgement

1. We will acknowledge receipt of your report within 3 business days and provide you with a reference number for tracking.

4.2. Assessment and Communication

1. We will assess the reported vulnerability and provide you with an initial evaluation of its validity and severity within 10 business days. We will keep you informed of our progress at regular intervals throughout the remediation process.

4.3. Remediation

1. We will work to remediate confirmed vulnerabilities in a timeframe commensurate with their severity. Critical / High severity issues will receive immediate investigation and temporary remediation. Medium and Low severity issues are prioritised and scheduled through our standard product release process. In all cases, security updates are made available without undue delay.

4.4. Coordinated Disclosure

1. We ask that you allow us a reasonable remediation period before publicly disclosing the vulnerability. We are committed to working with you to agree on a disclosure timeline that protects users while respecting your right to publish your findings. As a general guideline, we aim to remediate and coordinate public disclosure within 90 days of the initial report.

5. Responsible Disclosure

1. We request that vulnerability reports are handled in accordance with responsible disclosure practices.

2. When researching and reporting, you must:

- act in good faith, and test only systems or software you own or are authorised to test
- limit any testing to the minimum necessary to demonstrate a vulnerability exists
- report promptly and allow us a reasonable remediation period (see 4.4) before any public disclosure.

3. You must not:

- access, modify, corrupt, delete, or exfiltrate data belonging to Tech Soft 3D or other users, or violate the privacy of our users
- perform denial-of-service testing, use high-intensity or invasive automated scanning, or otherwise disrupt or degrade systems or services

- use social engineering, phishing, or physical attacks against our staff or infrastructure.

6. Safe Harbour for Security Research

1. We support good-faith security research.
2. If you identify a potential vulnerability and report it in accordance with this policy, including the rules of engagement in Section 5, we will consider your research to be authorised.
3. Activities that breach those rules or applicable law are not authorised under this policy and may result in legal action.

7. Handling of Vulnerability Reports

1. Vulnerability reports are received by Tech Soft 3D Support and routed to the Security Captain for the affected product, who is responsible for validation, assessment of impact, and co-ordination of the response with the relevant engineering and product teams.
2. The handling process typically includes:
 - a. Review and validation of the reported issue.
 - b. Assessment of the affected products and versions.
 - c. Evaluation of the potential impact and severity.
 - d. Initiation of remediation activities where appropriate.
3. During the investigation process, we may contact the reporting party to request additional information.
4. If a vulnerability is confirmed, remediation may include:
 - releasing a patched product version
 - providing mitigation guidance.
5. Security updates are made available without undue delay and free of charge through our official distribution channels.

8. Regulatory Reporting Obligations

1. In accordance with Article 14 of the EU Cyber Resilience Act, Tech Soft 3D is required to report actively exploited vulnerabilities and severe security incidents to the relevant national CSIRT and ENISA via the ENISA Single Reporting Platform.
2. Where a reported vulnerability is determined to be actively exploited, we may be required to notify authorities as part of our regulatory obligations. We will inform you if this is the case.
3. After becoming aware of an actively exploited vulnerability or a severe incident affecting the security of our products, we will inform impacted users, and where appropriate all users, of the vulnerability or incident and of any risk mitigation or corrective measures they can deploy.

9. Third-Party Components

1. Tech Soft 3D products may include third-party libraries or components.
2. If a vulnerability is reported in a third-party component that is distributed as part of a Tech Soft 3D product, we will assess whether the vulnerability affects our products, report the vulnerability to the maintainer or vendor of the affected component, and take appropriate remediation actions.
3. Issues affecting third-party components that are not distributed with our products should be reported directly to the relevant vendor.

10. Security Advisories

1. Once a security update has been made available, we will publish a security advisory describing:
 - the vulnerability
 - affected products and versions
 - the potential impact of the vulnerability
 - its severity (for example, a CVSS score and a Critical / High / Medium / Low rating)
 - remediation or mitigation guidance.
2. Security advisories may reference publicly assigned vulnerability identifiers such as CVE numbers.
3. In duly justified cases, where we consider that publishing full details of a vulnerability would create greater security risk than benefit, we may delay disclosure of those details until users have had a reasonable opportunity to apply the relevant security update.

11. Disclosure and Acknowledgement

1. We aim to coordinate disclosure of confirmed vulnerabilities with the reporting party whenever possible.
2. We value responsible vulnerability reporting under this policy. However, we do not offer monetary rewards for vulnerability disclosures.
3. Researchers who responsibly report vulnerabilities may be acknowledged in security advisories unless anonymity is requested.

12. Privacy

1. Information provided in vulnerability reports will be used solely for the purpose of investigating and resolving security issues.
2. Personal information will be handled in accordance with applicable data protection and privacy regulations.

13. Out of Scope

1. The following are out of scope of this policy:
 - Vulnerabilities in third-party services or infrastructure not operated by Tech Soft 3D.
 - Tech Soft 3D corporate IT and business systems, public websites and documentation sites, and customer-facing services and portals that do not themselves deliver product functionality, including the support portal and demonstration and trial environments.
 - Pre-release, preview, experimental and laboratory features that are not part of a generally available product release.
 - Sample code, tutorials, training material and standalone public code repositories that are not distributed as part of a supported product package.
 - Product versions that are outside their published support period.
2. Where a service operated by Tech Soft 3D delivers functionality that one of our products requires in order to perform one of its functions, that service is treated as part of the product and remains in scope of this policy.
3. Code distributed within a supported product release remains in scope of this policy however it is designated, including sample code, deprecated functionality and bundled third-party components.
4. Reports about anything listed above remain welcome via the channels in Section 3 and will be considered on their merits, although the commitments in Section 4 and the advisory process in Section 10 do not apply to them.

Issues affecting systems operated by Tech Soft 3D are handled through our internal incident management process.

5. Active security testing of the Tech Soft 3D systems and services listed above is not authorised under this policy, and the safe harbour in Section 6 does not extend to it.

14. Policy Updates

1. This policy is reviewed annually and updated as needed to reflect changes in our products, regulatory requirements, or industry best practices. The current version is always available on our website.
2. For questions about this policy, contact us at support@techsoft3d.com

15. Supporting Documents

Supporting Documentation	
TS3D-IS-02	Data Management Policy
TS3D-IS-12	Incident Response Policy
Regulation (EU) 2024/2847	EU Cyber Resilience Act
ISO/IEC 29147:2018	Information technology — Security techniques — Vulnerability disclosure
ISO/IEC 30111:2019	Information technology — Security techniques — Vulnerability handling processes