NIS2-MUSTER

F-01 Betroffenheitsprüfung

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

Hält fest, ob und wie die Musterwerk KWK-Service GmbH unter das BSI-Gesetz fällt, mit Begründung, verworfenen Alternativen und den Zahlen, auf denen die Einstufung beruht. Jährliche Prüfung nach dem Jahresabschluss.

2 Dokumentenlenkung

Feld	Eintrag
Dokument-Nr.	MW-ISMS-F-01
Version, Status	1.3, 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 Unternehmen

Firma, Rechtsform, Sitz: Musterwerk KWK-Service GmbH, Musterstraße 5, 12345 Musterstadt

Handelsregister: Amtsgericht Musterstadt, HRB 4711

Konzernzugehörigkeit: nein, keine Partner- oder verbundenen Unternehmen

Tätigkeiten: Verkauf, Installation und Wartung von Blockheizkraftwerken (BHKW); 24/7-Fernüberwachung über die eigene Leitwarte; Fernwartung der BHKW-Steuerungen für Kunden

4 Größe nach KMU-Empfehlung 2003/361/EG

Kennzahl	2025	2026	Schwelle mittel	Quelle
Beschäftigte (JAE)	10	10,8	50	Lohnbuchhaltung
Jahresumsatz	11,4 Mio. €	12,1 Mio. €	10 Mio. €	Jahresabschluss
Jahresbilanzsumme	10,3 Mio. €	10,9 Mio. €	10 Mio. €	Jahresabschluss

Umsatz und Bilanzsumme lagen 2025 erstmals über 10 Mio. €, 2026 erneut. Damit ist der Betrieb ein mittleres Unternehmen. Ob die Zwei-Jahres-Regel aus Art. 4 des Anhangs der KMU-Empfehlung für das BSIG gilt, ist nicht abschließend geklärt. Musterwerk hat die Pflichten deshalb vorsorglich ab Juli 2026 umgesetzt; seit dem Jahresabschluss 2026 (08.03.2027) gilt die Einstufung in jedem Fall.

5 Zuordnung

Einrichtungsart: Anlage 1 Nr. 6.1.10 BSIG, Anbieter verwalteter Dienste (Managed Services Provider)

Begründung: Wir warten und überwachen Netz- und Informationssysteme Dritter aus der Ferne: BHKW-Steuerungen, Mobilfunk-Router und die Anbindung an unsere Leitwarte. Der Dienst ist vertraglich vereinbart und laufend.

Verworfen: Anlage 1 Nr. 1.1 Energie, Betreiber von Erzeugungsanlagen: Betreiber ist jeweils der Kunde. Anlage 2 Maschinenbau: wir stellen keine Module her, wir bauen nur ein.

Ergebnis: wichtige Einrichtung nach § 28 Abs. 2 BSIG

Geltung seit: vorsorglich seit Beschluss B-01 am 20.07.2026, in jedem Fall seit dem Jahresabschluss 2026 am 08.03.2027

Registrierung: am 18.08.2026 im BSI-Portal abgeschlossen, Aktenzeichen in F-02

6 Prüfung 2027

- ✓ Jahresabschluss 2026 liegt vor, Zahlen übernommen (Steuerberater, 08.03.2027)
- ✓ Tätigkeiten unverändert, neue Kunden ändern die Einrichtungsart nicht
- ✓ Keine Konzernbeziehung entstanden
- ✓ Registrierungsdaten in F-02 geprüft, keine Änderungsmitteilung nötig
- ✓ Ergebnis der Geschäftsführung vorgelegt und bestätigt (12.03.2027)

7 Begriffe und Abkürzungen

BHKW: Blockheizkraftwerk

BSI: Bundesamt für Sicherheit in der Informationstechnik

BSIG: BSI-Gesetz

EG: Europäische Gemeinschaft (in älteren EU-Rechtsakten)

HRB: Handelsregister, Abteilung B

JAE: Jahresarbeitseinheiten, umgerechnet auf Vollzeitstellen

KMU: kleine und mittlere Unternehmen

KWK: Kraft-Wärme-Kopplung

8 Änderungshistorie und Freigabe

Version	Datum	Änderung	Freigabe
1.0	20.07.2026	Erstfassung im Projektstart	T. Berger
1.1	18.08.2026	Registrierungsnummer und Portalzugang ergänzt	T. Berger
1.2	12.03.2027	Jährliche Prüfung mit Jahresabschluss 2026, Einstufung bestätigt	T. Berger
1.3	28.09.2027	Größe und Geltung nach der KMU-Empfehlung klargestellt	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.

NIS2-MUSTER

F-02 Registrierungsdaten BSI

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 Angaben, die im BSI-Portal hinterlegt sind, und die Prüfung, dass sie aktuell sind. Änderungen meldet der Betrieb innerhalb von zwei Wochen.

2 Dokumentenlenkung

Feld	Eintrag
Dokument-Nr.	MW-ISMS-F-02
Version, Status	1.4, 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 Angaben für das BSI-Portal

Name der Einrichtung: Musterwerk KWK-Service GmbH

Anschrift: Musterstraße 5, 12345 Musterstadt

Kontakt für das BSI: sicherheit@musterwerk-kwk.example, 0123 456780

Sektor, Einrichtungsart: Verwaltung von IKT-Diensten (zwischen Unternehmen), Anbieter verwalteter Dienste

Mitgliedstaaten: Deutschland

Öffentliche IP-Bereiche: 203.0.113.0/29 Büro, 203.0.113.10 Fernwartungsplattform

Ansprechstelle: Julia Hartl, ISB, Mo bis Fr 7 bis 16 Uhr

Stellvertretung: Markus Wein, Leitwarte

24/7-Erreichbarkeit: Bereitschaftstelefon 0123 456789, Rufbereitschaft der Servicetechniker

ELSTER-Zertifikat: beantragt 16.07.2026, erhalten 06.08.2026, gültig bis 06.08.2029

Mein Unternehmenskonto: eingerichtet 07.08.2026, Administratorin S. Lang, zweite Person J. Hartl

Registrierung: abgeschlossen 18.08.2026, Aktenzeichen liegt in der Akte 01-02

4 Änderungen und Prüfungen

Datum	Anlass	Geändert im Portal	Durch
18.08.2026	Erstregistrierung	alle Angaben	J. Hartl
14.01.2027	Bereitschaftsnummer gewechselt	Telefon 24/7, Vertretung	J. Hartl
05.01.2027	Halbjahresprüfung	keine Änderung	M. Wein
05.07.2027	Halbjahresprüfung	keine Änderung	J. Hartl

Die Prüfung findet im Januar und Juli statt und zusätzlich bei jedem Personalwechsel in den Rollen aus F-04. Die Zugangsdaten zum Portal liegen im Passworttresor, Bereich Notfall, mit Zugriff für ISB, Vertretung und GF.

5 Begriffe und Abkürzungen

BSI: Bundesamt für Sicherheit in der Informationstechnik

ELSTER: Steuerportal; mit dem ELSTER-Organisationszertifikat meldet man sich im BSI-Portal an

GF: Geschäftsführung

IKT: Informations- und Kommunikationstechnik

IP: Netzwerkadresse eines Geräts

ISB: Informationssicherheitsbeauftragte oder Informationssicherheitsbeauftragter

KWK: Kraft-Wärme-Kopplung

6 Änderungshistorie und Freigabe

Version	Datum	Änderung	Freigabe
1.0	20.07.2026	Erstfassung im Projektstart	T. Berger
1.1	18.08.2026	Registrierung abgeschlossen	T. Berger
1.2	14.01.2027	Neue Bereitschaftsnummer und zweite Ansprechperson gemeldet	T. Berger
1.3	05.07.2027	Halbjährliche Prüfung, keine Änderung	T. Berger
1.4	28.09.2027	Sektor Verwaltung von IKT-Diensten	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.

