A CRA ANNEX I REQUIREMENT, DONE FOR YOU

# The CVD policy the CRA demands, *ready to adapt.*

Copy-paste policy text plus the 24h/72h/14-day reporting playbook every manufacturer of connected products needs under the EU Cyber Resilience Act.

This document gives product security teams two ready-to-use resources in one: a coordinated vulnerability disclosure (CVD) policy that meets the Annex I, Part II requirements of the EU Cyber Resilience Act, and a step-by-step reporting playbook for the mandatory authority notifications that apply from 11 September 2026. Adapt the template sections — every field marked with a dotted line is yours to fill — then publish and rehearse before the go-live date.

**Guidance, not legal advice.** This template is provided as practical compliance assistance. It does not constitute legal advice. Review with qualified counsel before publication, particularly if your products are sold across multiple EU member states.

© 2026 CRA Facts · cra-facts.com

CONTENTS

00

# Why the CRA requires CVD

The legal basis, the two distinct duties, and what happens if you ignore them.

## Why the CRA requires *coordinated disclosure*

The EU Cyber Resilience Act, which entered into force in December 2024, imposes binding cybersecurity obligations on manufacturers who place products with digital elements on the European market. Among those obligations is a requirement that often surprises legal teams who are still focused on the conformity assessment provisions: manufacturers must actively manage how vulnerabilities in their products are discovered, received, and reported — not just patched.

Annex I, Part II, item 5 of the CRA states that manufacturers shall "put in place and enforce a policy on coordinated vulnerability disclosure" and shall "provide a contact address for the reporting of vulnerabilities." This is not a soft recommendation. It is a mandatory essential requirement, sitting alongside the core security-by-design rules in Part I.

**WHAT ANNEX I, PART II ACTUALLY SAYS**

**Part II — Vulnerability handling requirements** applies to manufacturers of all products with digital elements except certain legacy and bespoke categories. Item 5 reads, in full:

"Manufacturers shall put in place and enforce a policy on coordinated vulnerability disclosure and shall provide a contact address for the reporting of vulnerabilities discovered in the product with digital elements."

Separately, Article 14 of the CRA requires manufacturers to report actively exploited vulnerabilities and severe incidents to national authorities via ENISA's Single Reporting Platform — a distinct and time-bound obligation that sits alongside the CVD policy.

### Two distinct strands — one document covers both

Manufacturers face **two related but separate duties**. Conflating them is one of the most common compliance mistakes.

**STRAND 1 · CHAPTERS 01–02**

#### Your standing CVD policy

A published document that tells security researchers how to report vulnerabilities, what you commit to doing, and on what timeline. Required by Annex I, Part II(5). Must be live before your product goes to market.

**STRAND 2 · CHAPTER 03**

#### Mandatory authority reporting

Time-bound notifications to national CSIRTs and ENISA when you discover or are informed of an actively exploited vulnerability or a severe incident. Required by Article 14. Applies from 11 Sep 2026.

Your CVD policy answers the question: "How can researchers tell you about a bug, and what will you do?" The mandatory reporting duty answers a different question: "When something is actively being exploited, which government bodies must you notify, and how fast?"

Both require preparation before the September 2026 enforcement date. Both are covered in this document.

## Who this applies to

The CRA's vulnerability handling requirements apply to all manufacturers that place products with digital elements on the EU market — regardless of where the manufacturer is established. If you sell a connected product, a software product, or a product containing software to customers in the EU, the CRA applies to you. Micro-enterprises (fewer than 10 employees and under €2M turnover) face somewhat reduced administrative requirements under Article 14, but the CVD policy obligation in Annex I, Part II applies to all manufacturers without exception.

Open-source software stewards who do not commercialise their software are explicitly excluded from the manufacturer definition, though they face a lighter set of obligations as "stewards."

**SCOPE CHECK**

If you manufacture any of the following, the CRA applies: consumer IoT devices, industrial control systems, network equipment, operating systems, hypervisors, applications handling personal data, and any other software or hardware product with a network interface or the ability to process data from external sources. The list of "important" and "critical" products subject to stricter conformity assessment is in Annex III and Annex IV.

