NIS2-MUSTER

F-17 Management-Review

Beispiel nach einem Jahr Betrieb, Stand 28.09.2027 · 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

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

1 Zweck und Geltungsbereich

Jährliche Bewertung durch die Geschäftsführung: Stand der Maßnahmen, Kennzahlen, Vorfälle, Änderungen, Entscheidungen. Das Protokoll ist der Nachweis der Überwachung nach § 38 BSIG.

2 Dokumentenlenkung

Feld	Eintrag
Dokument-Nr.	MW-ISMS-F-17
Version, Status	2.1, freigegeben
Geltungsbereich	Musterwerk KWK-Service GmbH, alle Standorte, Systeme und Fernzugänge zu Kundenanlagen
Ersteller	Julia Hartl, ISB
Geprüft	Markus Wein, Vertretung ISB
Freigabe	Thomas Berger, Geschäftsführer, 28.09.2027
Nächste Prüfung	30.06.2028 oder bei wesentlicher Änderung
Vertraulichkeit	intern
Ablage	ISMS-Ordner im Cloud-Büropaket, Bereich 01 Lenkung

3 Ergebnisse des Reviews

Datum, Teilnehmende: 30.06.2027, T. Berger, J. Hartl, M. Wein, S. Lang

4 Kennzahlen

Kennzahl	Ziel	10/2026	06/2027
Konten mit Hardware-Schlüssel	100 %	62 %	100 %
Router mit aktueller Firmware	100 %	82 von 85	89 von 91
Fernzugriffe über Plattform	100 %	100 %	100 %
Backup-Tests bestanden	alle	1 von 1	4 von 4
Schulungsquote	100 %	100 %	100 %
Klickrate Phishing	unter 10 %	10 %	18 %, 0 Eingaben
Alarm MDR bis Bereitschaft	unter 30 min	16 min	im Mittel 12 min
Maßnahmen erledigt	laut Plan	11 von 15	21 von 24

5 Bewertung

Vorfälle: ein erheblicher (SV-2026-003), fristgerecht gemeldet; sechs nicht erhebliche Ereignisse sauber bewertet.

Wirksamkeit: Pentest 01/2027 ohne kritischen Befund, drei mittlere Befunde behoben (M-20 bis M-22).

Änderungen: sechs Neukunden, ein Austritt, eine Neueinstellung, KI-Assistent im Büropaket eingeführt.

Klickrate gestiegen durch QR-Code-Übung; Kurzschulung erfolgt, Übung wird wiederholt.

6 Entscheidungen

Maßnahmenplan 2027/28 gebilligt, Budget bestätigt (B-09).

Restrisiken R-05 und R-12 akzeptiert.

Berichtstakt der ISB ab Juli 2027 quartalsweise (B-10).

Externe Prüfung der Umsetzung am 14.09.2027.

Nächstes Review: 30.06.2028

Unterschrift: T. Berger, 30.06.2027

7 Unabhängige Prüfung und internes Auditprogramm

Datum	Prüfung	Durch	Ergebnis
14.09.2027	Umsetzung § 30 BSIG und Anhang DVO 2024/2690	externer Prüfer, unabhängig vom ISMS	0 Abweichungen, 6 Hinweise
28.09.2027	Nachprüfung der Hinweise	Hartl, gegengezeichnet Berger	6 von 6 umgesetzt (M-24 bis M-33)
quartalsweise	Stichproben: Berechtigungen, Patchstand, Backup-Test, Notfallliste	Wein, Bericht an ISB	Q3/2027 ohne Befund

Die externe Prüfung findet jährlich statt, durch einen Prüfer, der am ISMS nicht mitarbeitet. Das interne Auditprogramm prüft jedes Quartal vier Stichproben; ein Befund geht als Maßnahme in F-08.

8 Begriffe und Abkürzungen

BSIG: BSI-Gesetz

DVO: Durchführungsverordnung (EU) 2024/2690 zu NIS2

ISB: Informationssicherheitsbeauftragte oder Informationssicherheitsbeauftragter

ISMS: Managementsystem für Informationssicherheit

KI: künstliche Intelligenz

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

QR: QR-Code

SV: Sicherheitsvorfall (Nummernkreis)

9 Änderungshistorie und Freigabe

Version	Datum	Änderung	Freigabe
1.0	20.07.2026	Erstfassung im Projektstart	T. Berger
1.1	30.10.2026	Review 1	T. Berger
2.0	30.06.2027	Review 2027	T. Berger
2.1	28.09.2027	Externe Prüfung und internes Auditprogramm	T. Berger

Freigegeben: Thomas Berger, Geschäftsführer, 28.09.2027 (im Original unterschrieben). Kostenfreies Muster von OT-Cyber.de, keine Rechtsberatung. Musterbetrieb und Daten frei erfunden.