NIS2-MUSTER

F-03 Beschlüsse der Geschäftsführung

Beispiel nach einem Jahr Betrieb, Stand 30.06.2027 · 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

Belegt, dass die Geschäftsführung die Maßnahmen nach § 30 BSIG billigt, ihre Umsetzung überwacht und ihre Pflichten aus § 38 BSIG wahrnimmt. Ein Eintrag je Beschluss, fortlaufend.

2 Dokumentenlenkung

Feld	Eintrag
Dokument-Nr.	MW-ISMS-F-03
Version, Status	1.4, 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, 30.06.2027
Nächste Prüfung	30.06.2028 oder bei wesentlicher Änderung
Vertraulichkeit	intern
Ablage	ISMS-Ordner im Cloud-Büropaket, Bereich 01 Lenkung

3 Beschlussregister

Nr.	Datum	Beschluss	Bezug	Umsetzung
B-01	20.07.2026	Einstufung als wichtige Einrichtung anerkannt	F-01	erledigt
B-02	20.07.2026	ISB J. Hartl (20 %), Vertretung M. Wein (5 %)	F-04	erledigt
B-03	20.07.2026	Leitlinie 1.0 gebilligt	F-05	erledigt
B-04	20.07.2026	Budget Jahr 1: 48.000 € einmalig, 2.900 €/Monat	F-08	erledigt
B-05	20.07.2026	ISB darf BSI-Meldung allein absenden, wenn GF 2 h nicht erreichbar	F-11	erledigt
B-06	30.10.2026	10 weitere Hardware-Schlüssel, Pentest Januar 2027	M-01, M-14	erledigt
B-07	18.01.2027	Budget 2027: 22.000 € einmalig, 3.100 €/Monat	F-08	erledigt
B-08	12.03.2027	Betroffenheit 2027 bestätigt	F-01	erledigt
B-09	30.06.2027	Maßnahmenplan 2027/28 gebilligt, Restrisiken R-05 und R-12 akzeptiert	F-07, F-08	erledigt

Nr.	Datum	Beschluss	Bezug	Umsetzung
B-10	30.06.2027	Berichtstakt ISB ab Juli 2027 quartalsweise	F-17	erledigt

4 Überwachung durch die Geschäftsführung

- ✓ Monatsbericht der ISB bis Juni 2027 lückenlos gelesen und abgezeichnet (12 Berichte)
- ✓ Management-Review 30.10.2026 und 30.06.2027 durchgeführt (F-17)
- ✓ Schulung der Geschäftsführung 18.09.2026, Auffrischung 07.06.2027 (F-16)
- ✓ Teilnahme an der Krisenübung 23.04.2027 (F-13)
- ✓ Restrisiken schriftlich akzeptiert (F-07)

Die Geschäftsführung ist nach § 38 BSIG persönlich verantwortlich. Delegiert ist die Durchführung an die ISB, nicht die Verantwortung. Abweichungen vom Maßnahmenplan entscheidet die Geschäftsführung, dokumentiert in diesem Register.

5 Begriffe und Abkürzungen

BSI: Bundesamt für Sicherheit in der Informationstechnik

BSIG: BSI-Gesetz

GF: Geschäftsführung

ISB: Informationssicherheitsbeauftragte oder Informationssicherheitsbeauftragter

6 Änderungshistorie und Freigabe

Version	Datum	Änderung	Freigabe
1.0	20.07.2026	Erstfassung im Projektstart	T. Berger
1.1	30.10.2026	Beschlüsse aus dem ersten Management-Review	T. Berger
1.2	18.01.2027	Pentest und Budget 2027	T. Berger
1.3	12.03.2027	Betroffenheit 2027 bestätigt	T. Berger
1.4	30.06.2027	Beschlüsse aus dem Management-Review 2027	T. Berger

Freigegeben: Thomas Berger, Geschäftsführer, 30.06.2027 (im Original unterschrieben). Kostenfreies Muster von OT-Cyber.de, keine Rechtsberatung. Musterbetrieb und Daten frei erfunden.

NIS2-MUSTER

F-04 Rollen und Zuständigkeiten

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

Wer welche Aufgabe in der Informationssicherheit hat, wer vertritt, welche Befugnisse gelten und wie die Personen erreichbar sind. Grundlage für Meldeweg, Rufbereitschaft und Berechtigungen.

2 Dokumentenlenkung

Feld	Eintrag
Dokument-Nr.	MW-ISMS-F-04
Version, Status	1.4, 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 Rollen und Vertretungen

Rolle	Person	Vertretung	Erreichbarkeit
Geschäftsführung	Thomas Berger	Sabine Lang (Prokura)	mobil, 24/7 im Vorfall
ISB	Julia Hartl	Markus Wein	Mo bis Fr 7 bis 16 Uhr
Meldeverantwortlich BSI	Thomas Berger	Julia Hartl	über Bereitschaft
Rufbereitschaft	Techniker im Wochenwechsel	nächster im Plan	24/7, 0123 456789
Leitwarte	Markus Wein	Julia Hartl	Mo bis Fr 6 bis 18 Uhr
IT-Administration	Systemhaus (L-02)	Ticketsystem	Hotline 7 bis 19 Uhr
Datenschutz	externer DSB (L-07)	Kanzlei	werktags
Krisenteam	Berger, Hartl, Wein, Systemhaus	Lang	Alarmkette F-13

4 Aufgaben und Befugnisse

ISB, Aufgaben: Risikoanalyse (F-07), Maßnahmenplan (F-08), Bewertung von Vorfällen (F-10), Schulungen (F-16), Bericht an die GF, Lieferantenbewertung (F-14), Berechtigungsfreigaben (F-15)

ISB, Befugnisse: darf Fernzugänge und Konten sofort sperren lassen, darf die BSI-Meldung absenden (B-05)

Rufbereitschaft, Aufgaben: Erstaufnahme von Störungen und Sicherheitshinweisen, F-09 ausfüllen, ISB alarmieren

Rufbereitschaft, Befugnisse: darf Fernwartungssitzungen beenden und Konten über das Systemhaus sperren lassen

Alle Mitarbeitenden: Regeln der Leitlinie einhalten, Auffälligkeiten sofort an die Bereitschaft melden

Die benannten Personen haben ihre Benennung schriftlich bestätigt (Bestätigungen in der Personalakte). Der Plan der Rufbereitschaft liegt im Teamkalender, Tausch nur mit Eintrag. Keine Rolle ist ohne Vertretung.

5 Überprüfung von Personen

Wann: vor dem ersten Zugriff auf Kundenanlagen und bei Wechsel in eine Rolle mit mehr Rechten

Was: Lebenslauf und Referenzen, Führungszeugnis wie im Arbeitsvertrag vereinbart, Vertraulichkeitsverpflichtung

Stand: 11 von 11 Personen geprüft am 25.09.2027, Ergebnis in der Personalakte, Prüfung bei Neueinstellung fest im Ablauf

6 Begriffe und Abkürzungen

BSI: Bundesamt für Sicherheit in der Informationstechnik

DSB: Datenschutzbeauftragte oder Datenschutzbeauftragter

GF: Geschäftsführung

ISB: Informationssicherheitsbeauftragte oder Informationssicherheitsbeauftragter

IT: Informationstechnik, z. B. Büro-PCs und Server

7 Änderungshistorie und Freigabe

Version	Datum	Änderung	Freigabe
1.0	20.07.2026	Erstfassung im Projektstart	T. Berger
1.1	05.10.2026	Neuer Techniker L. Ober in die Rufbereitschaft	T. Berger
1.2	14.01.2027	Neue Bereitschaftsnummer	T. Berger
1.3	05.07.2027	Halbjahresprüfung, unverändert	T. Berger

Version	Datum	Änderung	Freigabe
1.4	28.09.2027	Überprüfung von Personen ergänzt	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.