CHAPTER 00 CHECKLIST

---

- [ ] **Annex I, Part II confirmed** You have read and located the CVD requirement in your copy of the CRA text.
- [ ] **Scope confirmed** Legal or compliance team has confirmed your products fall within the CRA's scope.
- [ ] **Two duties distinguished** Your team understands that the standing CVD policy and the Article 14 reporting duty are separate obligations.

# 01

# Your CVD policy — the template

Real, adaptable policy text your team can publish. Fill the dotted fields, review with counsel, go live.

## Your CVD policy — *the template*

The policy below is designed to be published on your website (typically at `/security` or `/vulnerability-disclosure`) and linked from your `security.txt` file. It fulfils the Annex I, Part II(5) requirement and sets expectations for the security research community. Read through the whole thing before filling in the fields — some sections may need adjustment depending on your product portfolio, legal jurisdiction, and internal SLA capacity.

> **HOW TO USE THIS TEMPLATE**
>
> Every field marked with a dotted line is a placeholder. The label on the left tells you what to insert. Once filled, remove the labels. The body text in each section is designed to be used as written, but you are encouraged to adapt the tone to match your company voice. Have legal review the safe-harbour clause (§4) before publishing.

## Scope

TEMPLATE

# Coordinated Vulnerability Disclosure Policy

COMPANY / ORGANISATION NAME .....

WEBSITE URL WHERE THIS POLICY IS PUBLISHED .....

EFFECTIVE DATE .....

VERSION NUMBER .....

### 1. Scope

This policy applies to security vulnerabilities discovered in the following products and services manufactured or operated by

COMPANY NAME .....

(hereinafter “we,” “our,” or “the company”):

PRODUCT LINE 1 — NAME AND VERSION RANGE COVERED .....

PRODUCT LINE 2 — NAME AND VERSION RANGE COVERED .....

ADDITIONAL PRODUCTS OR SERVICES — OR WRITE 'ALL CURRENT PRODUCTS LISTED AT [URL]' .....

Vulnerabilities in third-party components integrated into our products should be reported directly to the relevant upstream vendor unless they manifest specifically in our implementation. Where you are unsure, please report to us and we will coordinate upstream disclosure.

## How to report

TEMPLATE

### Reporting channel and contact information

**2. How to report a vulnerability**

We welcome reports from security researchers, customers, and members of the public. Please submit your report using one of the following channels:

- **Email:**

  SECURITY@ OR PSIRT@ ADDRESS

- **Web form:**

  URL OF WEB FORM, OR 'NOT AVAILABLE'

- **PGP-encrypted email:** Our public key is available at

  URL OR KEY SERVER LINK

- **Key fingerprint:**

  FULL 40-CHARACTER PGP FINGERPRINT

Our `security.txt` file at `https://`

YOUR DOMAIN

`/.well-known/security.txt` lists these details in machine-readable form.

## What to include in a report

TEMPLATE

### Report contents guidance

**3. What to include**

To help us triage your report efficiently, please include:

- The affected product name and version number
- A description of the vulnerability type (e.g. buffer overflow, authentication bypass, hardcoded credential)
- Steps to reproduce the issue, or a proof-of-concept (where safe to share)
- The potential impact, including what an attacker could achieve if the vulnerability were exploited
- Whether you believe the vulnerability is already known or actively exploited
- Your preferred contact method for follow-up questions
- Whether you wish to be publicly credited when the vulnerability is disclosed

You do not need a full exploit to submit a report. Incomplete reports are always welcome — we may ask follow-up questions.

## Safe harbour

TEMPLATE

### Good-faith safe harbour

**4. Safe harbour — good-faith security research**

We consider vulnerability research conducted in good faith to be authorised and valuable. If you act in accordance with this policy, we commit that:

- We will not pursue, initiate, or support civil or criminal legal action against you in connection with your research.
- We will not file a complaint to law enforcement about your research activities.
- We will work with you cooperatively to understand and address the vulnerability.

