CRA-MUSTER

D08 Prozesshandbuch

Leere Vorlage · 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

Felder ausfüllen, mit Datum und Unterschrift freigeben, in der Ablage nach Dokumentenlenkung führen.

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.

So füllen Sie dieses Formular aus

Füllen Sie die Felder mit den Angaben Ihres Betriebs aus. Unter jeder Tabelle und neben jedem Feld steht ein Beispiel aus dem Musterbetrieb als Orientierung. Verweisen Sie auf Nachweise mit Nummer (z. B. Ticket oder Formular). Zum Schluss mit Datum und Unterschrift freigeben und nach der Dokumentenlenkung ablegen.

2 Dokumentenlenkung

Feld	Eintrag
Dokument-Nr.	
Version, Status	
Geltungsbereich	
Ersteller	
Geprüft	
Freigabe	
Nächste Prüfung	
Vertraulichkeit	
Ablage	

3 Die 20 Prozesse im Überblick

P	Prozess	Verantw.	Takt	Nachweis	Gelebt 03/2027 bis 02/2028

P	Prozess	Verantw.	Takt	Nachweis	Gelebt 03/2027 bis 02/2028

Beispielzeile aus dem Muster: P: P01 · Prozess: Regelwerks- und Normenmonitoring · Verantw.: Berger · Takt: monatlich · Nachweis: D01 · Gelebt 03/2027 bis 02/2028: 12 Monatsprotokolle

Legende: P = Prozess.

Beschreiben Sie hier Ihren Stand, konkret und mit Datum. Beispiel aus dem Muster: Jahresauswertung 05.02.2028: Alle Prozesse mit Takt sind gelaufen.

4 Die Prozesse im Einzelnen

4.1 P01 Regelwerks- und Normenmonitoring

Feld	Eintrag	Beispiel aus dem Muster
Zweck		Aktuelle Rechts- und Normenbasis sicherstellen, …
Verantwortlich		Berger
Takt		monatlich
Nachweis		D01
Gelebt 03/2027 bis 02/2028		12 Monatsprotokolle

Ablauf:

1. …

2. …

3. …

Beispiel aus dem Muster, erster Schritt: Amtsblatt, ENISA, BSI, CEN/CENELEC und Verbände monatlich auf Änderungen prüfen

4.2 P02 Anforderungsmanagement

Feld	Eintrag	Beispiel aus dem Muster
Zweck		Jede Anforderung aus Recht, Norm, Safety und …
Verantwortlich		Weiß
Takt		je Release
Nachweis		F01
Gelebt 03/2027 bis 02/2028		5 Releases geprüft

Ablauf:

1. …

2. …

3. …

Beispiel aus dem Muster, erster Schritt: Anforderung mit ID und Quelle in F01 erfassen

4.3 P03 Sichere Entwicklung

Feld	Eintrag	Beispiel aus dem Muster
Zweck		Gateway, Portal und App nach IEC 62443-4-1 …
Verantwortlich		Weiß
Takt		je Release
Nachweis		F14
Gelebt 03/2027 bis 02/2028		5 Freigaben, 1 Pentest

Ablauf:

1. …

2. …

3. …

Beispiel aus dem Muster, erster Schritt: Bedrohungsmodell D07 je Release prüfen

4.4 P04 Safety-Validierung

Feld	Eintrag	Beispiel aus dem Muster
Zweck		Sicherheitsfunktionen SF1 bis SF10 bleiben nach …
Verantwortlich		Weiß
Takt		bei Änderung
Nachweis		F09
Gelebt 03/2027 bis 02/2028		1 Signaturprüfung

Ablauf:

1. …

2. …

3. …

Beispiel aus dem Muster, erster Schritt: Änderung am Sicherheitsteil auf Auswirkung prüfen (Lechner)

4.5 P05 Komponenten und Lieferanten

Feld	Eintrag	Beispiel aus dem Muster
Zweck		Fremdkomponenten dürfen die Cybersicherheit …
Verantwortlich		Weiß
Takt		jährlich
Nachweis		F02
Gelebt 03/2027 bis 02/2028		Bewertung 11/2027

