CRA-MUSTER

D08 Prozesshandbuch

Beispiel nach einem Jahr Betrieb, Stand 28.02.2028 · Nordwald Wärmetechnik GmbH, vernetzter Hackgutkessel NWT HACKTHERM 60 connect

Herausgeber	OT-Cyber.de, Max Gilg, Rosenheim
Musterbetrieb	Nordwald Wärmetechnik GmbH, vernetzter Hackgutkessel NWT HACKTHERM 60 connect (frei erfunden)
Hinweis	Kostenfreies Muster, keine Rechtsberatung

Firma, Personen, Daten und Nummern sind frei erfunden. So sieht das Dokument nach einem Jahr gelebtem Betrieb aus.

1 Zweck und Geltungsbereich

20 Prozesse für einen Betrieb mit zwei Personen und Partnern, mit Verantwortung, Takt, Nachweis und dem Beleg, dass jeder Prozess im ersten Serienjahr gelaufen ist.

2 Dokumentenlenkung

Feld	Eintrag
Dokument-Nr.	NWT-CE-D08
Version, Status	1.4, freigegeben
Geltungsbereich	NWT HACKTHERM 60 connect (18 bis 60 kW), Steuerung, Gateway, Portal und App
Ersteller	Jonas Weiß, Technik und Product Security (PSO)
Geprüft	Ingenieurbüro Lechner (Safety), Sichtwerk Security (Security)
Freigabe	Michael Berger, Geschäftsführer, 28.02.2028
Nächste Prüfung	15.03.2029 oder bei wesentlicher Änderung
Vertraulichkeit	intern
Ablage	Technische Dokumentation NWT-TD-HT60C, aufbewahrt bis mindestens 10 Jahre nach Inverkehrbringen der letzten Einheit

3 Die 20 Prozesse im Überblick

P	Prozess	Verantw.	Takt	Nachweis	Gelebt 03/2027 bis 02/2028
P01	Regelwerks- und Normenmonitoring	Berger	monatlich	D01	12 Monatsprotokolle
P02	Anforderungsmanagement	Weiß	je Release	F01	5 Releases geprüft
P03	Sichere Entwicklung	Weiß	je Release	F14	5 Freigaben, 1 Pentest
P04	Safety-Validierung	Weiß	bei Änderung	F09	1 Signaturprüfung
P05	Komponenten und Lieferanten	Weiß	jährlich	F02	Bewertung 11/2027
P06	SBOM	Datenwerk	je Release	F04	5 SBOM-Fassungen
P07	Schwachstellenbehandlung	Weiß	laufend	F05	7 Tickets
P08	Koordinierte Offenlegung	Weiß	laufend	D14	3 externe Meldungen
P09	Meldung nach Art. 14	Weiß	im Ereignis	F06	1 Meldung, 1 Übung
P10	Sicherheitshinweise an Nutzer	Weiß	je Fall	F07	4 Hinweise

P	Prozess	Verantw.	Takt	Nachweis	Gelebt 03/2027 bis 02/2028
P11	Update-Bereitstellung	Datenwerk	je Release	F14	5 Rollouts gestuft
P12	Änderungsmanagement	Weiß	je Änderung	F08	9 Anträge
P13	Stückprüfung	Hofer	je Gerät	F10	34 Protokolle
P14	Inbetriebnahme	Berger	je Anlage	F11	31 Protokolle
P15	Marktbeobachtung	Berger	quartalsweise	MB-Bericht	4 Berichte
P16	Korrekturmaßnahmen	Berger	im Fall	F13	1 Fall
P17	Schulung	Berger	jährlich	F12	6 Schulungen
P18	Dokumentenlenkung	Berger	laufend	D09	Prüfung 02/2028
P19	Unterstützungszeitraum	Berger	jährlich	D15	Prüfung 12/2027
P20	Außerbetriebnahme	Weiß	im Fall	D13	0 Fälle, Ablauf geübt

Legende: P = Prozess.

Jahresauswertung 05.02.2028: Alle Prozesse mit Takt sind gelaufen. P07 war der aufwendigste Prozess (7 Tickets, davon eines aktiv ausgenutzt). Verbesserung: Datenwerk liefert die SBOM seit 1.5.0 maschinenlesbar mit jeder Freigabe, die Prüfung auf bekannte Lücken läuft täglich automatisch.