NIS2-MUSTER

F-05 Leitlinie zur Informationssicherheit

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

Die verbindliche Leitlinie der Geschäftsführung: Geltungsbereich, Ziele, Grundsätze, Verantwortung und Überprüfung. Allen Mitarbeitenden bekannt gemacht.

2 Dokumentenlenkung

Feld	Eintrag
Dokument-Nr.	MW-ISMS-F-05
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 Leitlinie

Geltungsbereich: alle Mitarbeitenden, alle Systeme der Musterwerk KWK-Service GmbH und alle Zugänge zu Anlagen unserer Kunden, auch über Lieferanten

Ziel 1: Die Anlagen unserer Kunden laufen sicher weiter, auch wenn bei uns etwas ausfällt. Messgröße: Notbetrieb in der Übung innerhalb von 4 Stunden hergestellt.

Ziel 2: Niemand Unbefugtes erreicht eine Kundenanlage über uns. Messgröße: 100 % der Fernzugriffe über die Plattform, mit persönlichem Konto und Hardware-Schlüssel.

Ziel 3: Wir erkennen Angriffe früh und melden fristgerecht. Messgröße: Alarm des MDR-Dienstes in der Bereitschaft innerhalb von 30 Minuten, BSI-Fristen zu 100 % eingehalten.

4 Grundsätze

Jede Person hat eigene Konten. Zweiter Faktor überall, Hardware-Schlüssel für Fernwartung und Administration.

Fernwartung nur über die zentrale Plattform, nur mit Freigabe je Sitzung und mit Aufzeichnung.

Wer einen Fehler oder Verdacht meldet, wird nicht bestraft. Melden geht vor Aufklären.

Lieferanten mit Zugriff erfüllen unsere Mindestanforderungen, vertraglich geregelt.

Neue Technik und neue Kunden gehen erst nach Prüfung durch die ISB in Betrieb.

Daten werden täglich gesichert, eine Kopie ist für Angreifer nicht veränderbar.

Wir betrachten alle Gefahren: Angriffe, Fehler, Brand, Wasser, Stromausfall und Menschen mit Zugriff.

5 Themenregeln

Kryptografie: Verfahren, Schlüssel und Zertifikate mit Ablaufdatum in der Schlüsselliste; Wartungsberichte und Laptops verschlüsselt (M-24, M-25)

Zutritt und Versorgung: Serverraum nur für Hartl, Wein und Systemhaus; Rauchmelder, Klima-Alarm, USV (M-26, F-13)

Personal: Überprüfung vor Zugriff auf Kundenanlagen, Vertraulichkeit, Austrittsliste (M-27, M-16, M-22)

Protokollierung: Quellen, Aufbewahrung und Auswertung nach Protokollkonzept (M-28, F-15)

Grundkonfiguration: feste Grundeinstellung für Router, Plattform und Laptops, monatlich geprüft (M-30, F-18)

Wechseldatenträger: USB-Speicher gesperrt, Ausnahme nur verschlüsselte Firmensticks (M-32, F-06)

Verantwortung: Die Geschäftsführung ist verantwortlich und überwacht. Die ISB steuert und berichtet. Jeder Mitarbeitende hält die Regeln ein.

Verstöße: werden besprochen; bei Vorsatz oder grober Fahrlässigkeit arbeitsrechtliche Folgen

Überprüfung: jährlich im Management-Review und nach jedem erheblichen Vorfall

Bekanntgabe: Version 2.0 am 05.07.2027, Themenregeln am 26.09.2027 an alle 11 Mitarbeitenden, Kenntnisnahme bestätigt (F-16)

6 Begriffe und Abkürzungen

BSI: Bundesamt für Sicherheit in der Informationstechnik

ISB: Informationssicherheitsbeauftragte oder Informationssicherheitsbeauftragter

KWK: Kraft-Wärme-Kopplung

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

USB: USB-Anschluss

USV: unterbrechungsfreie Stromversorgung, überbrückt kurze Stromausfälle

7 Änderungshistorie und Freigabe

Version	Datum	Änderung	Freigabe
1.0	20.07.2026	Erstfassung im Projektstart	T. Berger

Version	Datum	Änderung	Freigabe
1.1	30.10.2026	Hardware-Schlüssel für alle Fernwartungskonten als Grundsatz	T. Berger
2.0	30.06.2027	Jährliche Überprüfung, Ziele mit Kennzahlen, Lieferkette ergänzt	T. Berger
2.1	28.09.2027	Themenregeln, gefahrenübergreifender Grundsatz	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.

NIS2-MUSTER

F-06 Inventar: Systeme, Dienste, Zugänge

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 Werte, die für den Dienst wichtig sind, mit Verantwortlichen und Schutzbedarf. Grundlage für Risikoanalyse (F-07), Patchregister (F-18) und Notfallplan (F-13). Gepflegt bei jeder Änderung, vollständig geprüft halbjährlich.

2 Dokumentenlenkung

Feld	Eintrag
Dokument-Nr.	MW-ISMS-F-06
Version, Status	1.7, 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 Systeme, Dienste und Zugänge

ID	Wert	Art	Verantwortlich	Schutzbedarf
A-01	Cloud-Büropaket: Mail, Teams, Dateien	Cloud-Dienst	Systemhaus	hoch
A-02	Leitwarten-Server mit Überwachungssoftware	Server	M. Wein	sehr hoch
A-03	Fernwartungsplattform: VPN, Sprungserver	Server	J. Hartl	sehr hoch
A-04	Techniker-Laptops (7) mit BHKW-Software	Endgerät	Systemhaus	hoch
A-05	Smartphones (11)	Endgerät	Systemhaus	normal
A-06	Firewall Büro mit Zonen	Netz	Systemhaus	hoch
A-07	Warenwirtschaft und Auftragsdaten	Cloud-Dienst	S. Lang	normal
A-08	Passworttresor	Cloud-Dienst	J. Hartl	sehr hoch
A-09	Backup-Speicher, unveränderbar	Cloud-Dienst	Systemhaus	sehr hoch

ID	Wert	Art	Verantwortlich	Schutzbedarf
A-10	Bereitschaftstelefon und SMS-Gateway	Dienst	M. Wein	hoch
A-11	Hardware-Schlüssel (24)	Token	J. Hartl	hoch
A-12	Kundendaten: Verträge, Anlagendaten, Wartungsberichte	Daten	S. Lang	hoch
A-13	Ersatzhardware Leitwarte, vorinstalliert	Server	M. Wein	hoch
A-14	MDR-Sensoren und Protokollweiterleitung	Dienst	L-03	hoch
K-01 bis K-91	Mobilfunk-Router bei Kunden, K-01 und K-02 Klinikum	Kundenzugang	J. Hartl	sehr hoch

Die Detailliste der 91 Kundenrouter mit Standort, Firmwarestand, Seriennummer und Ansprechpartner beim Kunden steht in der Plattform und wird monatlich exportiert (Export vom 01.08.2027 abgelegt). Abweichungen zwischen Export und Liste klärt die ISB im Monatsbericht.

