VULNERABILITY DISCLOSURE POLICY

1 Introduction

1.1 White Paper Advisors Sweden AB is committed to ensuring the security of the whistleblower and our clients by protecting their information. This policy is intended to give security researchers clear guidelines for conducting vulnerability discovery activities and to convey our preferences in how to submit discovered vulnerabilities to us.

1.2 This policy describes **what systems and types of research** are covered under this policy, **how to send us** vulnerability reports, and **how long** we ask security researchers to wait before publicly disclosing vulnerabilities.

1.3 We encourage you to contact us to report potential vulnerabilities in our systems.

2 Authorization

2.1 If you make a good faith effort to comply with this policy during your security research, we will consider your research to be authorized we will work with you to understand and resolve the issue quickly, and White Paper Advisors Sweden AB will not recommend or pursue legal action related to your research. Should legal action be initiated by a third party against you for activities that were conducted in accordance with this policy, we will make this authorization known.

3 Guidelines

3.1 Under this policy, "research" means activities in which you:

3.1.1 Notify us as soon as possible after you discover a real or potential security issue.

3.1.2 Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data.

3.1.3 Only use exploits to the extent necessary to confirm a vulnerability's presence. Do not use an exploit to compromise or exfiltrate data, establish persistent command line access, or use the exploit to pivot to other systems.

3.1.4 Provide us a reasonable amount of time to resolve the issue before you disclose it publicly.

3.1.5 Do not submit a high volume of low-quality reports.

3.2 Once you've established that a vulnerability exists or encounter any sensitive data (including personally identifiable information, financial information, or proprietary information or trade secrets of any party), **you must stop your test, notify us immediately, and not disclose this data to anyone else.**

4 Test methods

4.1 The following test methods are not authorized:

4.1.1 Network denial of service (DoS or DDoS) tests or other tests that impair access to or damage a system or data

4.1.2 Physical testing (e.g. office access, open doors, tailgating), social engineering (e.g. phishing, vishing), or any other non-technical vulnerability testing

5 Scope

5.1 This policy applies to the following web applications:

5.1.1 https://trumpet-whistleblowing.eu/

5.1.2 https://*.trumpet-whistleblowing.eu/

5.1.3 https://casemanagement.trumpet-whistleblowing.eu

5.2 Any service not expressly listed above, such as any connected services, are excluded from scope and are not authorized for testing. Additionally, vulnerabilities found in systems from our vendors fall outside of this policy's scope and should be reported directly to the vendor according to their disclosure policy (if any). If you aren't sure whether a system is in scope or not, contact us at support@trumpet-solutions.se before starting your research.

6 Reporting a vulnerability

6.1 We accept vulnerability reports via support@trumpet-solutions.se or https://www.whitepaperadvisors.se/kontakt.

6.2 If you share contact information, we will acknowledge receipt of your report within 3 business days.

6.3 Information submitted under this policy will be used for defensive purposes only – to mitigate or remediate vulnerabilities. If your findings include newly discovered vulnerabilities that affect all users of a product or service and not solely White Paper Advisors Sweden AB, we may ask permissions to share your report with this third-party service provider. We will not share your name or contact information without express permission.

7 What we would like to see from you

7.1 To help us triage and prioritize submissions, we recommend that your reports:

- 7.1.1 Describe the location the vulnerability was discovered and the potential impact of exploitation.
- 7.1.2 Offer a detailed description of the steps needed to reproduce the vulnerability (proof of concept scripts or screenshots are helpful).
- 7.1.3 Be in Swedish or English, if possible.

8 What you can expect from us

8.1 When you choose to share your contact information with us, we commit to coordinating with you as openly and as quickly as possible.

- 8.1.1 Within 3 business days, we will acknowledge that your report has been received.
- 8.1.2 To the best of our ability, we will confirm the existence of the vulnerability to you and be as transparent as possible about what steps we are taking during the remediation process, including on issues or challenges that may delay resolution.
- 8.1.3 We will maintain an open dialogue to discuss issues.

9 Questions

9.1 Questions regarding this policy may be sent to support@trumpet-solutions.se. We also invite you to contact us with suggestions for improving this policy.

9.2 Document change history

Version	Date	Description
1.0	2021-10-06	First issuance.