Informationssicherheitsnachweis für Auftragnehmer

(Verpflichtungserklärung / Selbstauskunft)

Version	Datum	Bearbeitungsart / Betroffene Abschnitte	Bearbeiter
1.0	29.07.2020	Freigabe erste Version	J. Holtmannspötter
1.1	04.04.2024	Überarbeitung der Informationssicherheitsbestimmungen, Ergänzung von Punkt 10	E. Alic
1.2	29.04.2024	Anpassung Punkt 2, 6, 8 ,9	B. Läßig
2.0	25.02.2026	Komplette Überarbeitung des Dokuments (allgemein, modular, risikobasiert)	B. Läßig
2.1	03.07.2026	Anpassung: 2.7	B. Läßig

1. Verpflichtungserklärung / Selbstauskunft zur Erfüllung der Informationssicherheit

Dieser Nachweis dient als allgemeiner Informationssicherheitsnachweis in Lieferanten- und Dienstleisterbeziehungen. Der Nachweis ist so aufgebaut, dass er sowohl Vor-Ort-Leistungen als auch Remote- und Cloud/SaaS-Services abdeckt. Bitte füllen Sie die Stammdaten aus, wählen Sie das zutreffende Leistungsmodell und unterzeichnen Sie die Erklärung. Zusatzmodule sind nur auszufüllen, wenn sie zutreffen.

Geltungsdauer: min. 24 Monate ab Unterzeichnung, sofern sich Leistung / Umfang nicht wesentlich ändern. Eine jährliche interne Überprüfung der Verpflichtungserklärung kann im Einzelfall zu Anpassungen sowie zu Rückfragen führen.

1.1 Auftragnehmer Informationen / Stammdaten

Unternehmen / Rechtsform	
Adresse	
Ansprechpartner (fachlich / vertraglich)	
E-Mail / Telefon	
Informationssicherheitskontakt (Security/ ISO)	
E-Mail / Telefon (Securtiy)	
Leistung / Produkt / Service	
Datenstandort / Speicher- & Verarbeitungsort Bitte Land / Region angeben (**nur bei Modul C: Cloud/SaaS**)	
Kreditoren-Nr. (falls vorhanden)	

1.2 Leistungsmodell und Umfang

Bitte wählen Sie das zutreffende Leistungsmodell aus (Mehrfachauswahl möglich):

☐ **A:** Vor-Ort-Tätigkeit auf GELSENWASSER-Grundstücken / Anlagen (z.B. Wartung, Installation)

☐ **B:** Remote-Zugriff auf Systeme / Netze von GELSENWASSER / Beteiligungen / Töchter (z.B. IT-Service, Fernwartung)

☐ **C:** Verarbeitung / Hosting von GELSENWASSER-Informationen in Systemen des Auftragsnehmers (inkl. Cloud / SaaS)

Hinweis: Reine Lieferung (jeglicher Art, z.B. Beratung, Software, Hardware, etc.) ohne Zugriff auf Informationen / Systeme sind von der Verpflichtungserklärung / Selbstauskunft nicht betroffen und benötigen diese nicht.

Betroffene Informationsarten (falls zutreffend):

☐ **keine /** nur **öffentlich** bekannte Informationen

☐ **interne** Informationen

☐ **vertrauliche** Informationen (z.B. Betriebs- / Netzdaten)

☐ **personenbezogene** Informationen / Daten

☐ **KRITIS / OT** relevante Informationen oder Systeme (falls bekannt)

2. Basiserklärung (gültig für alle Leistungsmodelle des Abschnitts 1.2)

Mit der Unterschrift bestätigen wir, dass wir die folgenden Basispflichten einhalten:

2.1 Wir haben organisatorische Regelungen zur Informationssicherheit und eine verantwortliche Stelle / Person.

2.2 Unsere Mitarbeitenden sowie ggf. eingesetzte Unterauftragsnehmende sind zur Vertraulichkeit verpflichtet und werden durch geeignete Schulungs- und Awareness-Maßnahmen angemessen für die Anforderungen der Informationssicherheit sensibilisiert.

2.3 Wir setzen geeignete technische und organisatorische Maßnahmen um (u.a. Rollen- und Rechtekonzept, Prinzip der minimalen Rechte).