“Good faith” means you: act with the intent to identify and report vulnerabilities, avoid accessing data beyond what is necessary to confirm the vulnerability exists, do not exploit the vulnerability for any purpose other than demonstrating impact to us, do not publicly disclose the vulnerability before we have had a reasonable opportunity to remediate it, and do not take actions that affect the availability of our services to other users.

This safe-harbour statement does not authorise conduct that is prohibited by laws other than those directly related to unauthorised computer access, such as laws governing privacy, fraud, or export controls.

## Commitments and response targets

TEMPLATE

### Our commitments and SLA targets

#### 5. Our commitments and response targets

We commit to the following response targets from the date of receipt of a valid vulnerability report:

ACKNOWLEDGEMENT WITHIN X BUSINESS DAYS (E.G. 2)

INITIAL TRIAGE AND SEVERITY ASSESSMENT WITHIN X BUSINESS DAYS (E.G. 5)

STATUS UPDATE (REMEDIATION PLAN OR FIX TIMELINE) WITHIN X CALENDAR DAYS (E.G. 30)

FIX AVAILABILITY TARGET — E.G. 'WITHIN 90 DAYS FOR CRITICAL, 180 DAYS FOR HIGH'

We will keep you informed of progress at regular intervals, even if we cannot share technical details during the remediation process. If we anticipate that our remediation timeline will exceed the coordinated disclosure window, we will contact you proactively to discuss an extension.

## Coordinated disclosure timeline

TEMPLATE

### Coordinated disclosure timeline

**6. Coordinated disclosure timeline**

We follow a coordinated disclosure model. The standard timeline from confirmed report receipt is:

MAXIMUM EMBARGO PERIOD — E.G. 90 DAYS FOR CRITICAL, 120 DAYS FOR HIGH SEVERITY

At the end of the embargo period, we will publish a security advisory unless:

- A fix has already been released and you have agreed to a shorter timeline, or
- We have mutually agreed to extend the embargo due to exceptional circumstances (e.g. the vulnerability requires a complex supply-chain fix).

If a vulnerability is already being actively exploited before the embargo expires, we reserve the right to publish a security advisory immediately, in coordination with you where possible.

We will notify you at least

X DAYS — E.G. 7

before public disclosure so you have time to prepare.

## Recognition

TEMPLATE

### Researcher recognition

**7. Recognition and credit**

We maintain a public security acknowledgements page at:

URL OF ACKNOWLEDGEMENTS PAGE

If you discover a valid vulnerability and wish to be credited, please indicate this in your report and provide the name or alias you would like to appear. We will credit you by name (or pseudonym) in our security advisory and on the acknowledgements page unless you ask to remain anonymous.

We do not currently operate a financial bug bounty programme. Researchers are recognised through public acknowledgement only.

- [ ] **Scope list finalised** All products within CRA scope are named or referenced by URL.
- [ ] **Contact address active** The security@ or psirt@ inbox is live and monitored.
- [ ] **PGP key published** Key fingerprint is accurate and the key is available at the stated URL or key server.
- [ ] **Safe-harbour clause reviewed** Legal has reviewed the safe-harbour text for your jurisdiction.
- [ ] **SLA targets agreed internally** Product security team has signed off on the response target days and can operationally meet them.
- [ ] **Acknowledgements page exists** The URL in section 7 resolves and is maintained.

# 02

## Publish a security.txt

The machine-readable signpost that tells researchers — and scanners — exactly where to send reports.

## Publish a *security.txt*

`security.txt` (RFC 9116) is a plain-text file that lives at a well-known path on your web server. It tells security researchers — and the automated scanners they use — exactly where to report vulnerabilities, who the contact is, when the file expires, and where your full CVD policy is published. Major vulnerability databases and coordination centres query it routinely.

Publishing `security.txt` is not strictly mandated by the CRA text, but it is the standard technical implementation of the "contact point for reporting" that Annex I, Part II(5) requires. Without it, researchers have no reliable way to find your contact details, and reports are far more likely to go to the wrong place, arrive publicly on social media, or not arrive at all.

