

Coordinated vulnerability disclosure policy and security.txt

Shieldbook 0.1.0 · Last verified: 2026-10-05 · Applies from: 11 December 2027

Information and templates, not legal advice. Our reading of the official sources, not reviewed by a lawyer. You decide how the CRA applies to your product; for an opinion you can rely on, ask a lawyer; for a third-party conformity assessment, a notified body. This template helps you work with the EU Cyber Resilience Act (Regulation (EU) 2024/2847) but does not certify, assess or guarantee the compliance of any product. You remain responsible for your product's conformity assessment, CE marking and reporting. Last verified against official sources: 2026-10-05.

Coordinated vulnerability disclosure (CVD) means people who find a security flaw tell you privately first, and the details go public only after you have had a chance to fix it. The CRA requires manufacturers to put in place and enforce a CVD policy [1](#). It also requires them to make it easy to report vulnerabilities, including by providing a contact address [2](#).

This document gives you three things: the public policy page (section 1), a machine-readable security.txt file (section 2), and a list of places to show your contact (section 3).

What the CRA expects

These are the manufacturer's duties under the CRA; check in `01-scope-and-class` whether they apply to you.

- **A single point of contact.** Manufacturers must name a single point of contact so users can reach them directly and quickly, including to report vulnerabilities. It must be easy to find, and it must appear in the user information that comes with your product [3](#) [4](#).
- **A real choice of channel.** Users must be able to choose their preferred means of communication, and the manufacturer must not offer only automated tools such as a chatbot [5](#). If you run a chatbot, also offer a phone number, an email address or a contact form [6](#).
- **Reports through a CSIRT.** A reporter may prefer to go through a CSIRT, a national computer security incident response team designated as coordinator, and may ask to stay anonymous. Your policy should allow for that [7](#).
- **Evidence in your technical file.** The technical documentation must include the CVD policy and evidence that the manufacturer provided a contact address for reporting vulnerabilities [8](#).

Guidance for the person filling this document (delete this box when done)

Is a policy page plus `security.txt` enough? The CRA does not say. We take the cautious reading: they are not enough on their own, because Article 13(17) also requires the contact to be easy to identify, to be in your user information, and to let users choose their means of communication, not only automated tools ^{9 10}. This is our reading of the official sources, not reviewed by a lawyer.

So do all three: the policy page, `security.txt`, and the contact printed in your user information (07-technical-documentation). Offer at least two different means, for example an email address plus a contact form or a phone number, and make sure a person reads them

¹¹.

1. Policy page (publish this)

Copy everything from “Policy text” to “Last updated” to **[Disclosure policy address]**. Replace the bracketed parts with your own wording.

Policy text: security and vulnerability disclosure at **[Organisation legal name]**

We want to hear about security problems in our products. This page explains how to report them and what you can expect from us.

Scope. **[Product name]**, versions **[Versions in support]**, and the online services these products depend on. [List anything out of scope, such as third-party services we do not control.]

How to report. Email **[Security contact email]**. If you prefer a form, use **[Security contact form]**. We read reports in these languages: **[Report languages]**. You can also report through the national CSIRT designated as coordinator in your country, and ask to remain anonymous ¹².

What to include. The product and version, what an attacker could do, steps to reproduce or a proof of concept, and how we can reach you. Please do not send personal data of other people.

What we do and when.

Step	Our commitment
Confirm that we received your report	Within [Acknowledgement time (business days)] business days
Keep you informed	At least at every change of status, until the fix ships
Coordinated disclosure window	[Disclosure window (calendar days)] calendar days from your report, or until a fix is available if that is sooner
Publish an advisory	When the fix is available, at [Advisory location]

Disclosure. Please keep the details private until a fix is available or the disclosure window has ended. If we need longer, we will explain why and agree a new date with you.

Credit. With your permission, we name you in the advisory.

Good-faith research. [Your safe-harbour statement: see the guidance box below.]

What we will not do. We will not ignore your report, share your identity without your consent, or ask you to stay silent forever.

What we ask. Do not access, change or delete other people's data. Do not degrade our services. Stop and tell us if you reach data that is not yours.

Last updated: [date].

Guidance for the person filling this document (delete this box when done)

Response times. The acknowledgement time and the disclosure window are your own commitments. The CRA asks for a CVD policy but sets no numbers for either [13](#). Pick an acknowledgement time you can keep when you are travelling or ill. A 90-day disclosure window is common industry practice, not a legal requirement; set what fits your release cycle.

Safe harbour. A safe-harbour clause promises researchers you will not take legal action against good-faith research. The CRA itself does not provide one, and national law on researchers' liability varies [14](#). Your wording **needs professional review**. A plain statement such as "We will not take legal action against good-faith research that follows this policy" is a common starting point; check it before you publish. If you cannot have it checked, leave the safe-harbour line out rather than promise more than you can keep.

2. security.txt

security.txt is a small text file at `/.well-known/security.txt` on your website. It tells researchers and tools where to report a vulnerability. Its format is defined by RFC 9116, an internet standard. The CRA's recitals encourage manufacturers to consider publishing their security policies in a machine-readable format [15](#).

Generate it. In your filled repository, run:

```
node tools/security-txt.mjs
```

The tool reads the `cvd` values from `workbook.json` and writes `/.well-known/security.txt`. Add `--stdout` to print the file instead of writing it. It stops with a message naming the field if a value is invalid, for example an `http:` address. Add `--sign` to print the command for signing the file with your OpenPGP key; the tool never signs for you. Upload the file to your web server and open the address in a browser to check it.

Fields.

