CRA SAMPLE

D14 Coordinated vulnerability disclosure policy

Blank template · Nordwald Wärmetechnik GmbH, networked wood chip boiler NWT HACKTHERM 60 connect

Publisher	OT-Cyber.de, Max Gilg, Rosenheim
Sample company	Nordwald Wärmetechnik GmbH, networked wood chip boiler NWT HACKTHERM 60 connect (fictitious)
Note	Free sample, not legal advice

Fill in the fields, approve with date and signature, file according to document control.

1 Purpose and scope

How third parties report vulnerabilities to us, how we respond and when we publish. Published at nordwald-waerme.example/security with security.txt (Annex I, Part II, points (5) and (6)).

How to fill in this form

Fill in the fields with the details of your company. Below each table and next to each field there is an example from the sample company for orientation. Refer to evidence by number (e.g. ticket or form). Finally approve with date and signature and file according to document control.

2 Document control

Field	Entry
Document no.	
Version, status	
Scope	
Author	
Checked by	
Approval	
Next review	
Confidentiality	
Filing	

3 Coordinated vulnerability disclosure policy: overview

Field	Entry	Example from the sample
Scope		Boilers, gateway, portal, app and all Nordwald …
Contact		psirt@nordwald-waerme.example, encrypted with …
Acknowledgement of receipt		within 2 working days
Initial assessment		within 7 days
Remediation		critical 7 days, high 30 days, medium 90 days, …
Publication		after the update is available, coordinated with …

Field	Entry	Example from the sample
Protection of reporters		No legal action for reports made in good faith, …

4 External reports since entry into force

Received	From	Subject	Acknowledged	Outcome

Example row from the sample: Received: 22.05.2027 · From: Researcher · Subject: Portal: guessable user name · Acknowledged: 23.05.2027 · Outcome: fixed, NWT-VULN-2027-003

Describe your status here, specifically and with a date. Example from the sample: All three reports were acknowledged within the deadlines.

5 Terms and abbreviations

CE: CE marking: the manufacturer declares that the product meets EU requirements

CRA: Cyber Resilience Act, Regulation (EU) 2024/2847

NWT: abbreviation of the sample company in document and ticket numbers

SA: security advisory to users (number range)

TLS: encryption of the connection

VULN: vulnerability ticket (number range)

6 Revision history and approval

Version	Date	Change	Approval

Approved (name, function, date, signature): _____ · Free sample from OT-Cyber.de, not legal advice. Company, persons, serial numbers and data are entirely fictitious.