CRA SAMPLE

D14 Coordinated vulnerability disclosure policy

Example after one year of operation, status 11.12.2027 · 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

Company, people, data and numbers are fictitious. This is how the document looks after one year of operation.

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)).

2 Document control

Field	Entry
Document no.	NWT-CE-D14
Version, status	1.2, approved
Scope	NWT HACKTHERM 60 connect (18 to 60 kW), controller, gateway, portal and app
Author	Jonas Weiß, Engineering and Product Security (PSO)
Checked by	Ingenieurbüro Lechner (safety), Sichtwerk Security (security)
Approval	Michael Berger, Managing Director, 11.12.2027
Next review	15.03.2029 or in the event of a substantial modification
Confidentiality	internal
Filing	Technical documentation NWT-TD-HT60C, retained for at least 10 years after the last unit is placed on the market

3 Coordinated vulnerability disclosure policy: overview

Scope: Boilers, gateway, portal, app and all Nordwald web services

Contact: psirt@nordwald-waerme.example, encrypted with the published key; form in the portal

Acknowledgement of receipt: within 2 working days

Initial assessment: within 7 days

Remediation: critical 7 days, high 30 days, medium 90 days, with a status update every 14 days

Publication: after the update is available, coordinated with the reporter, credited on request

Protection of reporters: No legal action for reports made in good faith, without causing damage and without accessing third-party data

4 External reports since entry into force

Received	From	Subject	Acknowledged	Outcome
22.05.2027	Researcher	Portal: guessable user name	23.05.2027	fixed, NWT-VULN-2027-003

Received	From	Subject	Acknowledged	Outcome
09.09.2027	Customer	App shows outdated firmware	10.09.2027	no vulnerability, display corrected
14.01.2028	Researcher	Gateway: TLS setting	15.01.2028	fixed, NWT-VULN-2028-001

All three reports were acknowledged within the deadlines. The researcher who submitted the first report is credited in security advisory NWT-SA-2027-001.

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
1.0	15.03.2027	First issue for placing on the market (CE)	M. Berger
1.1	05.07.2027	Response deadlines clarified after first external report	M. Berger
1.2	11.12.2027	Aligned with full CRA application	M. Berger

Approved: Michael Berger, Managing Director, 11.12.2027 (signed in the original). Free sample from OT-Cyber.de, not legal advice. Company, persons, serial numbers and data are entirely fictitious.