✓ Halbjahresprüfung 05.07.2027: alle 14 Werte und 91 Router bestätigt, 3 Abweichungen korrigiert

✓ Jeder Wert hat eine verantwortliche Person oder einen Lieferanten mit Vertrag

✓ Schutzbedarf mit den Kunden-SLA abgeglichen (Klinikum: sehr hoch)

Wechseldatenträger: USB-Speicher an allen Laptops über die Geräteverwaltung gesperrt; vier verschlüsselte Firmensticks für Herstellersoftware, im Inventar unter A-11 geführt, Ausgabe gegen Unterschrift

4 Begriffe und Abkürzungen

BHKW: Blockheizkraftwerk

ISB: Informationssicherheitsbeauftragte oder Informationssicherheitsbeauftragter

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

SLA: vereinbarte Servicezeiten

SMS: Kurznachricht

USB: USB-Anschluss

VPN: verschlüsselter Zugang ins Netz von außen

5 Änderungshistorie und Freigabe

Version	Datum	Änderung	Freigabe
1.0	20.07.2026	Erstfassung im Projektstart	T. Berger

Version	Datum	Änderung	Freigabe
1.1	30.08.2026	Kundenrouter K-01 bis K-85 erfasst	T. Berger
1.2	30.10.2026	Fernwartungsplattform neu, Altzugänge entfernt	T. Berger
1.3	20.01.2027	Zwei Neukunden, Router K-86 bis K-88	T. Berger
1.4	05.04.2027	Ersatzhardware Leitwarte A-13 aufgenommen	T. Berger
1.5	05.07.2027	Halbjahresprüfung, A-05 Smartphones getauscht	T. Berger
1.6	15.08.2027	Neukunden, Router K-89 bis K-91	T. Berger
1.7	28.09.2027	Regel für Wechseldatenträger	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.

NIS2-MUSTER

F-07 Risikoregister

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 bewerteten Risiken für den Dienst mit Wahrscheinlichkeit, Auswirkung, Maßnahmen und Restrisiko. Bewertung vor und nach Maßnahmen, Entscheidung der Geschäftsführung. Methode: W und A je 1 bis 4, Risiko = W × A, akzeptabel bis 4.

2 Dokumentenlenkung

Feld	Eintrag
Dokument-Nr.	MW-ISMS-F-07
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 Risiken und Bewertung

So lesen Sie die Tabelle

Jede Zeile ist ein Risiko für den Dienst. „vorher“ ist das Risiko ohne Maßnahmen, „nachher“ mit Maßnahmen, jeweils Wahrscheinlichkeit mal Auswirkung, beides von 1 bis 4. Bis 4 ist das Risiko vertretbar, darüber braucht es weitere Maßnahmen oder eine Entscheidung der Geschäftsführung.

ID	Risiko	Werte	vorher	Maßnahmen	nachher	Entscheidung
R-01	Technikerkonto per Phishing übernommen	A-01, A-03	16	M-01, M-02, M-07	4	gemindert
R-02	Ransomware legt Leitwarte lahm	A-02, A-12	12	M-04, M-05, M-06	4	gemindert
R-03	Kundenrouter mit alter Firmware im Internet	K-01 bis K-91	12	M-03, M-08	3	gemindert

ID	Risiko	Werte	vorher	Maßnahmen	nachher	Entscheidung
R-04	Gemeinsame Zugangsdaten weitergegeben	A-03	9	M-02, M-03	2	gemindert
R-05	Hersteller-Fernzugang an uns vorbei	K-01 bis K-91	8	M-09, M-19	4	akzeptiert B-09
R-06	Ausfall Systemhaus im Vorfall	A-01, A-06	9	M-10, M-13	4	gemindert
R-07	Laptop mit Kundendaten verloren	A-04, A-12	9	M-11	2	gemindert
R-08	Leitwarte fällt aus, Störung unbemerkt	A-02, A-10	8	M-12, M-13	3	gemindert
R-09	Manipulierte Herstellersoftware auf Laptop	A-04	8	M-04, M-15	4	gemindert
R-10	Insider gibt Anlagendaten weiter	A-12	6	M-02, M-16	3	gemindert
R-11	Lücke in Fernwartungsplattform	A-03	12	M-08, M-14	4	gemindert
R-12	Mobilfunkausfall beim Kunden	K-01 bis K-91	6	M-12	4	akzeptiert B-09
R-13	Admin-Oberfläche Firewall aus Büronetz erreichbar	A-06	9	M-20	2	gemindert
R-14	Sprungserver ohne Aufzeichnung bei Ausfall	A-03	8	M-21	3	gemindert
R-15	Alte Konten nach Austritt aktiv	A-01, A-03	9	M-22	2	gemindert
R-16	KI-Assistent im Büropaket gibt Daten preis	A-01, A-12	6	M-23	3	gemindert
R-17	Brand, Wasser oder Stromausfall im Serverraum	A-02, A-10	8	M-26, M-13	3	gemindert
R-18	Mitarbeiter mit Zugriff handelt gegen uns	A-03, K-01 bis K-91	8	M-27, M-02, M-21	3	gemindert
R-19	Angreifer springt von einem Kunden zum nächsten	A-03, K-01 bis K-91	12	M-29, M-30	3	gemindert
R-20	Schadsoftware über USB-Stick	A-04	6	M-32, M-04	2	gemindert

Legende: Werte = betroffene Werte aus dem Inventar F-06 (A-Nummern); vorher und nachher = Risiko vor und nach den Maßnahmen, Risiko = W × A mit W = Wahrscheinlichkeit 1 bis 4 und A = Auswirkung 1 bis 4, akzeptabel bis 4; Maßnahmen = Nummern aus dem Maßnahmenplan F-08 (M-Nummern).

4 Bewertungsrunden

Datum	Anlass	Teilnehmende	Ergebnis
30.08.2026	Erstanalyse	Hartl, Wein, Berater	12 Risiken, 9 über 4
24.09.2026	Vorfall SV-2026-003	Hartl, MDR-Analyst	R-01 auf W 4 bestätigt, M-01 erweitert
05.02.2027	Pentestbericht	Hartl, Systemhaus, Pentester	3 neue Risiken
30.06.2027	Jahresbewertung	Berger, Hartl, Wein	alle bis auf R-05 und R-12 bei 4 oder darunter
20.09.2027	Externe Prüfung 14.09.2027	Berger, Hartl, Prüfer	gefahrenübergreifend ergänzt: R-17 bis R-20

R-05 und R-12 liegen nach Maßnahmen bei 4 und sind damit im akzeptablen Bereich; die Geschäftsführung hat sie zusätzlich ausdrücklich akzeptiert, weil weitere Senkung nur beim Kunden möglich ist. Nächste Bewertung: 30.06.2028 oder nach einem erheblichen Vorfall.

5 Begriffe und Abkürzungen

KI: künstliche Intelligenz

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

SV: Sicherheitsvorfall (Nummernkreis)

USB: USB-Anschluss

6 Änderungshistorie und Freigabe

Version	Datum	Änderung	Freigabe
1.0	20.07.2026	Erstfassung im Projektstart	T. Berger
1.1	30.08.2026	Erste vollständige Analyse, 12 Risiken	T. Berger
1.2	24.09.2026	Nach SV-2026-003: R-01 neu bewertet	T. Berger
2.0	05.02.2027	Nach Pentest: R-13 bis R-15 neu	T. Berger
2.1	30.06.2027	Jährliche Bewertung, R-16 neu, Restrisiken akzeptiert (B-09)	T. Berger
2.2	28.09.2027	Gefahrenübergreifend ergänzt: R-17 bis R-20	T. Berger
2.3	28.09.2027	Lesehilfe zur Tabelle	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.

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.

NIS2-MUSTER

F-09 Erstaufnahme Sicherheitsereignisse

Beispiel nach einem Jahr Betrieb, Stand 20.08.2027 · 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

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.

