Vereinbarung zur Informationssicherheit

(nachfolgend „Vereinbarung“)

zwischen der

GASCADE Gastransport GmbH
Kölnische Straße 108 - 112
34119 Kassel

– nachfolgend „GASCADE“ genannt –

und der

XXX
XXX
XXX

– nachfolgend „Auftragnehmer“ genannt –

oder Auftraggeber und Auftragnehmer nachfolgend gemeinsam „Parteien“ oder einzeln „Partei“ genannt

GASCADE ist gemäß § 5c EnWG zu einem sicheren Betrieb des Energieversorgungsnetzes verpflichtet. Dies umfasst insbesondere auch einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme. Darüber hinaus ist das von GASCADE betriebene Pipelinenetz als kritische Infrastruktur gemäß der Verordnung zur Bestimmung kritischer Infrastrukturen (BSI-KritisV) einzustufen. GASCADE ist daher verpflichtet ein Informationssicherheitsmanagementsystems („ISMS-Management“) nach ISO/IEC 27001 zu betreiben und die Anforderungen des IT-Sicherheitskatalog für Strom- und Gasnetze der Bundesnetzagentur (BNetzA) zu erfüllen.

Die Parteien haben einen Vertrag über XXX (nachfolgend „Vertrag“) geschlossen. Die nach dem Vertrag vom Auftragnehmer zu erfüllenden Leistungen unterfallen dem Anwendungsbereich des ISMS-Managements von GASCADE. Vor diesem Hintergrund vereinbaren die Parteien zur Wahrung der Informationssicherheit das Folgende:

1. Der Auftragnehmer versichert, dass ihm die Vorgaben der einschlägigen Sicherheitsstandards - insbesondere der ISO/IEC 27001, des BSI Grundschutzes und des IT-Sicherheitskataloges der BNetzA für Strom- und Gasnetze - bekannt sind und der Auftragnehmer die darin formulierten Anforderungen in seinen Betriebsprozessen beachtet.

2. Der Auftragnehmer hat bei der Erfüllung des Vertrages die in Anlage 1 zu dieser Vereinbarung bestimmten „Anforderungen an Dienstleister und Lieferanten zur Gewährleistung der Informationssicherheit“ (Anlage 1) in eigener Verantwortung zu erfüllen.

   Das gleiche gilt für die dem Auftragnehmer im Zusammenhang mit der Durchführung des Vertrages vom Auftraggeber bekannt gemachten und ausgehändigten IT-Sicherheitsrichtlinien der GASCADE Gastransport GmbH. Soweit der Auftragnehmer feststellt, dass er die in diesen IT-Sicherheitsrichtlinien bestimmten Anforderungen nicht erfüllen kann, wird er den Auftraggeber unverzüglich mindestens in Textform darauf hinweisen und mit dem Auftraggeber zusammenwirken, eine alternative Verfahrensweise zu entwickeln, um eine Gefährdung der IT-Sicherheit des Auftraggebers zu vermeiden.

3. Über die in Ziffer 2 beschriebenen hinausgehende Anforderungen an die Informationssicherheit können vertraglich vereinbart werden.

4. Werden durch den Auftragnehmer Informationssicherheits- oder Betriebsprozesse an ein anderes Unternehmen ausgelagert, muss diese dritte Partei mindestens GASCADE gegenüber benannt werden. Auf Anfrage von GASCADE muss der Auftragnehmer darlegen, inwiefern derartige Prozesse ausgelagert werden.

5. Der Auftragnehmer sichert zu, dass die zur Durchführung des Vertrages von ihm eingesetzten Mitarbeiter jeweils vorab mit den bei GASCADE geltenden Sicherheitsstandards und Betriebsprozessen vertraut gemacht werden, insbesondere indem der Auftragnehmer die in Ziffer 2 genannten Dokumente an die Mitarbeiter aushändigt und sie zur Einhaltung der dort bestimmten Regelungen zur Informationssicherheit unterweist.

