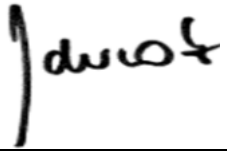
Neuss-Düsseldorfer Häfen GmbH & Co. KG

Informationssicherheitsleitlinie für Lieferanten

Klassifizierung:	öffentlich		Dokumentverantwortlich:	ISB	
Version:	1.0		Status:	freigegeben	
Freigabe am: 10.02.2026			Freigegeben von: 	Sascha Odermatt	
Letzte freigegebene Version:	1.0				

Inhaltsverzeichnis

1 Einleitung

Die Neuss-Düsseldorfer Häfen GmbH & Co. KG (NDH) sieht den Stellwert und die Unabdingbarkeit der Informationssicherheit für sich und ihr geschäftliches Umfeld. Entsprechend betreibt die Neuss-Düsseldorfer Häfen GmbH & Co. KG ein Informationssicherheitsmanagementsystem nach DIN EN ISO / IEC 27001:2022.

Die NDH ist sich der wachsenden Bedrohungslage bewusst und nimmt diese ernst. Entsprechend sehen wir die Notwendigkeit der Maßnahmenergreifung, insbesondere im Hinblick auf die Supply-Chain-Security, und definieren im Folgenden die grundlegende Erwartungshaltung an unsere Lieferanten, Dienstleister und Partner. Sie gilt als Orientierungshilfe für eine gemeinsame Sicherheitskultur und gilt für alle Organisationen, die Leistungen für uns erbringen oder auf unsere Informationen zugreifen.

2 Gemeinsames Grundverständnis

Informationssicherheit genießt bei uns einen sehr hohen Stellenwert und wird als integraler Bestandteil für verantwortungsvolles und nachhaltiges Wirtschaften verstanden. Sowohl der Schutz von vertraulichen Daten, als auch die Sicherstellung der Verfügbarkeit von Informationen und ihrer Integrität sind für uns von elementarer Bedeutung.

Wir verstehen Informationssicherheit als umfassendes System und als ein dynamisches Feld, das konsequente Beobachtung und eine stetige, unternehmensseitige Anpassung erfordert. Eine entsprechende Haltung erwarten wir auch von unseren Lieferanten.

3 Generelle Erwartungshaltung

Zur Sicherstellung und Wahrung eines gemeinsamen Mindestmaßes im Hinblick auf Informationssicherheit verpflichten sich unsere Lieferanten zu folgendem, grundlegenden Sicherheitsverhalten:

3.1 Wahrung der Schutzziele der Informationssicherheit

Die grundlegenden Schutzziele der Vertraulichkeit, der Verfügbarkeit und der Integrität von Informationen sind zu wahren. Für die einzelnen Schutzziele konkretisiert sich dies wie folgt:

3.1.1 Schutzziel der Vertraulichkeit

Sämtliche Informationen sind so zu behandeln, dass diese ausschließlich dem für sie bestimmten Empfängerkreis zugänglich gemacht werden können. Unbefugter Zugriff oder Offenlegung über den definierten Adressatenkreis hinaus ist zu unterbinden.

3.1.2 Schutzziel der Verfügbarkeit

Die Verfügbarkeit von Informationen ist in dem Maße sicherzustellen, dass diese stets dann zur Verfügung stehen, wenn diese vom berechtigten Empfängerkreis benötigt werden.

3.1.3 Schutzziel der Integrität

Der Schutz der Integrität sämtlicher Informationen ist zu wahren. Es wird sichergestellt, dass Informationen korrekt, vollständig und unverfälscht sind, unabhängig ihres Status.

3.2 Awareness

Es wird erwartet, dass eine regelmäßige und kontinuierliche Beschäftigung mit dem Thema der Informationssicherheit, insbesondere mit deren Bedrohungslage stattfindet und hieraus proaktiv Schlussfolgerungen und Maßnahmen abgeleitet werden.

3.3 Sicherstellung des Verständnisses und der Qualifizierung von Mitarbeitenden

Es ist sicherzustellen, dass die eingesetzten Mitarbeitenden ein angemessenes und zur Ausübung ihrer Tätigkeiten notwendiges, fach- und sachgerechtes Verständnis der Informationssicherheit aufweisen und in der Lage sind sich sicherheitskonform zu verhalten.

3.4 Technische und organisatorische Maßnahmen (TOM)

Wir erwarten eine adäquate Umsetzung von technischen und organisatorischen Maßnahmen zur Sicherstellung der Informationssicherheit, insbesondere in den Bereichen

- Zugangskontrolle und Berechtigungsmanagement
- Identitätsmanagement
- Datenverschlüsselung
- Schwachstellenmanagement
- Schutz vor Schadsoftware
- Backup – und Wiederherstellung
- Schulung und Sensibilisierung von Mitarbeitenden
- Arbeitsplatz- und Geräteschutz
- Cloud- und Dienstleistersicherheit
- Überwachung und Kontrolle

4 Meldung informationssicherheitsrelevanter Vorfälle

Sicherheitsvorfälle mit potenziellem Bezug zu den Informationen oder Systemen der Neuss-Düsseldorfer Häfen GmbH & Co. KG sind unverzüglich zu melden. Es wird ein transparenter und kooperativer Umgang mit Sicherheitsvorfällen erwartet. Im Zuge dessen ist ein entsprechender Ansprechpartner, respektive eine Kontaktstelle zu benennen.

5 Vertragsgrundlage und Recht auf Überprüfung

Diese Leitlinie bildet die Grundlage für unsere vertraglichen Sicherheitsanforderungen. Wir behalten uns das Recht auf Überprüfung der Einhaltung durch Nachweise und / oder Auditierung vor. Wir setzen hierbei auf eine partnerschaftliche und vertrauensvolle Zusammenarbeit.

6 Weiterentwicklung und Zusammenarbeit

Die Wahrung der Informationssicherheit ist ein kontinuierlicher Prozess. Entsprechend erwarten wir von unseren Partnern, dass sie sich proaktiv und kontinuierlich mit ihrem Verbesserungspotenzial auseinandersetzen und offen für gemeinschaftliche Verbesserungen sind.

7 Dokumentenhistorie

Version	Änderungsdatum	Geändert von	Änderung
0.1	16.01.2026	Alexander Neiken	Dokument erstellt
0.1	20.01.2026	Hans Oberlechner	Dokument geprüft
1.0	10.02.2026	Sascha Odermatt	Freigabe