Findity Policy - Vulnerability Disclosure & Safe Harbor

Expense Management.
Simplified. For you.

FINDITY

Document Version: 2	Approved Version date: 2025-11-26	Review date: 2025-11-29
Information Classification: External	Owner: Information Security Manager	By: CEO

Findity AB
556838-8200
findity.com
info@findity.com

FINDITY

Document Version: 2	Approved Version date: 2025-11-26	Review date: 2025-11-29
Information Classification: External	Owner: Information Security Manager	By: CEO

1 Introduction

Findity AB welcomes feedback from security researchers and the general public to help improve our security. If you believe you have discovered a vulnerability, privacy issue, exposed data, or other security issues in any of our assets, we want to hear from you. This policy outlines steps for reporting vulnerabilities to us, what we expect, what you can expect from us.

2 Systems in Scope

This policy applies to any digital assets owned, operated, or maintained by Findity AB.

3 Out of Scope

- Third-party systems and services not owned/operated by Findity.
- Social engineering, phishing, physical security tests
- DDoS/DoS, spam, brute force at scale, destructive testing.
- Mass data access/exfiltration.

Vulnerabilities discovered or suspected in out-of-scope systems should be reported to the appropriate vendor or applicable authority.

4 Our Commitments

When working with us, according to this policy, you can expect us to:

- Respond to your report promptly, and work with you to understand and validate your report;
- Strive to keep you informed about the progress of a vulnerability as it is processed;
- Work to remediate discovered vulnerabilities in a timely manner, within our operational constraints; and
- Extend Safe Harbor for your vulnerability research that is related to this policy.

5 Our Expectations

In participating in our vulnerability disclosure program in good faith, we ask that you:

- Play by the rules, including following this policy and any other relevant agreements. If there is any inconsistency between this policy and any other applicable terms, the terms of this policy will prevail;
- Report any vulnerability you've discovered promptly;
- Avoid violating the privacy of others, disrupting our systems, destroying data, and/or harming user experience;

- Use only the Official Channels to discuss vulnerability information with us;
- Provide us a reasonable amount of time (at least 90 days from the initial report) to resolve the issue before you disclose it publicly;
- Perform testing only on in-scope systems, and respect systems and activities which are out-of-scope;
- Limit any access to unintended data to the minimum necessary to demonstrate your proof of concept, and immediately stop testing and submit a report if you encounter any user data:, such as Personally Identifiable Information (PII), Personal Healthcare Information (PHI), credit card data, or proprietary information;
- Only interact with test accounts you own or with explicit permission from the account holder; and
- Do not engage in extortion, blackmail, ransom demands, or any attempt to leverage a vulnerability for undue advantage or payment.

6 Official Channels

Please report security issues via mailto:privacy@findity.com, providing all relevant information. The more details you provide, the easier it will be for us to triage and fix the issue.

7 Safe Harbor

When conducting vulnerability research under this policy, and provided you comply with it, we consider your research to be:

- Authorized concerning any applicable anti-hacking laws, and we will not initiate or support legal action against you for accidental, good-faith violations of this policy;
- Authorized concerning any relevant anti-circumvention laws, and we will not bring a claim against you for circumvention of technology controls;
- Exempt from restrictions in our Terms of Service and/or Acceptable Usage Policy that would interfere with conducting security research, and we waive those restrictions on a limited basis; and
- Lawful, helpful to the overall security of the Internet, and conducted in good faith.

You are expected, as always, to comply with all applicable laws. To the extent permitted by law and within our control, if legal action is initiated by a third party against you and you have complied with this policy, we will take steps to make it known that your actions were conducted in compliance with this policy.

If at any time you have concerns or are uncertain whether your security research is consistent with this policy, please submit a report through one of our Official Channels before going any further.

Note that the Safe Harbor applies only to legal claims under the control of the organization participating in this policy, and that the policy does not bind independent third parties.

FINDITY

Document Version: 2	Approved Version date: 2025-11-26	Review date: 2025-11-29
Information Classification: External	Owner: Information Security Manager	By: CEO

8 Revision history

Revision number	Created date	Created by	Approved date	Approved by
1	2025-11-05	Henrik Wejdmark		
2	2025-11-26	Per Qvarforth	2025-11-29	Patrick Olsson