6. Der Auftragnehmer benennt folgenden Ansprechpartner zur Informationssicherheit:

   Name, Vorname: _____

   E-Mail, Telefon: _____

7. Mündliche Nebenabreden sind nicht getroffen. Alle die Vereinbarung betreffenden Abreden, Änderungen und/oder Ergänzungen bedürfen aus Beweisgründen der Schriftform.

8. Diese Vereinbarung unterliegt dem Recht der Bundesrepublik Deutschland. Ausschließlicher Gerichtsstand für alle Streitigkeiten auf Grund oder im Zusammenhang mit dieser Vereinbarung ist - soweit sich nicht aus zwingenden gesetzlichen Bestimmungen Abweichendes ergibt - Kassel.

Kassel, den_____ _____, den_____

GASCADE Gastransport GmbH XXX

v. d. Grün Fink XXX

Anlage 1 zur Vereinbarung zur Informationssicherheit

Anforderungen an Dienstleister und Lieferanten zur Gewährleistung der Informationssicherheit der GASCADE Gastransport GmbH und NEL Gastransport GmbH

Die hier formulierten Anforderungen sind für Dienstleister und Lieferanten der GASCADE Gastransport GmbH und der NEL Gastransport GmbH verbindlich. Zur Verbesserung der Lesbarkeit und Übersichtlichkeit wird im Folgenden nur die GASCADE Gastransport GmbH („GASCADE“) erwähnt. Dennoch gelten alle Regelungen auch für die NEL Gastransport GmbH. Sofern im Einzelfall anderes gilt, wird darauf hingewiesen.

Die Sicherheitsanforderungen zur Gewährleistung der Informationssicherheit der GASCADE Gastransport GmbH sind im Rahmen der Auftragserfüllung, insbesondere bei Tätigkeiten an Informationstechnischen Systemen und im Umgang mit Informationswerten der GASCADE zu beachten und einzuhalten.

(1) Zulässiger Gebrauch von Informationssystemen und anderer Informationswerte von GASCADE

(a) Als Informationswerte gelten neben dem Informationssystem auch andere Informationen und Betriebsmittel, wie z.B. Papier- und digitale Dokumente, mobile Computer und Speichermedien.
(b) Informationswerte dürfen ausschließlich zur geschäftlichen Erfüllung und Bearbeitung von Aufgaben der GASCADE verwendet werden.
(c) Eine Nutzung der Informationswerte, welche unnötigerweise Kapazitäten belegt, die die Leistungsfähigkeit des Informationssystems beeinträchtigt oder eine Sicherheitsbedrohung für GASCADE darstellt, ist grundsätzlich untersagt.
(d) Erteilte Zugangsberechtigungen für Informationssysteme sind ausschließlich durch berechtigte und unterwiesene Mitarbeiter des Auftragnehmers im Rahmen der vereinbarten Nutzung zu verwenden.
(e) Die Nutzung sämtlicher von GASCADE bereitgestellter Informationssysteme, Kommunikationsmittel, Laufwerke, Ablagesysteme und Anwendungen (z.B. E-Mail, Postfächer, Festnetz, Mobiltelefone, Internetzugang, SharePoint sowie Word-, Excel- und sonstige IT-Systeme) ist ausschließlich für dienstliche Zwecke zulässig. Eine private Nutzung, insbesondere für private Telefongespräche oder die Speicherung, Verarbeitung oder Übermittlung nicht dienstlicher Inhalte, ist unzulässig. Soweit mehrere Personen auf Funktionslaufwerke, Funktionspostfächer oder sonstige gemeinsame Ablagesysteme zugreifen können, ist der Zugriff auf den dienstlich erforderlichen Umfang beschränkt. Die Nutzung unterliegt den bei GASCADE jeweils geltenden internen Vorgaben, Richtlinien und Weisungen zur Informationssicherheit und zur Nutzung organisationseigener Werte in ihrer jeweils aktuellen Fassung, soweit diese dem Auftragnehmer für die Durchführung des Vertrages bekannt gemacht oder zur Verfügung gestellt wurden.