2 Dokumentenlenkung

Feld	Eintrag
Dokument-Nr.	MW-ISMS-F-09
Version, Status	1.5, 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, 20.08.2027
Nächste Prüfung	30.06.2028 oder bei wesentlicher Änderung
Vertraulichkeit	intern
Ablage	ISMS-Ordner im Cloud-Büropaket, Bereich 01 Lenkung

3 Ereignisregister

Vorgang	Eingang	Quelle	Beobachtung	Bewertung F-10
SV-2026-001	28.08.2026	MDR	Anmeldeversuche auf Plattform	nicht erheblich
SV-2026-002	14.09.2026	Mitarbeiterin	Phishing-Mail gemeldet, nicht geklickt	nicht erheblich
SV-2026-003	22.09.2026	MDR	Kontoübernahme Techniker	erheblich, gemeldet
SV-2027-001	09.03.2027	Kunde	Router K-41 neu gestartet, Ursache Stromausfall	kein Sicherheitsvorfall
SV-2027-002	02.06.2027	MDR	Schadsoftware auf Laptop blockiert	nicht erheblich
SV-2027-003	16.06.2027	Hersteller	Lücke in Plattform-Software gemeldet	nicht erheblich, F-18
SV-2027-004	19.08.2027	Bereitschaft	Unbekannte Sitzung auf Sprungserver	nicht erheblich, Testkonto Systemhaus

4 Beispiel einer Erstaufnahme: SV-2026-003

Eingang: 22.09.2026, 06:42 Uhr, MDR-Dienst per Telefon und E-Mail

Beobachtung: Anmeldung am Konto des Servicetechnikers S. Kraus aus dem Ausland um 03:15 Uhr, danach neue Weiterleitungsregel im Postfach

Betroffen: Cloud-Konto S. Kraus (A-01), Postfach mit Wartungsberichten mehrerer Kunden (A-12)

Sofortmaßnahmen: 06:50 Konto gesperrt und Sitzungen beendet (Systemhaus); 06:55 Konto auf der Fernwartungsplattform gesperrt (Rufbereitschaft)

ISB alarmiert: 06:58 Uhr

Aufgenommen: P. Neumann, Rufbereitschaft

Lehre aus SV-2027-004: Testkonten der Lieferanten werden vorab angekündigt und mit Ablaufdatum angelegt (F-15). Seitdem keine unangekündigte Sitzung mehr.

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
1.0	20.07.2026	Erstfassung im Projektstart	T. Berger
1.1	22.09.2026	SV-2026-003 aufgenommen	T. Berger
1.2	11.12.2026	SV-2026-001/002 nachgetragen	T. Berger
1.3	09.03.2027	SV-2027-001	T. Berger
1.4	17.06.2027	SV-2027-002 und 003	T. Berger
1.5	20.08.2027	SV-2027-004	T. Berger

Freigegeben: Thomas Berger, Geschäftsführer, 20.08.2027 (im Original unterschrieben). Kostenfreies Muster von OT-Cyber.de, keine Rechtsberatung. Musterbetrieb und Daten frei erfunden.

NIS2-MUSTER

F-10 Bewertung der Erheblichkeit

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

Für jedes Sicherheitsereignis wird nach § 2 Nr. 11 BSIG und für Managed Service Provider nach Art. 3 und 10 der Durchführungsverordnung (EU) 2024/2690 geprüft, ob es erheblich und damit meldepflichtig ist. Ab der Feststellung laufen die Fristen.

2 Dokumentenlenkung

Feld	Eintrag
Dokument-Nr.	MW-ISMS-F-10
Version, Status	1.4, 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 Bewertungen im Überblick

Vorgang	Bewertet	Kriterium erfüllt	Ergebnis	Fristbeginn
SV-2026-001	28.08.2026	keines	nicht erheblich	entfällt
SV-2026-002	14.09.2026	keines	nicht erheblich	entfällt
SV-2026-003	22.09.2026	Art. 10 Nr. 3: Daten böswillig beeinträchtigt	erheblich	22.09.2026, 08:30
SV-2027-002	02.06.2027	keines, Schadsoftware vor Ausführung blockiert	nicht erheblich	entfällt
SV-2027-003	16.06.2027	keines, keine Ausnutzung	nicht erheblich	entfällt
SV-2027-004	19.08.2027	keines, Testkonto Lieferant	nicht erheblich	entfällt

4 Ausführliche Bewertung SV-2026-003

Bewertet von: J. Hartl mit dem MDR-Analysten, 22.09.2026, 08:30 Uhr

Finanzieller Schaden über Schwelle: nein

Abfluss von Geschäftsgeheimnissen: unklar: Wartungsberichte mit Anlagendaten wurden weitergeleitet

Gefahr für Leben oder Gesundheit: nein: kein Zugriff auf Anlagen, Fernwartungskonto durch Hardware-Schlüssel geschützt

Daten durch böswillige Handlung beeinträchtigt: ja: 37 Wartungsberichte von 12 Kunden, darunter das Klinikum

Ergebnis: erheblicher Sicherheitsvorfall nach Art. 10 Nr. 3 DVO; Fristen laufen ab 08:30 Uhr

Gegenzeichnung: T. Berger, 22.09.2026, 09:05 Uhr

Fristbeginn begründet: Der Anruf um 06:42 meldete ein Ereignis; erheblich war es nach der Prüfung um 08:30. Auch ab 06:42 gerechnet sind alle Fristen eingehalten (Frühwarnung nach 4 h 28 min)

Zweifelsfälle bewertet die ISB im Zweifel als erheblich und meldet. Jede Bewertung ist mit Uhrzeit dokumentiert; der MDR-Dienst liefert die technische Einschätzung schriftlich zu.

5 Begriffe und Abkürzungen

BSIG: BSI-Gesetz

DVO: Durchführungsverordnung (EU) 2024/2690 zu NIS2

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
1.0	20.07.2026	Erstfassung im Projektstart	T. Berger
1.1	22.09.2026	Bewertung SV-2026-003	T. Berger
1.2	17.06.2027	SV-2027-002 und 003	T. Berger
1.3	20.08.2027	SV-2027-004	T. Berger
1.4	28.09.2027	Fristbeginn begründet	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.

NIS2-MUSTER

F-11 Meldeprotokoll BSI

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

Belegt jede Meldung an das BSI nach § 32 BSIG mit Zeitpunkt, Inhalt, Absender und Portalreferenz. Fristen: frühe Erstmeldung 24 Stunden, Meldung 72 Stunden, Abschlussmeldung einen Monat nach der Meldung.

2 Dokumentenlenkung

Feld	Eintrag
Dokument-Nr.	MW-ISMS-F-11
Version, Status	1.4, 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 Meldungen an das BSI

Schritt	Frist	Gesendet	Durch	Abstand
Frühwarnung	23.09.2026, 08:30	22.09.2026, 11:10	J. Hartl	2 h 40 min
Meldung	25.09.2026, 08:30	24.09.2026, 15:20	J. Hartl	54 h 50 min
Zwischenmeldung	auf Anforderung	nicht angefordert		
Abschlussmeldung	24.10.2026	20.10.2026	J. Hartl	26 Tage

4 Inhalte

Frühwarnung: Verdacht auf böswillige Handlung ja (Kontoübernahme per Phishing), keine Hinweise auf Auswirkungen in anderen Mitgliedstaaten

Meldung: Kontoübernahme bestätigt; Einstieg über Phishing-Seite mit Abfangen der Sitzung; Weiterleitung von 37 E-Mails an externe Adresse; kein Zugriff auf Plattform oder Kundenanlagen; Schwere mittel; Indikatoren (Absender-Domain, IP-Adressen, Weiterleitungsadresse) übermittelt

Kompromittierungsindikatoren: zwei IP-Adressen des Angreifers und die Domain der Phishing-Seite, in der Meldung und an die betroffenen Kunden gegeben

Abschlussmeldung: Ursache: App-Bestätigung gegen Sitzungsübernahme wirkungslos; Abhilfe: Hardware-Schlüssel für alle (M-01), Weiterleitungen nach außen gesperrt, Routerzugänge der 12 Kunden geändert; keine grenzüberschreitenden Auswirkungen

Portalreferenzen: in der Vorfallakte SV-2026-003 abgelegt, Lesebestätigung des BSI vorhanden

Datenschutz: Meldung an die Aufsichtsbehörde nach Art. 33 DSGVO am 24.09.2026 durch den DSB (L-07)

5 Meldeübung 2027

Am 23.04.2027 wurde die Frühwarnung im Rahmen der Krisenübung (F-13) mit dem Testformular durchgespielt: Vorlage gefunden, Portalzugang funktioniert, Absenden ohne GF über B-05 geklärt. Dauer bis Absendebereitschaft: 38 Minuten.

