SOLIDWARETOOLS

CRACheck

DOCUMENT 6

Coordinated Vulnerability Disclosure Policy

Annex I, Part II, point 5 + Art. 13.8

NovaBridge Technologies Inc.

NovaBridge SmartHub v3.1

Reference: CRACHK-Y8IV87
Date of issuance: 15/10/2026
Contact: Sarah Chen, VP of Compliance
compliance@novabridge.io

Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 (Cyber Resilience Act)

This document does not constitute legal advice. Sole responsibility of the manufacturer.

>> COORDINATED VULNERABILITY DISCLOSURE POLICY

Pursuant to Annex I, Part II, point 5 of Regulation (EU) 2024/2847, the manufacturer must establish and apply a Coordinated Vulnerability Disclosure (CVD) policy. This document establishes the structured process for receiving, managing and disclosing vulnerabilities.

1. Scope

This policy applies to the product NovaBridge SmartHub v3.1 and to all software and hardware components that comprise it, including the associated remote data processing solution (if applicable).

2. Reporting channel

POINT OF CONTACT [Art. 13.17]

security@novabridge.io · https://www.novabridge.io/security · +1 302 555 0142 (EST hours)

The manufacturer allows researchers to choose their preferred communication medium. The point of contact is not based exclusively on automated tools (Art. 13.17).

3. Management process

DESCRIPTION

Coordinated disclosure policy published at https://www.novabridge.io/security/cvd-policy. Reporting channel: security@novabridge.io + HTTPS web form. Commitment to acknowledgement within 48 business hours. Target remediation time: 90 days from vulnerability confirmation. Coordinated public disclosure after patch availability. Active bug bounty programme on HackerOne (https://hackerone.com/novabridge) with $100-$5,000 rewards based on CVSS severity.

4. Response times

ACKNOWLEDGEMENT OF RECEIPT

As defined in the management process (section 3)

INITIAL ASSESSMENT

As defined in the management process (section 3)

TARGET REMEDIATION

According to CVSS classification — see remediation process (Document 3)

COORDINATED DISCLOSURE

After patch availability, coordinating with the researcher

5. Publication of fixed vulnerabilities

Pursuant to Annex I, Part II, point 4, after the availability of a security update, the manufacturer publishes: vulnerability description, affected products, impact, severity and clear information for users to apply the fix. In justified cases, publication may be deferred until users have had the opportunity to apply the patch.

6. Researcher protection

The manufacturer will not take legal action against security researchers who report vulnerabilities in good faith and responsibly, in accordance with this policy.

This document does not constitute legal advice. Sole responsibility of the manufacturer.

This document has been generated by CRACheck (SolidwareTools) from the information provided by the manufacturer. It does not constitute legal advice or a third-party audit. The accuracy of the data and effective compliance with applicable legal obligations are the sole responsibility of the manufacturer. The structure follows Regulation (EU) 2024/2847 as reviewed by SolidwareTools at the date of issuance. For personalised advice, consult a qualified professional.