4 Die Prozesse im Einzelnen

4.1 P01 Regelwerks- und Normenmonitoring

Zweck: Aktuelle Rechts- und Normenbasis sicherstellen, bevor etwas erklärt oder geliefert wird

Verantwortlich: Berger · **Takt:** monatlich · **Nachweis:** D01 · **Gelebt 03/2027 bis 02/2028:** 12 Monatsprotokolle

Ablauf:

1. Amtsblatt, ENISA, BSI, CEN/CENELEC und Verbände monatlich auf Änderungen prüfen
2. Auswirkung auf Kessel, Gateway und Erklärung bewerten
3. D01 fortschreiben, Normenliste anpassen
4. Ergebnis im Monatsprotokoll festhalten, Weiß informieren

4.2 P02 Anforderungsmanagement

Zweck: Jede Anforderung aus Recht, Norm, Safety und Security nachverfolgbar machen

Verantwortlich: Weiß · **Takt:** je Release · **Nachweis:** F01 · **Gelebt 03/2027 bis 02/2028:** 5 Releases geprüft

Ablauf:

1. Anforderung mit ID und Quelle in F01 erfassen

2. Architektur, Test und Nachweis zuordnen

3. vor jedem Release prüfen: jede Anforderung erfüllt und belegt

4.3 P03 Sichere Entwicklung

Zweck: Gateway, Portal und App nach IEC 62443-4-1 entwickeln (CRA Anhang I Teil I)

Verantwortlich: Weiß · **Takt:** je Release · **Nachweis:** F14 · **Gelebt 03/2027 bis 02/2028:** 5 Freigaben, 1 Pentest

Ablauf:

1. Bedrohungsmodell D07 je Release prüfen

2. Code-Review und statische Analyse bei Datenwerk

3. Schwachstellenscan und Schnittstellentest vor jeder Freigabe

4. Pentest durch Sichtwerk vor jeder Hauptversion, Freigabe in F14

4.4 P04 Safety-Validierung

Zweck: Sicherheitsfunktionen SF1 bis SF10 bleiben nach jeder Änderung wirksam (EN ISO 13849)

Verantwortlich: Weiß · **Takt:** bei Änderung · **Nachweis:** F09 · **Gelebt 03/2027 bis 02/2028:** 1 Signaturprüfung

Ablauf:

1. Änderung am Sicherheitsteil auf Auswirkung prüfen (Lechner)

2. betroffene Sicherheitsfunktion mit Fehlerinjektion prüfen

3. Signatur des F-Programms vergleichen

4. Ergebnis in F09, Freigabe durch Weiß

4.5 P05 Komponenten und Lieferanten

Zweck: Fremdkomponenten dürfen die Cybersicherheit nicht schwächen (Art. 13 Abs. 5 CRA)

Verantwortlich: Weiß · **Takt:** jährlich · **Nachweis:** F02 · **Gelebt 03/2027 bis 02/2028:** Bewertung 11/2027

Ablauf:

1. Komponenten nach Kritikalität einstufen

2. Nachweise anfordern: Erklärung, SBOM, Supportzusage

3. Bewertung in F02, Vertrag mit Meldepflicht (F03)

4. jährlich und bei jeder Sicherheitsmeldung neu bewerten

4.6 P06 SBOM

Zweck: Komponenten und Abhängigkeiten jeder Firmware dokumentieren (Anhang I Teil II Nr. 1)

Verantwortlich: Datenwerk · **Takt:** je Release · **Nachweis:** F04 · **Gelebt 03/2027 bis 02/2028:** 5 SBOM-Fassungen

Ablauf:

1. SBOM automatisch im Build erzeugen (Datenwerk)
2. gegen Schwachstellendatenbanken abgleichen
3. SBOM in F04 freigeben, ohne freigegebene SBOM kein Release

4.7 P07 Schwachstellenbehandlung

Zweck: Schwachstellen erkennen, bewerten und ohne Verzögerung beheben (Anhang I Teil II)

Verantwortlich: Weiß · **Takt:** laufend · **Nachweis:** F05 · **Gelebt 03/2027 bis 02/2028:** 7 Tickets

Ablauf:

1. Ticket in F05 anlegen, Triage am selben Arbeitstag
2. Schwere nach CVSS und Bezug zur Sicherheit bewerten
3. bei aktiver Ausnutzung sofort P09 starten
4. Behebung über P11, Nutzer über P10 informieren