Field	Required	What to put	Your value
Contact	Yes, one or more	mailto:, https: or tel: address	[Security contact email] and [Security contact form]
Expires	Yes	Date and time, less than a year ahead	Set by the tool, or your own date in cvd.security_txt_expires
Policy	No	Link to your policy page	[Disclosure policy address]
Preferred-Languages	No	Language codes	[Report languages]
Canonical	No	The file's own https: address	[security.txt address]
Encryption	No	Link to your OpenPGP key	Optional: cvd.encryption_url
Acknowledgments	No	Link to your thanks page	Optional: cvd.acknowledgments_url

No Git? Write the file by hand. Open a plain text editor, not Word. Copy the lines below and replace the example values with yours from the right-hand column. Keep one field per line and the exact spelling before each colon. Write `Expires` in this form, in UTC, less than a year ahead. Add one `Contact:` line per channel and delete the optional lines you do not use.

```
Contact: mailto:security@example.com
Contact: https://example.com/security/report
Expires: 2027-09-30T23:00:00Z
Policy: https://example.com/security/policy
Preferred-Languages: en, de
Canonical: https://example.com/.well-known/security.txt
```

Save it as `security.txt` with UTF-8 encoding and upload it to `/.well-known/` on your site.

Guidance for the person filling this document (delete this box when done)

Put a reminder in your calendar a month before `Expires`. An expired file tells researchers you may not be listening. Regenerate the file whenever your contact address changes.

3. Where to show your contact

Place	What to show
Policy page	Full policy (section 1)
<code>/.well-known/security.txt</code>	Contact, policy link, expiry
User information that comes with the product	Single point of contact and where to find the policy
Product itself, packaging or accompanying document	Your name, postal address and email or other digital contact
Website footer or “Security” page	Link to the policy

The user-information row comes from Annex II point 2 ¹⁶. The product row comes from Article 13(16), which asks for your name, postal address and a digital contact on the product, its packaging or an accompanying document ¹⁷.

4. Keep the evidence

Save a dated PDF or screenshot of the policy page and a copy of each `security.txt` you publish. Put them in `compliance/technical-file/02-design-development-vulnerability-handling.md`. They show that you provided a contact address and a CVD policy ¹⁸.

Send a test report to your own address every quarter. Write down the date and how long the acknowledgement took.

Worked examples

Worked example: WordPress plugin (ExampleForms Pro)

Example Plugins OÜ publishes the policy on its plugin site and links it from the plugin's `readme.txt` and the settings screen. It also enrolls ExampleForms Pro in Patchstack's free managed disclosure programme for plugin vendors and names it in the policy as a second reporting channel. Reports that arrive through Patchstack still go into the same vulnerability log.

Worked example: Desktop app (ExampleLedger)

Example Software SRL puts `security.txt` on the product domain and shows the security contact in the app's About box and in the app-store listings. The second channel is a contact form staffed by the support person, so users are not limited to email.

Worked example: IoT device firmware (ExampleThermo)

Example Devices GmbH puts `security.txt` on its company domain, because the device has no website of its own. The quick-start leaflet in the box prints the security contact and the policy address. The device's local status page shows the same contact.

1. Annex I Part II(5), Regulation (EU) 2024/2847 (Cyber Resilience Act) — <https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng> — verified 2026-10-05 ↗
2. Annex I Part II(6), Regulation (EU) 2024/2847 (Cyber Resilience Act) — <https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng> — verified 2026-10-05 ↗
3. Art. 13(17), Regulation (EU) 2024/2847 (Cyber Resilience Act) — <https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng> — verified 2026-10-05 ↗

4. Annex II point 2, Regulation (EU) 2024/2847 (Cyber Resilience Act) — <https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng> — verified 2026-10-05↵
5. Art. 13(17), Regulation (EU) 2024/2847 (Cyber Resilience Act) — <https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng> — verified 2026-10-05↵
6. Recital 63, Regulation (EU) 2024/2847 (Cyber Resilience Act) — <https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng> — verified 2026-10-05↵
7. Recital 76, Regulation (EU) 2024/2847 (Cyber Resilience Act) — <https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng> — verified 2026-10-05↵
8. Annex VII point 2(b), Regulation (EU) 2024/2847 (Cyber Resilience Act) — <https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng> — verified 2026-10-05↵
9. Art. 13(17), Regulation (EU) 2024/2847 (Cyber Resilience Act) — <https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng> — verified 2026-10-05↵
10. Annex II point 2, Regulation (EU) 2024/2847 (Cyber Resilience Act) — <https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng> — verified 2026-10-05↵
11. Recital 63, Regulation (EU) 2024/2847 (Cyber Resilience Act) — <https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng> — verified 2026-10-05↵
12. Recital 76, Regulation (EU) 2024/2847 (Cyber Resilience Act) — <https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng> — verified 2026-10-05↵
13. Annex I Part II(5), Regulation (EU) 2024/2847 (Cyber Resilience Act) — <https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng> — verified 2026-10-05↵
14. Recital 75, Regulation (EU) 2024/2847 (Cyber Resilience Act) — <https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng> — verified 2026-10-05↵
15. Recital 76, Regulation (EU) 2024/2847 (Cyber Resilience Act) — <https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng> — verified 2026-10-05↵
16. Annex II point 2, Regulation (EU) 2024/2847 (Cyber Resilience Act) — <https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng> — verified 2026-10-05↵
17. Art. 13(16), Regulation (EU) 2024/2847 (Cyber Resilience Act) — <https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng> — verified 2026-10-05↵
18. Annex VII point 2(b), Regulation (EU) 2024/2847 (Cyber Resilience Act) — <https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng> — verified 2026-10-05↵