6 Begriffe und Abkürzungen

BSI: Bundesamt für Sicherheit in der Informationstechnik

BSIG: BSI-Gesetz

DSB: Datenschutzbeauftragte oder Datenschutzbeauftragter

DSGVO: Datenschutz-Grundverordnung

GF: Geschäftsführung

IP: Netzwerkadresse eines Geräts

SV: Sicherheitsvorfall (Nummernkreis)

7 Änderungshistorie und Freigabe

Version	Datum	Änderung	Freigabe
1.0	20.07.2026	Erstfassung im Projektstart	T. Berger
1.1	24.09.2026	Frühwarnung und Meldung SV-2026-003	T. Berger
1.2	20.10.2026	Abschlussmeldung SV-2026-003	T. Berger
1.3	23.04.2027	Meldeübung in der Krisenübung ergänzt	T. Berger
1.4	28.09.2027	Kompromittierungsindikatoren nachgetragen	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.

NIS2-MUSTER

F-12 Information der Kunden

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

Belegt, wann und wie Kunden über Vorfälle und Schwachstellen informiert wurden, die ihre Anlagen oder Daten betreffen. Grundlage: Wartungsvertrag mit Sicherheitsanhang, § 35 BSIG auf Anordnung, eigene Entscheidung.

2 Dokumentenlenkung

Feld	Eintrag
Dokument-Nr.	MW-ISMS-F-12
Version, Status	1.3, 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 Information der Kunden

Vorgang	Empfänger	Weg	Gesendet	Rückmeldung
SV-2026-003	Klinikum (Haustechnik)	Telefon	22.09.2026, 10:15	keine Auffälligkeiten
SV-2026-003	alle 12 betroffenen Kunden	E-Mail	22.09.2026, 14:00	12 von 12 bestätigt
SV-2027-003	alle Kunden mit Fernwartung	E-Mail	16.06.2027, 16:00	Kenntnisnahme 74 von 81

4 Inhalt der Information zu SV-2026-003

Was passiert ist: Das Postfach eines Technikers wurde übernommen, Wartungsberichte wurden weitergeleitet.

Was betroffen ist: Anlagendaten und IP-Adressen Ihrer Anlage, kein Zugriff auf die Anlage selbst.

Was wir getan haben: Konto gesperrt, Zugangsdaten Ihres Routers geändert, Hardware-Schlüssel für alle.

Was Sie tun sollten: eigene Protokolle auf Zugriffe von den beigefügten IP-Adressen prüfen.

Ansprechpartnerin: Julia Hartl, 0123 456780, sicherheit@musterwerk-kwk.example

Erhebliche Cyberbedrohungen: Kunden, die betroffen sein könnten, erhalten die Bedrohung und was sie selbst tun können, auch ohne eigenen Vorfall (Beispiel SV-2027-003)

Rechtsgrund: Wartungsvertrag, Sicherheitsanhang Nr. 4: Information bei Vorfällen mit Bezug zur Anlage innerhalb von 24 Stunden; § 35 BSIG geprüft, keine Anordnung des BSI

Datenschutz: Information der betroffenen Personen nicht nötig, Bewertung des DSB vom 23.09.2026 in der Akte

Freigabe des Textes: J. Hartl und T. Berger, 22.09.2026, 13:40 Uhr

Kunden mit Fernwartung erhalten seit 2027 außerdem einmal im Quartal einen kurzen Sicherheitsbericht: Firmwarestand ihres Routers, Fernzugriffe im Quartal, offene Punkte.

5 Begriffe und Abkürzungen

BSI: Bundesamt für Sicherheit in der Informationstechnik

BSIG: BSI-Gesetz

DSB: Datenschutzbeauftragte oder Datenschutzbeauftragter

IP: Netzwerkadresse eines Geräts

SV: Sicherheitsvorfall (Nummernkreis)

6 Änderungshistorie und Freigabe

Version	Datum	Änderung	Freigabe
1.0	20.07.2026	Erstfassung im Projektstart	T. Berger
1.1	22.09.2026	Information zu SV-2026-003	T. Berger
1.2	16.06.2027	Hinweis zu SV-2027-003	T. Berger
1.3	28.09.2027	Mitteilung erheblicher Cyberbedrohungen	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.

NIS2-MUSTER

F-13 Notfall- und Wiederanlaufplan

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

Wie der Dienst bei Ausfall oder Angriff weiterläuft und wieder anläuft: kritische Dienste mit Ausfallzeiten, Notbetrieb, Reihenfolge, Backup, Krisenteam, Tests und Übungen.

2 Dokumentenlenkung

Feld	Eintrag
Dokument-Nr.	MW-ISMS-F-13
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 Szenarien und Wiederanlauf

Dienst	Max. Ausfall	Datenverlust max.	Notbetrieb
Fernüberwachung 24/7 (A-02)	4 h	1 h	SMS-Störmeldung direkt an Bereitschaft
Fernwartung (A-03)	24 h	24 h	Techniker fahren zur Anlage
E-Mail, Dateien (A-01)	24 h	24 h	Telefon, Bereitschaftsordner
Warenwirtschaft (A-07)	3 Tage	24 h	Aufträge auf Papier

4 Wiederanlauf

1. Firewall (A-06) aus gesicherter Konfiguration
2. Fernwartungsplattform (A-03), Konten prüfen
3. Leitwarten-Server (A-02) aus Backup oder auf Ersatzhardware (A-13)
4. Cloud-Konten (A-01) prüfen, Passwörter neu

5. Warenwirtschaft (A-07)

Serverraum und Versorgung: Zutritt nur für Hartl, Wein und Systemhaus mit Protokoll; Rauchmelder und Klima-Alarm auf das Bereitschaftstelefon; USV 30 Minuten mit geordnetem Herunterfahren

Ausweichbetrieb: Ersatzhardware A-13 im zweiten Brandabschnitt; Leitwarte notfalls vom Laptop über die Cloud

Backup: Leitwarten-Server und Cloud-Daten täglich; eine Kopie 30 Tage unveränderbar (A-09); Konfigurationen Firewall und Plattform wöchentlich

Krisenteam: T. Berger, J. Hartl, M. Wein, Systemhaus; Alarmkette über Bereitschaft, Ausweichkanal verschlüsselter Messenger, gedruckte Kontaktliste im Bereitschaftsordner

5 Tests und Übungen

Datum	Art	Ergebnis	Dauer	Folgemaßnahme
15.10.2026	Wiederherstellung Leitwarte	bestanden	3 h 20 min	Ersatzhardware beschaffen
20.01.2027	Wiederherstellung Cloud-Daten	bestanden	1 h 05 min	keine
23.04.2027	Krisenübung Ransomware Büro	bestanden mit 2 Lehren	4 h	Alarmkette, Ersatzhardware A-13
12.07.2027	Wiederherstellung auf A-13	bestanden	1 h 40 min	keine

Lehren aus der Übung 04/2027: Die Telefonnummer des Systemhauses für Notfälle fehlte auf der gedruckten Liste, und die Wiederherstellung auf Fremdhardware dauerte zu lange. Beides ist erledigt (Liste neu gedruckt, Ersatzhardware A-13 vorinstalliert). Nächste Übung: April 2028, Szenario Ausfall Fernwartungsplattform.

6 Begriffe und Abkürzungen

SMS: Kurznachricht

USV: unterbrechungsfreie Stromversorgung, überbrückt kurze Stromausfälle

7 Änderungshistorie und Freigabe

Version	Datum	Änderung	Freigabe
1.0	20.07.2026	Erstfassung im Projektstart	T. Berger
1.1	15.10.2026	Erster Wiederherstellungstest	T. Berger
2.0	10.05.2027	Nach Krisenübung: Alarmkette und Ersatzhardware	T. Berger
2.1	28.09.2027	Serverraum, Versorgung und Ausweichbetrieb	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.