4.8 P08 Koordinierte Offenlegung

Zweck: Meldungen Dritter annehmen und abgestimmt veröffentlichen (Anhang I Teil II Nr. 5 und 6)

Verantwortlich: Weiß · **Takt:** laufend · **Nachweis:** D14 · **Gelebt 03/2027 bis 02/2028:** 3 externe Meldungen

Ablauf:

1. Eingang über die Kontaktstelle nach D14, Bestätigung binnen 3 Arbeitstagen
2. mit dem Melder Termin und Inhalt abstimmen
3. Behandlung nach P07, Veröffentlichung nach Behebung

4.9 P09 Meldung nach Art. 14

Zweck: Aktiv ausgenutzte Schwachstellen und schwere Vorfälle fristgerecht melden

Verantwortlich: Weiß · **Takt:** im Ereignis · **Nachweis:** F06 · **Gelebt 03/2027 bis 02/2028:** 1 Meldung, 1 Übung

Ablauf:

1. Zeitpunkt der Kenntnis festhalten, ab hier laufen die Fristen
2. Frühwarnung binnen 24 Stunden, Meldung binnen 72 Stunden über die ENISA-Plattform
3. Abschlussbericht nach 14 Tagen bzw. einem Monat
4. alles im Meldeprotokoll F06, Notfallkarte D16

4.10 P10 Sicherheitshinweise an Nutzer

Zweck: Betroffene Nutzer verständlich und rechtzeitig informieren (Art. 14 Abs. 8)

Verantwortlich: Weiß · **Takt:** je Fall · **Nachweis:** F07 · **Gelebt 03/2027 bis 02/2028:** 4 Hinweise

Ablauf:

1. Hinweis nach Vorlage F07 schreiben: was, wer betroffen, was tun
2. Versand über Portal, App und E-Mail
3. Veröffentlichung auf der Webseite nach Behebung

4.11 P11 Update-Bereitstellung

Zweck: Sichere, kostenlose Updates über den ganzen Unterstützungszeitraum (Anhang I Teil II Nr. 7 und 8)

Verantwortlich: Datenwerk · **Takt:** je Release · **Nachweis:** F14 · **Gelebt 03/2027 bis 02/2028:** 5 Rollouts gestuft

Ablauf:

1. Release mit SBOM (P06) und Security-Freigabe (F14)
2. Signatur nach dem Vier-Augen-Prinzip
3. gestufter Rollout: 1 Prozent, 10 Prozent, alle
4. Release Notes veröffentlichen, Rollout überwachen

4.12 P12 Änderungsmanagement

Zweck: Änderungen kontrolliert umsetzen und die Konformität erhalten

Verantwortlich: Weiß · **Takt:** je Änderung · **Nachweis:** F08 · **Gelebt 03/2027 bis 02/2028:** 9 Anträge

Ablauf:

1. Antrag in F08 mit Grund und Umfang
2. Auswirkung auf D06, D07 und die Erklärung bewerten
3. prüfen, ob eine wesentliche Änderung vorliegt
4. erst nach Freigabe umsetzen

4.13 P13 Stückprüfung

Zweck: Jede Einheit entspricht dem geprüften Typ

Verantwortlich: Hofer · **Takt:** je Gerät · **Nachweis:** F10 · **Gelebt 03/2027 bis 02/2028:** 34 Protokolle

Ablauf:

1. Sichtprüfung und elektrische Prüfung nach EN 60204-1 (Hofer)
2. Kurztest aller Sicherheitsfunktionen
3. Firmware- und Signaturstand je Seriennummer festhalten

4. Protokoll F10, ohne Protokoll keine Auslieferung

4.14 P14 Inbetriebnahme

Zweck: Jede Anlage startet beim Kunden in sicherer Grundeinstellung

Verantwortlich: Berger · **Takt:** je Anlage · **Nachweis:** F11 · **Gelebt 03/2027 bis 02/2028:** 31 Protokolle

Ablauf:

1. Sicherheitsfunktionen vor Ort prüfen
2. Erstkonfiguration: eigenes Passwort, Fernwartung aus, Updates an
3. Kunde einweisen, Unterlagen übergeben
4. Protokoll F11 mit Unterschrift des Kunden

4.15 P15 Marktbeobachtung

Zweck: Felderfahrung und Bedrohungslage auswerten

Verantwortlich: Berger · **Takt:** quartalsweise · **Nachweis:** MB-Bericht · **Gelebt 03/2027 bis 02/2028:** 4 Berichte

