HUMLY

Vulnerability Disclosure Policy

Humly Solutions AB — coordinated vulnerability disclosure

Version 1.1 — 9 October 2026

1. Reporting a security vulnerability

Humly builds workplace booking devices and software used by organisations worldwide, and we take the security of our products seriously. We welcome reports from security researchers, customers, and anyone else who believes they have found a vulnerability in a Humly product or service. This page describes how to report it to us and what you can expect in return.

2. Scope

This policy covers vulnerabilities in:

- Humly Room Display (device hardware, firmware and software)
- Humly Booking Device (device hardware, firmware and software)
- Humly Control Panel (server software and Humly-operated cloud services)
- Humly's other software, integrations and the humly.com website

Out of scope:

- Denial-of-service testing against systems or devices in production use
- Social engineering or phishing of Humly staff, customers or partners
- Physical attacks against premises or hardware you do not own
- Findings that require physically opening or destroying a device you do not own
- Reports about third-party services not operated by Humly (report those to the respective vendor; we appreciate a heads-up if a Humly product is affected)

3. How to report

Email your report to security@humly.com. Please include where possible:

- The product or service affected, with version or firmware number if known
- Steps to reproduce the issue, or a proof of concept
- The impact you believe the vulnerability has
- Your name/handle and whether you would like public credit
- If your report contains sensitive material, say so in a first short email and we will arrange a secure channel for the details

4. What we promise

- Acknowledgment of your report within 3 business days
- An initial assessment and a point of contact within 10 business days
- Status updates as we investigate and remediate, and a heads-up before we publish a fix
- Credit in our security advisory if you wish (or anonymity if you prefer)
- Within Humly's authority, we will not pursue legal action against research conducted and reported in good faith within this policy's scope. Authorisation is limited to systems and activities Humly may authorise; it does not permit access to another customer's systems or data and does not bind third parties or public authorities.

5. What we ask

- Give us reasonable time to remediate before public disclosure. We aim to resolve confirmed vulnerabilities within 90 days and coordinate disclosure with you; urgent mitigation, remediation and reporting required by law take priority over that target.
- Do not access, modify or delete data that is not yours; if you encounter personal data, stop and report immediately
- Only test against devices and accounts you own or have permission to test
- Do not degrade the service for others

6. Our disclosure practice

Humly publishes security advisories describing fixed vulnerabilities and affected versions as required by applicable law, subject to any legally permitted delay needed to protect users. Security updates required during the applicable support period are supplied free through the standard update mechanisms. The acknowledgement and assessment targets above do not delay urgent escalation, notification or reporting required by the Cyber Resilience Act or data protection law.

This policy will be reviewed at least annually. Questions about the policy itself can be sent to the same address.