Ablauf:

1. …
2. …
3. …

Beispiel aus dem Muster, erster Schritt: Komponenten nach Kritikalität einstufen

4.6 P06 SBOM

Feld	Eintrag	Beispiel aus dem Muster
Zweck		Komponenten und Abhängigkeiten jeder Firmware …
Verantwortlich		Datenwerk
Takt		je Release
Nachweis		F04
Gelebt 03/2027 bis 02/2028		5 SBOM-Fassungen

Ablauf:

1. …
2. …
3. …

Beispiel aus dem Muster, erster Schritt: SBOM automatisch im Build erzeugen (Datenwerk)

4.7 P07 Schwachstellenbehandlung

Feld	Eintrag	Beispiel aus dem Muster
Zweck		Schwachstellen erkennen, bewerten und ohne …
Verantwortlich		Weiß

Feld	Eintrag	Beispiel aus dem Muster
Takt		laufend
Nachweis		F05
Gelebt 03/2027 bis 02/2028		7 Tickets

Ablauf:

1. …

2. …

3. …

Beispiel aus dem Muster, erster Schritt: Ticket in F05 anlegen, Triage am selben Arbeitstag

4.8 P08 Koordinierte Offenlegung

Feld	Eintrag	Beispiel aus dem Muster
Zweck		Meldungen Dritter annehmen und abgestimmt …
Verantwortlich		Weiß
Takt		laufend
Nachweis		D14
Gelebt 03/2027 bis 02/2028		3 externe Meldungen

Ablauf:

1. …

2. …

3. …

Beispiel aus dem Muster, erster Schritt: Eingang über die Kontaktstelle nach D14, Bestätigung binnen 3 Arbeitstagen

4.9 P09 Meldung nach Art. 14

Feld	Eintrag	Beispiel aus dem Muster
Zweck		Aktiv ausgenutzte Schwachstellen und schwere …
Verantwortlich		Weiß
Takt		im Ereignis
Nachweis		F06
Gelebt 03/2027 bis 02/2028		1 Meldung, 1 Übung

Ablauf:

1. …

2. …

3. …

Beispiel aus dem Muster, erster Schritt: Zeitpunkt der Kenntnis festhalten, ab hier laufen die Fristen

4.10 P10 Sicherheitshinweise an Nutzer

Feld	Eintrag	Beispiel aus dem Muster
Zweck		Betroffene Nutzer verständlich und rechtzeitig …
Verantwortlich		Weiß
Takt		je Fall
Nachweis		F07
Gelebt 03/2027 bis 02/2028		4 Hinweise

Ablauf:

1. …

2. …

3. …

Beispiel aus dem Muster, erster Schritt: Hinweis nach Vorlage F07 schreiben: was, wer betroffen, was tun

4.11 P11 Update-Bereitstellung

Feld	Eintrag	Beispiel aus dem Muster
Zweck		Sichere, kostenlose Updates über den ganzen …
Verantwortlich		Datenwerk
Takt		je Release
Nachweis		F14
Gelebt 03/2027 bis 02/2028		5 Rollouts gestuft

Ablauf:

1. …

2. …

3. …

Beispiel aus dem Muster, erster Schritt: Release mit SBOM (P06) und Security-Freigabe (F14)

4.12 P12 Änderungsmanagement

Feld	Eintrag	Beispiel aus dem Muster
Zweck		Änderungen kontrolliert umsetzen und die …
Verantwortlich		Weiß
Takt		je Änderung
Nachweis		F08
Gelebt 03/2027 bis 02/2028		9 Anträge

Ablauf:

1. …
2. …
3. …

Beispiel aus dem Muster, erster Schritt: Antrag in F08 mit Grund und Umfang

4.13 P13 Stückprüfung

Feld	Eintrag	Beispiel aus dem Muster
Zweck		Jede Einheit entspricht dem geprüften Typ
Verantwortlich		Hofer
Takt		je Gerät
Nachweis		F10
Gelebt 03/2027 bis 02/2028		34 Protokolle

