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.