### Where it lives

The file must be placed at exactly this path:

`https://[yourdomain]/.well-known/security.txt`

If you operate multiple domains for different products, you should publish a `security.txt` on each one, pointing back to the same central security contact. The `.well-known` directory is a standardised namespace defined by RFC 8615; your web server must be configured to serve files from it.

### What to put in it

RFC 9116 defines a small set of fields. The `Contact` and `Expires` fields are **required**. All others are optional but strongly recommended for CRA compliance purposes.

## SECURITY.TXT — READY TO EDIT

```
# Security contact for [Company Name]
# RFC 9116 · https://securitytxt.org

Contact: mailto:security@
```

**YOUR DOMAIN**

```
Contact: https://
```

**YOUR DOMAIN/SECURITY OR WEB FORM URL**

```
Expires:
```

**ISO 8601 DATE ONE YEAR FROM NOW — E.G. 2027-09-01T00:00:00.000Z**

```
Encryption: https://
```

**URL TO YOUR PGP PUBLIC KEY FILE**

```
Policy: https://
```

**URL TO YOUR PUBLISHED CVD POLICY — E.G. HTTPS://EXAMPLE.COM/SECURITY**

```
Acknowledgments: https://
```

**URL TO YOUR ACKNOWLEDGEMENTS / HALL-OF-FAME PAGE**

```
Preferred-Languages:
```

**BCP 47 LANGUAGE TAGS — E.G. EN, DE, FR**

```
# Canonical location of this file:
Canonical: https://
```

**YOUR DOMAIN**

```
/.well-known/security.txt
```

FIELD NOTES

**Contact:** You may list multiple `Contact:` lines in order of preference. Email is universal; a web form is useful for researchers who prefer structured submission.

**Expires:** RFC 9116 requires this field and warns that stale files should not be trusted. Set a calendar reminder to refresh it annually — or automate the rotation.

**Encryption:** Link directly to the ASCII-armored public key file (`.asc`), not a key-server search page. Key-server URLs can change; a hosted file on your own domain is more reliable.

**Preferred-Languages:** List all languages in which your security team can receive and respond to reports. This helps international researchers choose the right language upfront.

## Signing your security.txt

RFC 9116 allows (and recommends) that the `security.txt` file be signed with your PGP key. This provides researchers with cryptographic assurance that the file has not been tampered with. To sign:

1. Create and verify the `security.txt` content.
2. Run: `gpg --clearsign security.txt` — this produces `security.txt.asc`.
3. Upload `security.txt.asc` as your `/.well-known/security.txt`.
4. The signed format wraps the content in `-----BEGIN PGP SIGNED MESSAGE-----` headers; RFC 9116 parsers handle this correctly.

HANDS-ON · 30 MIN

**Get your security.txt live today.** Fill the template above with your real values. Create a `.well-known/` directory in your web root if it does not exist. Upload the file. Test with `curl https://[yourdomain]/.well-known/security.txt` — you should see the file contents returned with a `200 OK` status, not a redirect. Also verify it at securitytxt.org using the built-in validator.

CHAPTER 02 CHECKLIST

- [ ] **security.txt drafted** All required and recommended fields completed with real values.
- [ ] **File deployed** Accessible at /.well-known/security.txt with HTTP 200 on all product domains.
- [ ] **Expires date set** Date is no more than one year from today; calendar reminder created for renewal.
- [ ] **PGP key URL resolves** The Encryption: URL returns the correct public key in ASCII-armored format.
- [ ] **Signed version uploaded** File is PGP-signed and the signature verifies against your published key.

- [ ] **Validator passed** securitytxt.org or equivalent confirms the file parses without errors.

# 03

# The mandatory reporting duty

24 hours. 72 hours. 14 days. Three deadlines, one platform, zero margin for guessing.