(f) Die Ausführung von Tätigkeiten, die eine Gefährdung des Informationssystems zur Folge haben, sind zu unterlassen (u.a. Installation von nicht durch GASCADE freigegebener Software).
(g) Ausschließliche Nutzung von Kommunikationsverbindungen, Hardware, Software und Informationen im Rahmen der vereinbarten Nutzungsrechte.
(h) Der Auftragnehmer darf Informationswerte der GASCADE nicht durch KI verarbeiten, es sei denn, GASCADE hat dies zuvor ausdrücklich in Textform freigegeben; eine Freigabe gilt auch als erteilt, soweit die Nutzung von KI-Funktionalitäten Gegenstand der vertraglich vereinbarten Leistungen ist.

(2) Operationelle Sicherheit

(a) Ausschließliche Verwendung von Datenträgern (Externe Datenträger, USB-Sticks, CD's und DVD's) an mit der GASCADE Infrastruktur verbundenen, informationstechnischen Systemen, die unmittelbar vor der Verwendung auf Schadprogramme geprüft wurden.
(b) Sicherstellung, dass bei einer Verbindung von externen informationstechnischen Systemen mit der GASCADE Infrastruktur (z.B. zum Upload/Download von Dateien, Parametrierungsdaten und Konfigurationen, Abrufen von Messwerten oder Bereitstellung von Software etc.) diese zum Zeitpunkt der Installation auf dem aktuellsten Stand sind (Softwareversionen, Betriebssysteme) und über einen aktuellen Virenschutz verfügen.
(c) Sicherstellung von regelmäßigen Update- und Patch- Prozessen (Softwarekomponenten, Betriebssystem, Virenschutz) für die, mit der GASCADE Infrastruktur verbundenen, informationstechnischen Systemen.
(d) Sicherstellung, dass bei Inbetriebnahme von informationstechnischen Systemen für GASCADE oder im Rahmen von beauftragten Aktualisierungen nicht genutzte Dienste, Management-Schnittstellen, Ports und Softwarekomponenten deaktiviert werden. Alle unverschlüsselten Dienste (z.B. http, telnet, …) sind, wenn nicht zwingend betrieblich erforderlich, zu deaktivieren.
(e) Sicherstellung, dass bei Austausch, Außerbetriebnahme und Entsorgung von GASCADE Infrastrukturkomponenten (z.B. Server, Speichersysteme, externe Datenträger, Speichermedien und Netzwerkkomponenten) Standards zur sicheren Entsorgung, Löschung bzw. Zerstörung von GASCADE-Daten und Konfigurationen berücksichtigt werden.
(f) Sicherstellung, dass die, dem Auftragnehmer zu Prüf- oder Testzwecken bereitgestellte, GASCADE-Daten und Konfigurationen nach Abschluss der Prüfungen vollständig gelöscht werden.
(g) Sicherstellung, dass die im Rahmen der Auftragserfüllung vereinbarte Datensicherungs- und Wiederherstellungsprozesse implementiert sind und regelmäßig getestet sowie Änderungen dokumentiert werden.

(3) Clean Workplace

(a) Vor dem Verlassen des Arbeitsplatzes müssen alle sensiblen Informationen vom Schreibtisch und anderen Plätzen (Drucker, Kopierer, Scanner, etc.) entfernt und für andere unzugänglich gemacht sowie vor unbefugtem Zugriff während der Abwesenheit geschützt werden.
(b) Vor dem Verlassen des Arbeitsplatzes muss sichergestellt werden, dass keine sensiblen Informationen auf dem Bildschirm dargestellt werden und kein Zugriff auf Systeme besteht, zu welchen der Auftragnehmer über Zugriffsberechtigungen verfügt. Gemeinsam genutzte Gerätschaften müssen vor unbefugter Verwendung geschützt werden.
(c) Nach Besprechungen dürfen keine vertraulichen Informationen zurückgelassen werden.
(d) Für vertrauliche und streng vertrauliche Informationen gelten besondere Schutzmaßnahmen. Für die Vorgaben zur Übermittlung und Aufbewahrung von vertraulichen und streng vertraulichen Informationen wenden Sie sich bitte an ihren Ansprechpartner bei GASCADE.

