SOLIDWARETOOLS

CRACheck

DOCUMENT 4

User Information and Instructions

Annex II

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.

>> MANDATORY INFORMATION (Annex II)

1. Manufacturer data

NAME [Annex II, point 1]
NovaBridge Technologies Inc.

ADDRESS
1200 Tech Park Drive, Suite 400, Wilmington, DE 19801, USA

EMAIL
compliance@novabridge.io

WEBSITE
https://www.novabridge.io

2. Vulnerability contact point

CONTACT [Annex II, point 2]
security@novabridge.io · https://www.novabridge.io/security · +1 302 555 0142 (EST hours)

CVD POLICY
Available on the manufacturer's website

3. Product identification

NAME AND TYPE [Annex II, point 3]
NovaBridge SmartHub v3.1

VERSION
3.1.0

TYPE/BATCH/SERIAL
SH-2026-LOT04

4. Intended purpose and security environment

INTENDED PURPOSE [Annex II, point 4]
WiFi/Zigbee smart home hub for centralised control of smart home devices (lights, smart locks, security cameras, motion and temperature sensors). Includes iOS/Android mobile app and cloud backend (AWS eu-west-1) for remote access and push notifications. Intended for residential consumers in the EU, sold through Amazon.de, Amazon.fr and Amazon.es.

5. Known cybersecurity risks

RISK CIRCUMSTANCES [Annex II, point 5]
(1) Use on open WiFi networks or with weak encryption (WEP) may expose communication between the hub and the router. Mitigation: the hub rejects connections to networks without WPA2/WPA3. (2) Not updating the firmware may leave the device vulnerable to known exploits. Mitigation: automatic updates enabled by default. (3) Reusing the device without factory reset may expose the previous user's data and configurations. Mitigation: visible warning in the app when unlinking the device. (4) Weak cloud account passwords may allow unauthorised remote access. Mitigation: password complexity requirements + MFA recommended on first use.

6. Declaration of conformity

ACCESS [Annex II, point 6]

See Document 5 of this dossier or on the manufacturer's website

7. Technical support and support period

SUPPORT PERIOD [Annex II, point 7]

5 years — until 03/2031

TYPE OF SUPPORT

Free security updates throughout the support period

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

8. Detailed instructions

8(A) SECURE INSTALLATION AND USE [Annex II, 8(a)]

1. Connect only to WiFi networks protected with WPA2 or WPA3. 2. Change the admin password during initial setup (the system requires it). 3. Enable two-factor authentication (MFA) in the NovaBridge mobile app. 4. Keep firmware updated — automatic updates are enabled by default. 5. Do not expose the local management port (443) to the internet; always use the secure cloud connection for remote access. 6. Periodically review paired Zigbee devices and remove unknown ones. 7. Review access logs in the app (Settings > Security > Access history).

8(B) CHANGES AND DATA SECURITY [Annex II, 8(b)]

Firmware updates may modify security configurations. It is recommended to review the configuration after each major update.

8(C) UPDATE INSTALLATION [Annex II, 8(c)]

OTA (Over-The-Air) with Ed25519 digital package signing. TLS 1.3 end-to-end encrypted channel. Firmware integrity verification (SHA-256) before and after installation. Automatic rollback to previous firmware in case of verification failure. Security updates separated from functional ones whenever technically feasible. Each security update remains available for download for a minimum of 10 years (Art. 13.9).

8(D) SECURE DECOMMISSIONING [Annex II, 8(d)]

Factory reset from the app (Settings > System > Restore factory defaults) or physical button on the device (hold for 5 seconds). The reset erases: all stored WiFi credentials, cloud access tokens, configurations and scenes, paired Zigbee device list, local event logs. After resetting, the hub automatically unlinks from the user's cloud account. The user can request complete deletion of their cloud data at https://www.novabridge.io/privacy/data-deletion.

8(E) DISABLE AUTOMATIC UPDATES [Annex II, 8(e)]

[To be completed by the manufacturer: how the user can turn off the automatic installation of security updates, where applicable]

9. SBOM

SBOM AVAILABILITY [Annex II, point 9]

The manufacturer makes the SBOM available to the user upon request. Contact security@novabridge.io · https://www.novabridge.io/security · +1 302 555 0142 (EST hours)

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.