Ablauf:

1. …
2. …
3. …

Beispiel aus dem Muster, erster Schritt: Sichtprüfung und elektrische Prüfung nach EN 60204-1 (Hofer)

4.14 P14 Inbetriebnahme

Feld	Eintrag	Beispiel aus dem Muster
Zweck		Jede Anlage startet beim Kunden in sicherer …
Verantwortlich		Berger

Feld	Eintrag	Beispiel aus dem Muster
Takt		je Anlage
Nachweis		F11
Gelebt 03/2027 bis 02/2028		31 Protokolle

Ablauf:

1. …

2. …

3. …

Beispiel aus dem Muster, erster Schritt: Sicherheitsfunktionen vor Ort prüfen

4.15 P15 Marktbeobachtung

Feld	Eintrag	Beispiel aus dem Muster
Zweck		Felderfahrung und Bedrohungslage auswerten
Verantwortlich		Berger
Takt		quartalsweise
Nachweis		MB-Bericht
Gelebt 03/2027 bis 02/2028		4 Berichte

Ablauf:

1. …

2. …

3. …

Beispiel aus dem Muster, erster Schritt: Störungen, Tickets, Kundenhinweise und Lagemeldungen sammeln

4.16 P16 Korrekturmaßnahmen

Feld	Eintrag	Beispiel aus dem Muster
Zweck		Nichtkonformität beheben und Behörden einbinden
Verantwortlich		Berger
Takt		im Fall
Nachweis		F13
Gelebt 03/2027 bis 02/2028		1 Fall

Ablauf:

1. …

2. …

3. …

Beispiel aus dem Muster, erster Schritt: Bewertung durch Berger und Weiß

4.17 P17 Schulung

Feld	Eintrag	Beispiel aus dem Muster
Zweck		Beide Personen und die Partner kennen ihre …
Verantwortlich		Berger
Takt		jährlich
Nachweis		F12
Gelebt 03/2027 bis 02/2028		6 Schulungen

Ablauf:

1. …

2. …

3. …

Beispiel aus dem Muster, erster Schritt: Schulungsbedarf je Rolle festlegen

4.18 P18 Dokumentenlenkung

Feld	Eintrag	Beispiel aus dem Muster
Zweck		Jedes Dokument ist aktuell, freigegeben und …
Verantwortlich		Berger
Takt		laufend
Nachweis		D09
Gelebt 03/2027 bis 02/2028		Prüfung 02/2028

Ablauf:

1. …

2. …

3. …

Beispiel aus dem Muster, erster Schritt: Nummer, Version, Freigabe und nächste Prüfung in jedem Dokument

4.19 P19 Unterstützungszeitraum

Feld	Eintrag	Beispiel aus dem Muster
Zweck		Unterstützungszeitraum begründen, angeben und …
Verantwortlich		Berger
Takt		jährlich
Nachweis		D15
Gelebt 03/2027 bis 02/2028		Prüfung 12/2027

Ablauf:

1. …
2. …
3. …

Beispiel aus dem Muster, erster Schritt: erwartete Nutzungsdauer ermitteln (15 Jahre ab Übergabe jeder Einheit)

4.20 P20 Außerbetriebnahme

Feld	Eintrag	Beispiel aus dem Muster
Zweck		Anlage sicher stilllegen, Daten und Zugänge …
Verantwortlich		Weiß
Takt		im Fall
Nachweis		D13
Gelebt 03/2027 bis 02/2028		0 Fälle, Ablauf geübt

Ablauf:

1. …
2. …
3. …

Beispiel aus dem Muster, erster Schritt: Fernzugang und Kundenkonto deaktivieren

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

Freigegeben (Name, Funktion, Datum, Unterschrift): _____ · Kostenfreies Muster von OT-Cyber.de, keine Rechtsberatung. Firma, Personen, Seriennummern und Daten frei erfunden.