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.