## The mandatory reporting *duty*

From 11 September 2026, the CRA's Article 14 obligations become enforceable. Any manufacturer placing products with digital elements on the EU market must report two categories of event to national authorities via ENISA's Single Reporting Platform (SRP):

- **Actively exploited vulnerabilities:** any vulnerability in your product that you discover or are credibly informed is being actively exploited in the wild — regardless of severity.
- **Severe incidents:** security incidents that have, or may have, a significant impact on the provision of your product in the internal market.

The SRP is designed as a single-entry reporting point: you file once, and ENISA routes the report to your national CSIRT (Computer Security Incident Response Team) automatically. You do not need to identify and contact your national CSIRT separately.

**GO-LIVE DATE: 11 SEPTEMBER 2026**

Article 14 reporting obligations and the SRP become mandatory on **11 September 2026**, the date the CRA's vulnerability handling provisions apply. Manufacturers who have not registered on the SRP or identified their responsible national CSIRT by that date risk being in immediate breach. Register early — see Chapter 04 for the action item.

### The three-tier timeline

The CRA sets a strict, tiered notification schedule. Each tier adds more detail. The clock starts when you become aware of the actively exploited vulnerability or severe incident — not when you have a fix ready.

1 **Early warning — within 24 hours**

Notify ENISA via the SRP that you are aware of an actively exploited vulnerability or severe incident. Include: product name and version, the nature of the issue, whether it is already publicly known, and any interim mitigation available. No root-cause analysis is required at this stage — this is a signal, not a full report.

2 **Notification — within 72 hours**

Submit an updated notification with more detail: technical description of the vulnerability or incident, affected user population estimate, evidence of exploitation observed, CVE identifier if assigned, and actions taken or planned. This replaces or supplements the early warning on the SRP.

3 **Final report — within 14 days (or 1 month for severe incidents)**

Submit a comprehensive final report including: full technical analysis, root cause if known, complete mitigation and remediation actions, coordinated disclosure timeline (including whether a CVE has been issued and a security advisory published), and any relevant information for other manufacturers who may be affected by the same vulnerability.

## One report reaches two authorities

A single submission on the SRP simultaneously fulfils your reporting obligation to both ENISA and to your responsible national CSIRT. ENISA operates the SRP as a pan-EU coordination hub. Your national CSIRT is determined by where your company is established, or — for non-EU manufacturers — by the EU market where you have the most significant presence or where your authorised representative is established.

If you are a micro-enterprise (fewer than 10 employees and under €2M annual turnover), you will not be fined for missing the 24-hour early warning deadline. However, the 72-hour and 14-day obligations still apply, and the 24-hour best-effort expectation remains. Open-source software stewards who are not commercial manufacturers are not subject to Article 14 at all.

## Early warning message template

TEMPLATE

# Article 14 Early Warning — 24-hour notification

**Report type:** Early Warning (Article 14, CRA) **Submitted via:** ENISA Single Reporting Platform

MANUFACTURER LEGAL NAME .....

MANUFACTURER REGISTERED ADDRESS / EU AUTHORISED REPRESENTATIVE .....

CONTACT NAME AND ROLE (E.G. CISO, HEAD OF PRODUCT SECURITY) .....

CONTACT EMAIL AND PHONE .....

## Product information:

PRODUCT NAME AND MODEL NUMBER .....

AFFECTED VERSION(S) .....

CRA PRODUCT CATEGORY (E.G. 'IMPORTANT — CLASS I', OR 'OTHER') .....

## Nature of the vulnerability or incident:

BRIEF DESCRIPTION — VULNERABILITY TYPE OR INCIDENT CATEGORY (1-3 SENTENCES) .....

IS THIS VULNERABILITY ALREADY PUBLICLY KNOWN? YES / NO / UNKNOWN .....

CVE IDENTIFIER, IF ALREADY ASSIGNED .....

## Evidence of exploitation:

SUMMARY OF EXPLOITATION EVIDENCE — E.G. 'OBSERVED IN THREAT INTELLIGENCE FEEDS', 'CUSTOMER REPORTED ACTIVE ATTACK', 'INTERNAL TELEMETRY' .....

## Affected users:

ESTIMATED NUMBER OR RANGE OF AFFECTED END USERS OR DEPLOYED INSTANCES .....