(4) Benutzerkonten und Kennwörter

(a) Benutzerkonten sind grundsätzlich personalisiert und dürfen nicht geteilt werden. Für Empfang und Poststelle sind hiervon ausschließlich die von GASCADE eingerichteten Funktionsbenutzer und Funktionspostfächer als eng begrenzte Ausnahme zulässig. Die Nutzung dieser Funktionszugänge ist auf einen festgelegten, unterwiesenen und zur Aufgabenerfüllung erforderlichen Personenkreis zu beschränken; Zugangsdaten sind geheim zu halten, vor unbefugtem Zugriff zu schützen und bei personellen Änderungen oder Verdacht auf Kenntniserlangung durch Unbefugte unverzüglich über GASCADE-FM ändern zu lassen. Eine weitergehende Weitergabe oder sonstige Nutzung ist unzulässig.
(b) Die Prüfung von Benutzerkonten sowie die Meldung von Benutzern oder sonstigen Änderungen erfolgt mindestens jährlich und über das Facility Management. Nicht mehr benötigte Benutzerkonten sind unverzüglich, insbesondere bei Ausscheiden eines Mitarbeiters, an das Facility Management zu melden.
(c) Kennwörter müssen mindestens 12 Zeichen aus mindestens 3 verschiedenen der 4 üblichen Zeichenkategorien enthalten: Großbuchstaben, Kleinbuchstaben, Zahlen und nicht-alphanumerische Zeichen.
(d) PINs müssen mindestens 4 Ziffern im Rahmen der PKI, sonst 6 Ziffern enthalten.
(e) Kennwörter und PINs sind stets geheim zu halten und vor unbefugtem Zugriff zu schützen.
(f) Kennwörter sind regelmäßig zu wechseln, hierbei gelten folgende Wechselintervalle:
    a. Benutzerkonto alle 6 Monate
    b. Administratorenkonto alle 3 Monate

(5) Ansprechpartner und Meldeweg für Informationssicherheitsvorfälle

(a) Erhebliche Sicherheitsvorfälle: Ein Vorfall gilt als erheblich, wenn er einen erheblichen Schaden durch den Verlust der Vertraulichkeit oder Integrität von Informationen verursachen kann oder der eine Unterbrechung der Verfügbarkeit von Informationen und/oder Prozessen über eine inakzeptable Zeitspanne verursachen könnte.

Erkannte **Sicherheitslücken und erhebliche Sicherheitsvorfälle, die eine Beeinträchtigung der GASCADE zur Folge haben könnten**, sind **unverzüglich** an das Computer Emergency Response Team („CERT“) zu **melden**, dies ist wie folgt zu erreichen:

CERT (24x7)	**0561/934-4444**	cert@gascade.de

Das CERT der GASCADE ist bei allen erheblichen Vorfällen zu informieren und 24x7 unter der genannten Rufnummer erreichbar. Die Aufgabe der CERT-Rufbereitschaft ist die Analyse und Bewertung von eingehenden IT-Security-Events und die Behebung von Informationssicherheitsvorfällen im Tagesbetrieb und im Rahmen einer Rufbereitschaft.

(b) Geringer Vorfall: Liegt ein geringer Vorfall vor, der keine bedeutende Auswirkung auf die Vertraulichkeit oder Integrität von Informationen hat und keinen längerfristigen Ausfall der Verfügbarkeit verursachen kann, muss dieser über den Service Desk gemeldet werden. Der **Service Desk** der GASCADE ist werktags immer von 08:00-17:00 unter folgenden Kontaktdaten erreichbar:

Service Desk	0561/934-1010	1010@gascade.de

(c) Die **Informationssicherheitsbeauftragte** ist Ansprechpartnerin zur Informationssicherheit.

Lara Berdelsmann	0561/ 934-2854	Lara.Berdelsmann@gascade.de