NIS2-MUSTER

F-09 Erstaufnahme Sicherheitsereignisse

Leere Vorlage · Musterwerk KWK-Service GmbH, BHKW-Service mit Fernwartung

Herausgeber	OT-Cyber.de, Max Gilg, Rosenheim
Musterbetrieb	Musterwerk KWK-Service GmbH, BHKW-Service mit Fernwartung (frei erfunden)
Hinweis	Kostenfreies Muster, keine Rechtsberatung

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

1 Zweck und Geltungsbereich

Jedes Sicherheitsereignis wird sofort mit Uhrzeit, Quelle, Beobachtung und Sofortmaßnahmen aufgenommen, auch wenn es sich später als harmlos erweist. Das Register zeigt, dass der Meldeweg gelebt wird.

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 Ereignisregister

Vorgang	Eingang	Quelle	Beobachtung	Bewertung F-10

Vorgang	Eingang	Quelle	Beobachtung	Bewertung F-10

Beispielzeile aus dem Muster: Vorgang: SV-2026-001 · Eingang: 28.08.2026 · Quelle: MDR · Beobachtung: Anmeldeversuche auf Plattform · Bewertung F-10: nicht erheblich

4 Beispiel einer Erstaufnahme: SV-2026-003

Feld	Eintrag	Beispiel aus dem Muster
Eingang		22.09.2026, 06:42 Uhr, MDR-Dienst per Telefon …
Beobachtung		Anmeldung am Konto des Servicetechnikers S. …
Betroffen		Cloud-Konto S. Kraus (A-01), Postfach mit …
Sofortmaßnahmen		06:50 Konto gesperrt und Sitzungen beendet …
ISB alarmiert		06:58 Uhr
Aufgenommen		P. Neumann, Rufbereitschaft

Beschreiben Sie hier Ihren Stand, konkret und mit Datum. Beispiel aus dem Muster: Lehre aus SV-2027-004: Testkonten der Lieferanten werden vorab angekündigt und mit Ablaufdatum angelegt (F-15).

5 Begriffe und Abkürzungen

ISB: Informationssicherheitsbeauftragte oder Informationssicherheitsbeauftragter

MDR: Dienst, der Alarme rund um die Uhr auswertet (Managed Detection and Response)

SV: Sicherheitsvorfall (Nummernkreis)

6 Änderungshistorie und Freigabe

Version	Datum	Änderung	Freigabe

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