Ablauf:

1. Störungen, Tickets, Kundenhinweise und Lagemeldungen sammeln
2. quartalsweise auswerten, Trends erkennen
3. D06 und D07 bei neuen Erkenntnissen fortschreiben
4. bei Hinweis auf Nichtkonformität P16 starten

4.16 P16 Korrekturmaßnahmen

Zweck: Nichtkonformität beheben und Behörden einbinden

Verantwortlich: Berger · **Takt:** im Fall · **Nachweis:** F13 · **Gelebt 03/2027 bis 02/2028:** 1 Fall

Ablauf:

1. Bewertung durch Berger und Weiß
2. Maßnahme festlegen: Update, Nachrüstung oder Rücknahme
3. bei ernstem Risiko sofort die Marktüberwachung informieren
4. alles in F13 festhalten

4.17 P17 Schulung

Zweck: Beide Personen und die Partner kennen ihre Pflichten

Verantwortlich: Berger · **Takt:** jährlich · **Nachweis:** F12 · **Gelebt 03/2027 bis 02/2028:** 6 Schulungen

Ablauf:

1. Schulungsbedarf je Rolle festlegen

2. jährliche Schulung zu CRA, Meldewegen und sicherer Entwicklung

3. Wirksamkeit prüfen, Nachweis F12

4.18 P18 Dokumentenlenkung

Zweck: Jedes Dokument ist aktuell, freigegeben und auffindbar

Verantwortlich: Berger · **Takt:** laufend · **Nachweis:** D09 · **Gelebt 03/2027 bis 02/2028:** Prüfung 02/2028

Ablauf:

1. Nummer, Version, Freigabe und nächste Prüfung in jedem Dokument

2. Änderungshistorie bei jeder Änderung fortschreiben

3. Aufbewahrung mindestens 10 Jahre nach Inverkehrbringen der letzten Einheit

4.19 P19 Unterstützungszeitraum

Zweck: Unterstützungszeitraum begründen, angeben und einhalten (Art. 13 Abs. 8)

Verantwortlich: Berger · **Takt:** jährlich · **Nachweis:** D15 · **Gelebt 03/2027 bis 02/2028:** Prüfung 12/2027

Ablauf:

1. erwartete Nutzungsdauer ermitteln (15 Jahre ab Übergabe jeder Einheit)

2. Supportzusagen der Komponenten prüfen

3. Erklärung D15, Enddatum je Einheit auf dem Etikett und beim Kauf

4. jährlich prüfen, ob die Zusage zu halten ist

4.20 P20 Außerbetriebnahme

Zweck: Anlage sicher stilllegen, Daten und Zugänge löschen

Verantwortlich: Weiß · **Takt:** im Fall · **Nachweis:** D13 · **Gelebt 03/2027 bis 02/2028:** 0 Fälle, Ablauf geübt

Ablauf:

1. Fernzugang und Kundenkonto deaktivieren

2. Daten im Gateway sicher löschen

3. Kunden nach Nutzerinformation D13 anleiten, Ablauf dokumentieren

5 Begriffe und Abkürzungen

BSI: Bundesamt für Sicherheit in der Informationstechnik

CEN: Europäisches Komitee für Normung

CRA: Cyber Resilience Act, EU-Verordnung 2024/2847

CVSS: Schweregrad einer Schwachstelle von 0 bis 10

ENISA: EU-Agentur für Cybersicherheit, betreibt die Meldeplattform nach CRA

MB: Marktbeobachtung (Nummernkreis der Berichte)

SBOM: Stückliste der Software: welche Bausteine in welcher Version enthalten sind

SF: Sicherheitsfunktion

6 Änderungshistorie und Freigabe

Version	Datum	Änderung	Freigabe
1.0	20.12.2026	Prozesse eingeführt	M. Berger
1.1	15.03.2027	Freigabe zum Inverkehrbringen	M. Berger
1.2	11.12.2027	P09 und P10 auf CRA voll angepasst	M. Berger
1.3	05.02.2028	Jahresauswertung der Prozesse	M. Berger
1.4	28.02.2028	Nachweise konkretisiert, Unterstützungszeitraum je Einheit	M. Berger

Freigegeben: Michael Berger, Geschäftsführer, 28.02.2028 (im Original unterschrieben). Kostenfreies Muster von OT-Cyber.de, keine Rechtsberatung. Firma, Personen, Seriennummern und Daten frei erfunden.