NIS2-MUSTER

F-08 Maßnahmenplan nach § 30 Abs. 2 BSIG

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

Alle Maßnahmen mit Zuordnung zu § 30 Abs. 2 Nr. 1 bis 10 BSIG, Verantwortlichen, Termin, Status und Nachweis. Monatlich fortgeschrieben, Grundlage des Berichts an die Geschäftsführung.

2 Dokumentenlenkung

Feld	Eintrag
Dokument-Nr.	MW-ISMS-F-08
Version, Status	2.3, 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 Maßnahmen nach § 30 Abs. 2 BSIG

ID	Maßnahme	Nr.	Verantw.	Status	Nachweis
M-01	Zweiter Faktor überall, Hardware-Schlüssel für alle	10	Systemhaus	erledigt 10/2026	Kontenbericht 10/2026
M-02	Persönliche Konten statt Sammelkonten	9	Hartl	erledigt 10/2026	Benutzerliste 10/2026
M-03	Zentrale Plattform, Router nur ausgehend	5, 9	Hartl	erledigt 10/2026	Router-Export 01.08.2027
M-04	EDR auf Laptops und Leitwarten-Server	2	Systemhaus	erledigt 08/2026	EDR-Bericht 08/2026
M-05	MDR-Dienst 24/7	2	Berger	erledigt 09/2026	Vertrag L-03
M-06	Backup 3-2-1 mit unveränderbarer Kopie	3	Systemhaus	erledigt 09/2026	Testprotokolle F-13
M-07	Schulung und Phishing-Übungen	7	Hartl	laufend, 4 Übungen	F-16
M-08	Patchprozess mit Fristen	5	Hartl	laufend	F-18

ID	Maßnahme	Nr.	Verantw.	Status	Nachweis
M-09	Herstellerzugriff nur über Plattform	4	Hartl	erledigt 03/2027	Vertragsanhang L-01
M-10	Vorfallbewältigung, Meldeprozess	2	Hartl	erledigt 09/2026	F-09 bis F-12
M-11	Festplattenverschlüsselung, Fernlöschung	8	Systemhaus	erledigt 08/2026	Bericht Geräteverwaltung 08/2026
M-12	SMS-Störmeldung direkt an Bereitschaft	3	Wein	erledigt 10/2026	Testprotokoll 10/2026
M-13	Notfallplan und jährliche Übung	3	Hartl	erledigt, Übung 04/2027	F-13
M-14	Jährlicher Pentest der Plattform	6	Berger	erledigt 01/2027	Pentest-Bericht 05.02.2027
M-15	Software nur aus geprüfter Quelle	5	Systemhaus	erledigt 11/2026	Freigabeliste 11/2026
M-16	Vertraulichkeit im Arbeitsvertrag	9	Lang	erledigt 12/2026	Vertragsmuster 12/2026
M-17	Lieferantenbewertung jährlich	4	Hartl	erledigt 2027	F-14
M-18	Wirksamkeitsprüfung der Maßnahmen	6	Hartl	erledigt 06/2027	F-17
M-19	Hersteller-Mobilfunkzugänge abgeschaltet	4	Hartl	88 von 91, Rest bis 30.11.2027 vereinbart	Router-Export 01.08.2027
M-20	Firewall-Verwaltung nur aus Admin-Zone	9	Systemhaus	erledigt 02/2027	Firewall-Regelwerk 02/2027
M-21	Aufzeichnung redundant speichern	2	Hartl	erledigt 03/2027	Konfigurationsbericht 03/2027
M-22	Austrittsprozess mit Kontenprüfung	9	Lang	erledigt 02/2027	Austrittsliste 02/2027
M-23	Regeln für KI-Assistenten	7	Hartl	erledigt 05/2027	Richtlinie KI 1.0
M-24	Verschlüsselung der Wartungsberichte	8	Systemhaus	erledigt 09/2027	Konfigurationsbericht 09/2027
M-25	Kryptoregelung: Verfahren, Schlüssel, Zertifikate mit Ablauf	8	Hartl	erledigt 09/2027	Schlüsselliste 09/2027
M-26	Serverraum: Zutritt, Rauchmelder, Klima-Alarm, USV	3	Wein	erledigt 09/2027	Abnahme 22.09.2027
M-27	Überprüfung von Personen mit Zugriff auf Kundenanlagen	9	Lang	erledigt 09/2027	11 von 11 geprüft
M-28	Protokollierung: Quellen, 12 Monate, Zeitabgleich	2	Systemhaus	erledigt 09/2027	Protokollkonzept 1.0

ID	Maßnahme	Nr.	Verantw.	Status	Nachweis
M-29	Trennung der Kunden auf der Plattform	5	Hartl	erledigt 09/2027	Test 21.09.2027
M-30	Grundkonfiguration mit monatlicher Abweichungsprüfung	5	Systemhaus	erledigt 09/2027	Prüfung 09/2027
M-31	Internes Auditprogramm, externe Prüfung jährlich	6	Hartl	erledigt 09/2027	Prüfbericht 14.09.2027
M-32	Regel für USB-Speicher und Wechseldatenträger	9	Systemhaus	erledigt 09/2027	Richtlinie Geräteverwaltung 09/2027
M-33	Meldestelle für Schwachstellen (security.txt)	5	Hartl	erledigt 09/2027	security.txt 09/2027

Legende: Nr. = Nummer der Mindestmaßnahme in § 30 Abs. 2 BSIG.

4 Abdeckung § 30 Abs. 2 BSIG

Nr.	Inhalt	Maßnahmen
1	Risikoanalyse, Sicherheitskonzept	F-07, F-05
2	Bewältigung von Sicherheitsvorfällen	M-04, M-05, M-10, M-21, M-28
3	Betrieb aufrechterhalten, Backup, Krisen, Versorgung	M-06, M-12, M-13, M-26
4	Lieferkette	M-09, M-17, M-19
5	Erwerb, Entwicklung, Wartung, Schwachstellen	M-03, M-08, M-15, M-29, M-30, M-33
6	Wirksamkeit bewerten	M-14, M-18, M-31
7	Cyberhygiene, Schulung	M-07, M-23
8	Kryptografie, Verschlüsselung	M-11, M-24, M-25
9	Personal, Zugriffskontrolle, Inventar	M-02, M-16, M-20, M-22, M-27, M-32, F-06
10	MFA, gesicherte Notfallkommunikation	M-01, F-13

Legende: Nr. = Nummer der Mindestmaßnahme in § 30 Abs. 2 BSIG.

5 Begriffe und Abkürzungen

BSIG: BSI-Gesetz

EDR: Schutzsoftware auf Rechnern, die Angriffe erkennt und meldet

KI: künstliche Intelligenz

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

MFA: Anmeldung mit zweitem Faktor, z. B. Code aufs Handy

SMS: Kurznachricht

USB: USB-Anschluss

USV: unterbrechungsfreie Stromversorgung, überbrückt kurze Stromausfälle

6 Änderungshistorie und Freigabe

Version	Datum	Änderung	Freigabe
1.0	20.07.2026	Erstfassung im Projektstart	T. Berger
1.1	30.08.2026	15 Maßnahmen aus der Erstanalyse	T. Berger
1.2	30.10.2026	Stand Review 1: 11 von 15 erledigt	T. Berger
2.0	05.02.2027	Maßnahmen aus dem Pentest	T. Berger
2.1	30.06.2027	Plan 2027/28 gebilligt (B-09)	T. Berger
2.2	15.08.2027	Monatsstand August	T. Berger
2.3	28.09.2027	Hinweise der externen Prüfung als M-24 bis M-33, Nachweise konkret	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.