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.