CRA SAMPLE

D08 Process manual

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

20 processes for a two-person company working with partners, stating owner, frequency and record, with evidence that each process was carried out in the first year of series production.

2 Document control

Field	Entry
Document no.	NWT-CE-D08
Version, status	1.4, 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 Process manual: overview

P	Process	Owner	Frequency	Record	Practised 03/2027 to 02/2028
P01	Regulatory and standards monitoring	Berger	monthly	D01	12 monthly reports
P02	Requirements management	Weiß	per release	F01	5 releases checked
P03	Secure development	Weiß	per release	F14	5 approvals, 1 pentest
P04	Safety validation	Weiß	on change	F09	1 signature check
P05	Components and suppliers	Weiß	annually	F02	Assessment 11/2027
P06	SBOM	Datenwerk	per release	F04	5 SBOM versions
P07	Vulnerability handling	Weiß	ongoing	F05	7 tickets
P08	Coordinated vulnerability disclosure	Weiß	ongoing	D14	3 external reports

P	Process	Owner	Frequency	Record	Practised 03/2027 to 02/2028
P09	Reporting under Article 14	Weiß	on event	F06	1 report, 1 drill
P10	Security advisories to users	Weiß	per case	F07	4 advisories
P11	Update provision	Datenwerk	per release	F14	5 staged rollouts
P12	Change management	Weiß	per change	F08	9 requests
P13	Routine testing	Hofer	per unit	F10	34 reports
P14	Commissioning	Berger	per installation	F11	31 reports
P15	Market monitoring	Berger	quarterly	Monitoring report	4 reports
P16	Corrective actions	Berger	as required	F13	1 case
P17	Training	Berger	annually	F12	6 training sessions
P18	Document control	Berger	ongoing	D09	Review 02/2028
P19	Support period	Berger	annually	D15	Review 12/2027
P20	Decommissioning	Weiß	as required	D13	0 cases, procedure rehearsed

Legend: P = process.

Annual review 05.02.2028: All scheduled processes were carried out. P07 was the most demanding process (7 tickets, one of them an actively exploited vulnerability). Improvement: since 1.5.0, Datenwerk delivers the SBOM in machine-readable form with every release, and the check for known vulnerabilities runs automatically every day.

4 The processes in detail

4.1 P01 Regulatory and standards monitoring

Purpose: Ensure the legal and standards basis is current before anything is declared or delivered

Owner: Berger · **Frequency:** monthly · **Record:** D01 · **Practised 03/2027 to 02/2028:** 12 monthly reports

Procedure:

1. Check the Official Journal, ENISA, BSI, CEN/CENELEC and industry associations monthly for changes
2. Assess the impact on boiler, gateway and declaration
3. Update D01, adjust the list of standards
4. Record the result in the monthly report, inform Weiß

4.2 P02 Requirements management

Purpose: Make every legal, standards, safety and security requirement traceable

Owner: Weiß · **Frequency:** per release · **Record:** F01 · **Practised 03/2027 to 02/2028:** 5 releases checked

Procedure:

1. Record each requirement with ID and source in F01
2. Assign architecture, test and evidence
3. Before each release, verify that every requirement is met and evidenced

4.3 P03 Secure development

Purpose: Develop gateway, portal and app in accordance with IEC 62443-4-1 (CRA Annex I, Part I)

Owner: Weiß · **Frequency:** per release · **Record:** F14 · **Practised 03/2027 to 02/2028:** 5 approvals, 1 pentest

Procedure:

1. Review threat model D07 for each release
2. Code review and static analysis at Datenwerk
3. Vulnerability scan and interface testing before each release
4. Pentest by Sichtwerk before each major version, approval in F14

4.4 P04 Safety validation

Purpose: Safety functions SF1 to SF10 remain effective after every change (EN ISO 13849)

Owner: Weiß · **Frequency:** on change · **Record:** F09 · **Practised 03/2027 to 02/2028:** 1 signature check

Procedure:

1. Assess changes to the safety-related part for impact (Lechner)
2. Test the affected safety function with fault injection
3. Compare the signature of the F program
4. Record the result in F09, approval by Weiß

4.5 P05 Components and suppliers

Purpose: Third-party components must not compromise cybersecurity (Article 13(5) CRA)

Owner: Weiß · **Frequency:** annually · **Record:** F02 · **Practised 03/2027 to 02/2028:** Assessment 11/2027

Procedure:

1. Classify components by criticality
2. Request evidence: declaration, SBOM, support commitment

3. Assessment in F02, contract with reporting obligation (F03)

4. Reassess annually and after every security notification

4.6 P06 SBOM

Purpose: Document the components and dependencies of every firmware version (Annex I, Part II, point (1))

Owner: Datenwerk · **Frequency:** per release · **Record:** F04 · **Practised 03/2027 to 02/2028:** 5 SBOM versions

Procedure:

1. Generate the SBOM automatically in the build (Datenwerk)

2. Check against vulnerability databases

3. Approve the SBOM in F04, no release without an approved SBOM

4.7 P07 Vulnerability handling

Purpose: Identify, assess and remediate vulnerabilities without delay (Annex I, Part II)

Owner: Weiß · **Frequency:** ongoing · **Record:** F05 · **Practised 03/2027 to 02/2028:** 7 tickets

Procedure:

1. Open a ticket in F05, triage on the same working day

2. Assess severity by CVSS and relevance to safety

3. If actively exploited, start P09 immediately

4. Remediate via P11, inform users via P10

4.8 P08 Coordinated vulnerability disclosure

Purpose: Receive third-party reports and publish in coordination (Annex I, Part II, points (5) and (6))

Owner: Weiß · **Frequency:** ongoing · **Record:** D14 · **Practised 03/2027 to 02/2028:** 3 external reports

