CRA SAMPLE

D16 Emergency card: reporting under Article 14 CRA

Example after one year of operation, status 28.02.2028 · 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

One page for an emergency: when to report, deadlines, access, roles and what every report must contain. It is posted in the office and stored on the on-call phone.

2 Document control

Field	Entry
Document no.	NWT-CE-D16
Version, status	1.3, 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, 28.02.2028
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 Emergency card: reporting under Article 14 CRA: overview

What	Deadline	Content
Early warning	24 h from awareness	affected product, suspicion, Member States
Notification	72 h from awareness	nature of vulnerability, exploitation, measures, severity
Final report, vulnerability	14 days after remedy	description, cause, update
Final report, incident	1 month after notification	cause, impact, remedy
Inform users	without undue delay	risk, remedy, what users should do

✓ Reportable: actively exploited vulnerability or severe security incident affecting the product. Actively exploited means there is reliable evidence that someone has exploited the vulnerability, including at other operators

✓ Recipient: BSI as coordinating CSIRT, via the ENISA single reporting platform

✓ Third party component affected: its manufacturer is informed immediately (Article 13(6) CRA)

✓ Access: ENISA single reporting platform, accounts Weiß and Berger, credentials kept in the vault

✓ Who reports: PSO J. Weiß, deputy M. Berger; Sichtwerk provides support

✓ Documentation: time of awareness and every report with its reference recorded in F06

✓ Microenterprises: no fine for missing the 24 h deadline, the obligation remains (Article 64(10) CRA)

Exercise or case	Date	Result
Reporting exercise with Sichtwerk	28.09.2027	Early warning after 1 h 50 min, lesson learned on access route
Real report NWT-VULN-2027-006	14.10.2027	all deadlines met (F06)

4 Terms and abbreviations

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

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

CSIRT: national computer security incident response team, receives the reports

ENISA: EU Agency for Cybersecurity, runs the single reporting platform under the CRA

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

PSO: product security officer

VULN: vulnerability ticket (number range)

5 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	05.10.2027	After reporting exercise: access route to the ENISA platform clarified	M. Berger
1.2	20.10.2027	After real report (F06): content checklist extended	M. Berger
1.3	28.02.2028	Added definition of actively exploited, recipients and notification of component manufacturers	M. Berger

Approved: Michael Berger, Managing Director, 28.02.2028 (signed in the original). Free sample from OT-Cyber.de, not legal advice. Company, persons, serial numbers and data are entirely fictitious.