NIS2-MUSTER

F-14 Lieferantenbewertung

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

Bewertet jeden Lieferanten mit Zugriff auf unsere Systeme oder Kundenanlagen nach Kritikalität, Nachweisen, Meldepflicht und vertraglicher Regelung. Jährliche Wiederholung, bei kritischen Lieferanten mit Nachweisen.

2 Dokumentenlenkung

Feld	Eintrag
Dokument-Nr.	MW-ISMS-F-14
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 Bewertete Lieferanten

ID	Lieferant, Leistung	Zugriff	Kritikalität	Nachweis	Ergebnis 2027
L-01	BHKW-Hersteller, Garantie-Fernzugriff	über Plattform	hoch	IEC 62443-4-1-Zertifikat, Prüfung vor Ort 03/2027	zugelassen
L-02	Systemhaus, Büro-IT	Admin	hoch	ISO 27001	zugelassen
L-03	MDR-Dienst	Protokolle	hoch	ISO 27001, SOC 2	zugelassen
L-04	Mobilfunkanbieter Router-SIM	keiner	mittel	Vertrag	zugelassen
L-05	Anbieter Cloud-Büropaket	Daten	hoch	ISO 27001, C5	zugelassen
L-06	Router-Hersteller	keiner, Firmware	hoch	PSIRT, Advisories	zugelassen mit Auflage
L-07	Externer Datenschutzbeauftragter	Unterlagen	gering	Vertrag	zugelassen

4 Mindestanforderungen an Lieferanten mit Zugriff

✓ Zugriff nur über unsere Plattform mit persönlichem Konto und zweitem Faktor

✓ Meldung von Sicherheitsvorfällen an uns innerhalb von 24 Stunden

✓ Vertraulichkeit und Rückgabe von Daten vereinbart

✓ Nachweis eines Sicherheitsmanagements (Zertifikat oder Selbstauskunft mit Belegen)

✓ Benennung eines Sicherheitskontakts

5 Ablauf der Bewertung

Fragebogen an den Lieferanten mit Frist von vier Wochen

Nachweise prüfen: Gültigkeit, Geltungsbereich, Datum

Kritikalität nach Zugriff und Bedeutung für den Dienst festlegen

Ergebnis: zugelassen, mit Auflage oder nicht zugelassen

Freigabe durch die ISB, bei kritischen Lieferanten zusätzlich durch die GF

Auflage L-06: Der Router-Hersteller veröffentlicht Schwachstellen nur auf Englisch und ohne festen Rhythmus. Die ISB prüft dessen Hinweisseite wöchentlich (F-18). Nächste Bewertung aller Lieferanten: 06/2028.

6 Begriffe und Abkürzungen

BHKW: Blockheizkraftwerk

GF: Geschäftsführung

ISB: Informationssicherheitsbeauftragte oder Informationssicherheitsbeauftragter

IT: Informationstechnik, z. B. Büro-PCs und Server

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

PSIRT: Team, das Sicherheitsmeldungen zu Produkten bearbeitet

SIM: SIM-Karte im Mobilfunk-Router

SOC: Sicherheitsleitstelle, die Alarme auswertet

7 Änderungshistorie und Freigabe

Version	Datum	Änderung	Freigabe
1.0	20.07.2026	Erstfassung im Projektstart	T. Berger
1.1	30.09.2026	Erstbewertung	T. Berger
2.0	30.06.2027	Jahresbewertung 2027	T. Berger

Version	Datum	Änderung	Freigabe
2.1	28.09.2027	Nachweise L-01 verstärkt	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.

NIS2-MUSTER

F-15 Berechtigungen und Fernzugriff

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

Jede Berechtigung auf Plattform, Kundenanlagen und Administratorkonten wird beantragt, freigegeben, befristet, eingerichtet und wieder entzogen. Halbjährlich prüft die ISB alle Berechtigungen.

2 Dokumentenlenkung

Feld	Eintrag
Dokument-Nr.	MW-ISMS-F-15
Version, Status	1.7, 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 Berechtigungen und Fernzugriffe

Antrag	Person	Zugriff	Befristet	Freigabe	Entzogen
03.10.2026	L. Ober	K-01, K-02 bedienen	31.03.2027	Hartl, Klinikum	verlängert
31.03.2027	L. Ober	alle Router bedienen	31.03.2028	Hartl; Klinikum 30.03.2027, übrige Kunden je Wartungsvertrag	
12.11.2026	BHKW-Hersteller	K-17 lesen, Garantie	13.11.2026	Hartl, Kunde	13.11.2026
15.02.2027	Pentester	Plattform Test	19.02.2027	Berger	19.02.2027
28.02.2027	R. Huber (Austritt)	alle		Lang	28.02.2027, 16:00
04.05.2027	BHKW-Hersteller	K-63 Programm ändern	04.05.2027	Hartl, Kunde	04.05.2027
01.07.2027	A. Seidl	Lesezugriff Leitwarte	unbefristet	Hartl	

Antrag	Person	Zugriff	Befristet	Freigabe	Entzogen
21.08.2027	Systemhaus Testkonto	Sprungserver	25.08.2027	Hartl	25.08.2027

4 Halbjahresprüfungen

Datum	Geprüft	Abweichungen	Erledigt
31.01.2027	38 Konten, 24 Schlüssel	1 Konto ohne Nutzung seit 60 Tagen	gesperrt 01.02.2027
31.07.2027	41 Konten, 24 Schlüssel	keine	

5 Regeln

✓ Antrag schriftlich durch die vorgesetzte Person, Freigabe durch die ISB, bei Kundenanlagen zusätzlich durch den Kunden

✓ Rechte nur so weit wie nötig: lesen, bedienen oder Programm ändern, je Anlage

✓ Lieferanten und Testkonten immer befristet, Ablauf technisch hinterlegt

✓ Entzug bei Austritt am letzten Arbeitstag vor 18 Uhr, Hardware-Schlüssel zurück

✓ Administratorkonten getrennt von den Arbeitskonten, nur mit Hardware-Schlüssel

Programmänderungen an Kundenanlagen werden nur mit schriftlicher Freigabe des Kunden für den Einzelfall eingerichtet und am selben Tag entzogen. Die Sitzungen sind aufgezeichnet und 12 Monate gespeichert.

6 Trennung der Kunden auf der Plattform

Aufbau: jeder Kunde in einer eigenen Zone der Plattform; Router eines Kunden erreichen nur den Sprungserver, nie Router anderer Kunden; Rechte je Anlage

Prüfung: Test am 21.09.2027 von einem Testrouter aus: kein Weg zu anderen Kunden, Ergebnis im Prüfbericht; Wiederholung im jährlichen Pentest

7 Protokollierung

Quellen: Plattform und Sprungserver, Firewall, Cloud-Konten, EDR, Leitwarten-Server, Router-Anmeldungen

Aufbewahrung: 12 Monate beim MDR-Dienst, Sitzungsaufzeichnungen 12 Monate, Zugriff nur ISB und MDR

Zeit: alle Systeme gleichen die Uhrzeit mit einem gemeinsamen Zeitserver ab, Abweichung monatlich geprüft

Auswertung: MDR-Dienst rund um die Uhr; ISB monatlich mit Stichprobe von zehn Fernwartungssitzungen

8 Begriffe und Abkürzungen

BHKW: Blockheizkraftwerk

EDR: Schutzsoftware auf Rechnern, die Angriffe erkennt und meldet

ISB: Informationssicherheitsbeauftragte oder Informationssicherheitsbeauftragter

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

9 Änderungshistorie und Freigabe

Version	Datum	Änderung	Freigabe
1.0	20.07.2026	Erstfassung im Projektstart	T. Berger
1.1	05.10.2026	L. Ober eingerichtet	T. Berger
1.2	31.01.2027	Halbjahresprüfung	T. Berger
1.3	28.02.2027	Austritt R. Huber	T. Berger
1.4	31.03.2027	L. Ober unbefristet	T. Berger
1.5	31.07.2027	Halbjahresprüfung	T. Berger
1.6	22.08.2027	Testkonto Systemhaus befristet	T. Berger
1.7	28.09.2027	Kundenfreigabe L. Ober, Trennung der Kunden, Protokollierung	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.