Procedure:

1. Receipt via the point of contact defined in D14, acknowledgement within 3 working days

2. Agree timing and content with the reporter

3. Handling in accordance with P07, publication after remediation

4.9 P09 Reporting under Article 14

Purpose: Report actively exploited vulnerabilities and severe incidents within the deadlines

Owner: Weiß · **Frequency:** on event · **Record:** F06 · **Practised 03/2027 to 02/2028:** 1 report, 1 drill

Procedure:

1. Record the time of becoming aware, the deadlines run from this point

2. Early warning within 24 hours, notification within 72 hours via the ENISA platform

3. Final report after 14 days or one month respectively

4. Record everything in reporting log F06, emergency card D16

4.10 P10 Security advisories to users

Purpose: Inform affected users clearly and in good time (Article 14(8))

Owner: Weiß · **Frequency:** per case · **Record:** F07 · **Practised 03/2027 to 02/2028:** 4 advisories

Procedure:

1. Write the advisory using template F07: what, who is affected, what to do

2. Distribution via portal, app and email

3. Publication on the website after remediation

4.11 P11 Update provision

Purpose: Secure, free updates throughout the entire support period (Annex I, Part II, points (7) and (8))

Owner: Datenwerk · **Frequency:** per release · **Record:** F14 · **Practised 03/2027 to 02/2028:** 5 staged rollouts

Procedure:

1. Release with SBOM (P06) and security approval (F14)

2. Signing under the four-eyes principle

3. Staged rollout: 1 percent, 10 percent, all

4. Publish release notes, monitor the rollout

4.12 P12 Change management

Purpose: Implement changes in a controlled manner and maintain conformity

Owner: Weiß · **Frequency:** per change · **Record:** F08 · **Practised 03/2027 to 02/2028:** 9 requests

Procedure:

1. Request in F08 stating reason and scope

2. Assess the impact on D06, D07 and the declaration

3. Check whether the change is a substantial modification

4. Implement only after approval

4.13 P13 Routine testing

Purpose: Every unit conforms to the tested type · **Owner:** Hofer · **Frequency:** per unit · **Record:** F10 · **Practised 03/2027 to 02/2028:** 34 reports

Procedure:

1. Visual inspection and electrical testing in accordance with EN 60204-1 (Hofer)

2. Short test of all safety functions

3. Record firmware and signature status per serial number

4. Report F10, no delivery without a report

4.14 P14 Commissioning

Purpose: Every installation starts at the customer site with secure default settings

Owner: Berger · **Frequency:** per installation · **Record:** F11 · **Practised 03/2027 to 02/2028:** 31 reports

Procedure:

1. Test the safety functions on site

2. Initial configuration: individual password, remote maintenance off, updates on

3. Instruct the customer, hand over the documentation

4. Report F11 signed by the customer

4.15 P15 Market monitoring

Purpose: Evaluate field experience and the threat landscape

Owner: Berger · **Frequency:** quarterly · **Record:** Monitoring report · **Practised 03/2027 to 02/2028:** 4 reports

Procedure:

1. Collect faults, tickets, customer feedback and threat reports

2. Evaluate quarterly, identify trends

3. Update D06 and D07 when new findings emerge

4. Start P16 if there is an indication of non-conformity

4.16 P16 Corrective actions

Purpose: Remedy non-conformity and involve the authorities

Owner: Berger · **Frequency:** as required · **Record:** F13 · **Practised 03/2027 to 02/2028:** 1 case

Procedure:

1. Assessment by Berger and Weiß

2. Define the action: update, retrofit or withdrawal

3. In the event of a serious risk, inform market surveillance immediately

4. Record everything in F13

4.17 P17 Training

Purpose: Both staff members and the partners know their obligations

Owner: Berger · **Frequency:** annually · **Record:** F12 · **Practised 03/2027 to 02/2028:** 6 training sessions

Procedure:

1. Define training needs per role
2. Annual training on the CRA, reporting channels and secure development
3. Check effectiveness, record F12

4.18 P18 Document control

Purpose: Every document is current, approved and retrievable

Owner: Berger · **Frequency:** ongoing · **Record:** D09 · **Practised 03/2027 to 02/2028:** Review 02/2028

Procedure:

1. Number, version, approval and next review date in every document
2. Update the revision history with every change
3. Retention for at least 10 years after the last unit is placed on the market

4.19 P19 Support period

Purpose: Justify, state and honour the support period (Article 13(8))

Owner: Berger · **Frequency:** annually · **Record:** D15 · **Practised 03/2027 to 02/2028:** Review 12/2027

Procedure:

1. Determine the expected period of use (15 years from handover of each unit)
2. Check the support commitments for the components
3. Statement D15, end date per unit on the label and at the time of purchase
4. Check annually whether the commitment can be kept

4.20 P20 Decommissioning

Purpose: Shut down the installation safely, delete data and access credentials

Owner: Weiß · **Frequency:** as required · **Record:** D13 · **Practised 03/2027 to 02/2028:** 0 cases, procedure rehearsed

Procedure:

1. Deactivate remote access and the customer account
2. Securely erase data in the gateway
3. Guide the customer using user information D13, document the procedure

5 Terms and abbreviations

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

CVSS: severity score of a vulnerability from 0 to 10

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

SBOM: software bill of materials: which components in which version

SF: safety function

6 Revision history and approval

Version	Date	Change	Approval
1.0	20.12.2026	Processes introduced	M. Berger
1.1	15.03.2027	Release for placing on the market	M. Berger
1.2	11.12.2027	P09 and P10 fully aligned with the CRA	M. Berger
1.3	05.02.2028	Annual process review	M. Berger
1.4	28.02.2028	Records made more specific, support period per unit	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.