2.4 Zugriffe mit erhöhten Rechten werden besonders geschützt (z.B. MFA/2FA, getrennte Konten) und nachvollziehbar protokolliert.

2.5 Sicherheitsrelevante Updates/Patches werden risikobasiert zeitnah eingespielt; kritische Schwachstellen werden priorisiert behandelt.

2.6 Wir verfügen über ein Verfahren zur Erkennung, Behandlung und Meldung von Sicherheitsvorfällen.

2.7 Wir melden Sicherheitsvorfälle, die GELSENWASSER-Informationen oder -Systeme betreffen können, unverzüglich, spätestens innerhalb von 24 Stunden nach Bekanntwerden an: Informationssicherheit@gelsenwasser.de

2.8 Unterauftragnehmer / Subdienstleister werden nur nach vorheriger Bekanntmachung und Zustimmung durch Gelsenwasser eingesetzt.

2.9 Nach Vertragsende werden GELSENWASSER-Informationen nach Weisung zurückgegeben oder sicher gelöscht.

2.10 Der Auftraggeber ist berechtigt, nach vorheriger und gemeinsamer Abstimmung ein Lieferantenaudit durchzuführen. Form, Umfang und Ablauf des Audits werden im Vorfeld einer Anfrage einvernehmlich festgelegt. Der Lieferant unterstützt das Audit in angemessenem Umfang und stellt die hierfür erforderlichen Informationen und Ansprechpartner zur Verfügung.

Abweichungen / Kompensationsmaßnahmen (nur falls erforderlich):

Betroffene Anforderung (Zahl)	Abweichung (kurz beschreiben)	Kompensationsmaßnahme / Hinweis

3. Zusatzmodule (nur ausfüllen, wenn in Abschnitt 1.2 ausgewählt)

3.1 Modul A: Vor-Ort-Tätigkeit

Falls Leistungsmodell A zutrifft, bestätigen wir zusätzlich:

☐ **3.1.1** Wir betreten ausschließlich freigegebene Bereiche und halten Zutritts- / Ausweisregeln sowie Weisungen ein. Arbeiten, die ein informationstechnisches Sicherheitsrisiko darstellen oder in Räumlichkeiten mit bestimmten Zutrittsklassen durchzuführen sind, dürfen grundsätzlich nur unter Aufsicht erfolgen.

☐ **3.1.2** Fotografieren / Filmen sowie das Mitnehmen von Unterlage / Datenträgern erfolgt nur nach Freigabe.

☐ **3.1.3** Arbeitsmittel / Endgeräte werden vor Diebstahl und unbefugter Nutzung geschützt. Es dürfen ausschließlich durch die GELSENWASSER freigegebene Komponenten an das GELSENWASSER-Netzwerk angeschlossen werden.

☐ **3.1.4** Informationen (z.B. Ausdrucke, Pläne, Installationsdokumentationen) werden vertraulich behandelt und nicht unbeaufsichtigt gelassen.

☐ **3.1.5** Ausschließlich zur Erfüllung des Auftrags wird die Möglichkeit eingeräumt, sich am Kommunikationsnetz der GELSENWASSER anzumelden. Der Zugriff ist auf die zur Erfüllung des Auftrags erforderlichen Systeme anzuwenden.

☐ **3.1.6** Eine Erweiterung des GELSENWASSER-Netzwerks ist ohne vorherige Zustimmung nicht erlaubt. Das GELSENWASSER-Netzwerk darf nicht durch eigene Netzwerkkomponenten erweitert werden (LAN-, WAN- oder WLAN-Netzwerk).

3. Zusatzmodule (nur ausfüllen, wenn in Abschnitt 1.2 ausgewählt)

3.2 Modul B: Remote-Zugriff

Falls Leistungsmodell B zutrifft, bestätigen wir zusätzlich:

☐ **3.2.1** Remote-Zugriffe erfolgen ausschließlich über von GELSENWASSER oder vorab gemeinsam freigegebene Verfahren / Verbindungen und nur für den vereinbarten Zweck.

☐ **3.2.2** Es werden nur die erforderlichen Konten / Rechte genutzt; Rechte werden nach Abschluss entzogen bzw. angepasst.