NIS2-MUSTER

F-16 Schulungsnachweis

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

Belegt Schulungen der Geschäftsführung (§ 38 Abs. 3 BSIG) und aller Mitarbeitenden, Phishing-Übungen und die Kenntnisnahme der Leitlinie, jeweils mit Wirksamkeitsprüfung.

2 Dokumentenlenkung

Feld	Eintrag
Dokument-Nr.	MW-ISMS-F-16
Version, Status	1.6, 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 Schulungen und Teilnehmer

Datum	Thema	Teilnehmende	Dauer	Wirksamkeit
18.09.2026	GF: Pflichten, Haftung, Risiken	T. Berger	4 h	Test bestanden
24.09.2026	Team: Phishing, MFA, Melden	10 von 10	2 h	Test 10 von 10
20.10.2026	Phishing-Übung 1	10		1 Klick, 0 Eingaben
10.10.2026	Einweisung L. Ober	1	1 h	Test bestanden
15.02.2027	Phishing-Übung 2	11		0 Klicks
07.06.2027	GF-Auffrischung, Lage 2027	T. Berger, S. Lang	2 h	Test bestanden
14.06.2027	Phishing-Übung 3 (QR-Code)	11		2 Klicks, 0 Eingaben
05.07.2027	Leitlinie 2.0, Neues im ISMS	11 von 11	1 h	Kenntnisnahme 11 von 11
26.09.2027	Themenregeln, USB und Zutritt	11 von 11	30 min	Kenntnisnahme 11 von 11

4 Inhalte der Team-Schulung

Phishing und gefälschte Anmeldeseiten erkennen, auch per QR-Code und Telefon

Hardware-Schlüssel richtig nutzen, Verlust sofort der Bereitschaft melden

Fernwartung nur über die Plattform, keine Freigaben auf Zuruf von Herstellern

Was ein Sicherheitsereignis ist und wie es gemeldet wird (Bereitschaft, F-09)

Umgang mit Kundendaten und Wartungsberichten, keine Weiterleitung an private Adressen

Eigene Fehler melden: Wer meldet, wird nicht bestraft (Leitlinie F-05)

Nachweise: Teilnehmerlisten mit Unterschrift, Testergebnisse und Auswertungen der Übungen in der Akte 07

Nach Übung 3 erhielten die zwei Personen mit Klick eine Kurzschulung zu QR-Codes am 21.06.2027. Nächste Termine: Team-Schulung 09/2027, GF-Schulung 06/2028, Phishing-Übung je Quartal.

5 Begriffe und Abkürzungen

BSIG: BSI-Gesetz

GF: Geschäftsführung

ISMS: Managementsystem für Informationssicherheit

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

QR: QR-Code

USB: USB-Anschluss

6 Änderungshistorie und Freigabe

Version	Datum	Änderung	Freigabe
1.0	20.07.2026	Erstfassung im Projektstart	T. Berger
1.1	24.09.2026	GF- und Team-Schulung	T. Berger
1.2	20.10.2026	Phishing-Übung 1	T. Berger
1.3	15.02.2027	Übung 2, Neueinstellung	T. Berger
1.4	07.06.2027	Auffrischung GF, Übung 3	T. Berger
1.5	05.07.2027	Leitlinie 2.0 bekannt gemacht	T. Berger
1.6	28.09.2027	Themenregeln bekannt gemacht	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.

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.

NIS2-MUSTER

F-18 Schwachstellen- und Patchregister

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

Jede bekannt gewordene Schwachstelle in unseren Systemen und den Kundenroutern mit Quelle, Schwere, Frist, Maßnahme und Nachweis. Fristen: kritisch 7 Tage, hoch 30 Tage, mittel 90 Tage; Ausnahmen nur mit Begründung und Ersatzmaßnahme.

2 Dokumentenlenkung

Feld	Eintrag
Dokument-Nr.	MW-ISMS-F-18
Version, Status	2.5, 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 Schwachstellen und Patches

ID	Quelle	Betroffen	Schwere	Frist	Erledigt
S-2026-011	Hersteller L-06	Router K-01 bis K-85	hoch	06.11.2026	85 von 85 am 03.12.2026
S-2026-014	Advisory Büropaket	A-01	hoch	20.11.2026	automatisch, 25.10.2026
S-2026-017	MDR-Hinweis	A-06 Firewall	kritisch	19.12.2026	13.12.2026
S-2027-002	Hersteller BHKW-Software	A-04 Laptops	mittel	12.04.2027	28.02.2027
S-2027-007	Pentest	A-03 Plattform	mittel	05.05.2027	22.03.2027
S-2027-011	Hersteller L-06	K-01 bis K-88	hoch	14.05.2027	86 bis Frist, 2 bis 30.05.2027
S-2027-015	Advisory Betriebssystem	A-02, A-13	hoch	20.05.2027	06.05.2027
S-2027-019	Hersteller Plattform (SV-2027-003)	A-03	hoch	16.07.2027	24.06.2027

ID	Quelle	Betroffen	Schwere	Frist	Erledigt
S-2027-024	CERT-Bund	A-06	mittel	31.10.2027	15.08.2027
S-2027-026	Hersteller L-06	K-89 bis K-91	mittel	20.11.2027	geplant 09/2027

4 Auswertung Halbjahr 1/2027

Fristgerecht geschlossen: 9 von 10, eine Ausnahme mit Begründung

Ausnahme S-2027-011: zwei Router beim Kunden nur im Wartungsfenster erreichbar; Ersatzmaßnahme: Zugriff in der Zwischenzeit nur ausgehend und überwacht; geschlossen am 30.05.2027

Quellen wöchentlich geprüft: Hersteller-Hinweise L-01 und L-06, CERT-Bund, Hinweise des MDR-Dienstes

5 Grundkonfiguration und Meldestelle

Grundkonfiguration: feste Grundeinstellung je Gerätetyp: Kundenrouter (nur ausgehend, Dienste aus, eigenes Passwort), Plattform und Sprungserver, Laptops, Firewall; monatlicher Abgleich, Abweichung wird Ticket

Abgleich 09/2027: 91 Router, Plattform, 7 Laptops, Firewall: 2 Abweichungen an Laptops, am selben Tag behoben

Meldestelle: Schwachstellen in unseren Diensten an security@musterwerk-kwk.example, veröffentlicht mit security.txt; Eingangsbestätigung in 3 Werktagen

6 Begriffe und Abkürzungen

BHKW: Blockheizkraftwerk

CERT: Team, das auf Sicherheitsvorfälle reagiert (z. B. CERT-Bund, CERT@VDE)

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

SV: Sicherheitsvorfall (Nummernkreis)

7 Änderungshistorie und Freigabe

Version	Datum	Änderung	Freigabe
1.0	20.07.2026	Erstfassung im Projektstart	T. Berger
1.1	07.10.2026	Router-Firmware S-2026-011	T. Berger
2.0	31.01.2027	Fristen festgelegt	T. Berger
2.1	17.06.2027	S-2027-019 Plattform	T. Berger

Version	Datum	Änderung	Freigabe
2.2	05.07.2027	Halbjahresauswertung	T. Berger
2.3	02.08.2027	S-2027-024	T. Berger
2.4	25.08.2027	S-2027-026	T. Berger
2.5	28.09.2027	Grundkonfiguration und Meldestelle	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.