ANY CROSS-BORDER IMPACT WITHIN THE EU? IF SO, WHICH MEMBER STATES ARE AFFECTED .....

## Mitigation:

NOTIFICATION TO USERS — PLANNED OR ISSUED, AND WHEN .....

REMEDIATION — PATCH AVAILABLE, WORKAROUND, OR NONE AVAILABLE AT THIS TIME' .....

**WHAT HAPPENS AFTER YOU REPORT**

Once your early warning is received, ENISA and your national CSIRT may reach out with questions or guidance. They are in coordination mode, not enforcement mode, at this early stage — their goal is to understand the threat landscape and coordinate cross-border response if the vulnerability affects products across multiple member states. You are not required to have a fix ready before filing. Filing late or not filing is the enforcement risk.

## CHAPTER 03 CHECKLIST

- [ ] **SRP account created** Your organisation is registered on ENISA's Single Reporting Platform before 11 Sep 2026.
- [ ] **National CSIRT identified** You know which CSIRT is responsible for your organisation based on your EU establishment or authorised representative.
- [ ] **24h escalation path defined** Internal process documented: who discovers, who decides, who files, in under 24 hours.
- [ ] **Early warning template ready** The template above is pre-filled with your organisation's static data and accessible to the on-call team.
- [ ] **Micro-enterprise status checked** Legal has confirmed whether you qualify for the reduced 24h penalty exemption — and documented the finding.
- [ ] **Playbook rehearsed** At least one tabletop exercise has tested the 24h / 72h / 14-day timeline with named individuals.

# 04

# Checklist & next steps

Six actions that make the difference between a policy that lives in a drawer and one that protects you on audit day.

## Checklist & *next steps*

Compliance with the CRA's CVD requirements is not a one-time project — it is an operational programme. The policy template gives you the legal artefact. The security.txt gives researchers the signpost. The reporting playbook gives your team a clear process under pressure. What follows is the master checklist that ties them together.

A good way to use this chapter: assign each item to a named owner with a deadline, and track it in your product security backlog. Review the whole checklist quarterly, since product releases, contact changes, and regulatory updates can make previously complete items stale.

MASTER CVD COMPLIANCE CHECKLIST

---

- [ ] **CVD policy published** The policy from Chapter 01 is live on your website, reviewed by legal, and linked from your homepage footer or /security page.
- [ ] **Security contact point active** The email address (and optional web form) in your policy is monitored by a named individual or on-call rotation with an SLA for first response.
- [ ] **security.txt deployed and validated** The file at /.well-known/security.txt on all product domains passes RFC 9116 validation and is signed with your PGP key.
- [ ] **SRP registered** Your organisation has an active account on ENISA's Single Reporting Platform and at least two staff members have login access.
- [ ] **National CSIRT identified and documented** You know your responsible CSIRT, have their contact details on file, and have tested that contact at least once.
- [ ] **24h/72h/14-day playbook rehearsed** A tabletop exercise has been run with the product security team, engineering lead, and communications contact. Findings are documented and actioned.

GO FURTHER WITH CRA FACTS

## Turn compliance into a competitive edge.

These six items are the minimum. The CRA Facts documentation library goes further — covering technical file preparation, conformity assessment routes for Class I and Class II products, post-market surveillance, and the Article 13 notification obligations that sit alongside Article 14.

**Read the full CRA Facts documentation:**
cra-facts.com/documentation

**Sign up for The CRA Brief** — the weekly briefing that tracks enforcement guidance, ENISA SRP updates, and CEN/CENELEC standard publications:

cra-facts.com

QUICK NAVIGATION

# Jump to any chapter

Click a tile to go directly to that section.



Questions? Reach the CRA Facts team at cra-facts.com — or subscribe to The CRA Brief for weekly updates as Article 14 guidance evolves.

Read the documentation →

Visit cra-facts.com →

CRA Facts

# CVD policy published.

# Playbook ready.

## *September 2026 is not far away.*

cra-facts.com

© 2026 CRA FACTS · CRA-FACTS.COM