☐ **3.2.3** Endgeräte, von denen aus auf GELSENWASSER zugegriffen wird, sind angemessen geschützt (z.B. Malware-Schutz, Updates, Bildschirmsperre).

☐ **3.2.4** Externe Dateiübertragungen sowie die Nutzung von externen Datenträgern innerhalb der GELSENWASSER-Umgebung sind grundsätzlich nicht zulässig. Sofern diese im Einzelfall erforderlich sind, dürfen sie ausschließlich nach vorheriger ausdrücklicher Freigabe erfolgen.

☐ **3.2.5** Wir unterstützen die Aufklärung von Sicherheitsvorfällen durch Bereitstellung relevanter Informationen (z.B. Logs), soweit verfügbar und zulässig.

3. Zusatzmodule (nur ausfüllen, wenn in Abschnitt 1.2 ausgewählt)

3.3 Modul C: Verarbeitung / Hosting (inkl. Cloud / SaaS)

Falls Leistungsmodell C zutrifft, bestätigen wir zusätzlich:

☐ **3.3.1** Daten werden bei Übertragung verschlüsselt (z.B. TLS) und bei Speicherung angemessen geschützt (z.B. Verschlüsselung oder gleichwertig).

☐ **3.3.2** Mandanten- / Kundentrennung ist umgesetzt, sofern mehrere Kunden dieselbe Plattform nutzen.

☐ **3.3.3** Backup und Wiederherstellbarkeit sind umgesetzt; Wiederherstellung wird angemessen getestet.

☐ **3.3.4** Verfügbarkeit wird entsprechend der vereinbarten Service Levels durch geeignete Maßnahmen unterstützt (z.B. Monitoring, Redundanzen, Notfallplanung).

☐ **3.3.5** Schwachstellen werden regelmäßig identifiziert (z.B. Scans / Penetrationstests) und behandelt; wesentliche Findings werden nachverfolgt.

☐ **3.3.6** Protokollierung / Monitoring sicherheitsrelevanter Ereignisse ist eingerichtet und Logdaten werden geschützt.

☐ **3.3.7** Speicher- und Verarbeitungsort der Daten liegt ausschließlich in der EU (inkl. Deutschland); eine Verarbeitung außerhalb der EU erfolgt nur nach vorheriger schriftlicher Zustimmung von GELSENWASSER. Wesentliche Änderungen werden vorab kommuniziert.

☐ **3.3.8** Unterauftragnehmer (z.B. Cloud-Provider) werden risikobasiert gesteuert; für kritische Unterauftragnehmer können Nachweise bereitgestellt werden.

4. Nachweise (optional / falls vorhanden beifügen)

Bitte kreuzen Sie an, welche Nachweise Sie beifügen können / wollen.

Hinweis: Sollten Sie den vorstehenden Abschnitten 2 und 3 nicht zustimmen, sind die entsprechenden Nachweise verpflichtend einzureichen. Diese werden durch den bzw. die Informationssicherheitsbeauftragte*n geprüft und bei erfolgreicher Prüfung mit einer Ausnahmeregelung, der sogenannten „Offerte ohne IS-Nachweis“ versehen.

☐ **4.1** ISO / IEC 27001 Zertifikat (oder gleichwertig)

☐ **4.2** SOC 2 (Type II) oder vergleichbarer Auditbericht

☐ **4.3** BSI C5 Testat (Cloud) oder vergleichbares Testat

☐ **4.4** Sonstiges: _____

5. Unterschriften (bitte den Punkt streichen, der nicht zutrifft)

Wir bestätigen,

5.1 dass die oben gemachten Angaben vollständig und zutreffend sind und dass wir die für uns zutreffenden Anforderungen (Basiserklärung und zutreffende Zusatzmodule) einhalten.

oder

5.2 einen entsprechenden gleichwertigen Nachweis unverzüglich verpflichtend einreichen; damit gelten die Verpflichtungen als nicht akzeptiert und eine Ausnahmeregelung „Offerte – ohne IS-Nachweis“ wird beantragt.

Wir informieren GELSENWASSER, falls sich wesentliche Aspekte (Leistungsmodell, Subdienstleister, Datenarten, Sicherheitsniveau) ändern.

Ort, Datum	
Name / Funktion (zeichnungsberechtigt)	
Unterschrift	