# Informationssicherheitsrichtlinie für Lieferanten & Auftragnehmer

## Inhaltsverzeichnis



# Tabellenverzeichnis

# 1. Übersicht

Dieses Dokument ist ein Arbeitsergebnis, das im Rahmen der Informationssicherheitstätigkeiten der Niedersächsischen Hafengesellschaften erarbeitet wurde, namentlich:

**Niedersachsen Ports GmbH & Co. KG** **(NPorts)**

**JadeWeserPort Realisierungs GmbH & Co. KG** **(JWP-R)**

**Container Terminal Wilhelmshaven JadeWeserPort-Marketing GmbH & Co. KG** **(JWP-M)**

Die vorgenannten Gesellschaften werden nachfolgend zusammengefasst als

**„Hafengesellschaften (NPorts & JWP)“** bezeichnet. **(NPorts & JWP)**

## 1.1 Verantwortlichkeiten

Die Verantwortung für die Einhaltung dieser Richtlinie unterliegt den Auftragnehmern (z.B. Lieferanten und Dienstleitstern).

Der Ansprechpartner beim Auftragnehmer ist für das Einhalten dieser Richtlinie beim Auftragnehmer verantwortlich. Verstöße sind dem Ansprechpartner der Hafengesellschaften (NPorts & JWP) (z.B. dem Projektleiter; dem ISMS-Koordinator; der IT; dem zuständigen Einkauf) zu melden.

Der Auftragnehmer ist für alle Belange der Informationssicherheit verantwortlich, die sich auf seine Geschäftsbeziehung mit den Hafengesellschaften (NPorts & JWP) auswirken bzw. direkten Einfluss haben. Der Ansprechpartner innerhalb der Hafengesellschaften (NPorts & JWP) wird dem Auftragnehmer im Rahmen der Vertragsbeziehung genannt und steht als Ansprechpartner für Fragen zum ISMS zur Verfügung.

## 1.2 Zweck, Anwendungsbereich und Benutzer

Das Ziel dieses Dokuments ist die Festlegung zum Informationssicherheitsmanagement (ISMS) so zusammenzufassen, dass Auftragnehmer (Lieferanten bzw. externen Dienstleister) ein Grundverständnis für das ISMS der Hafengesellschaften (NPorts & JWP) entwickeln können. Es wird erwartet, dass die Auftragnehmer der Hafengesellschaften (NPorts & JWP) sich konform zu den Anforderungen dieser Leitlinie und allen daraus abgeleiteten Sicherheitsanweisungen verhalten. Es gilt für alle informationsverarbeitenden Systeme (IT, Anwendungen etc.) die für Kunden der Hafengesellschaften (NPorts & JWP) bereitgestellt oder auf denen Kundendaten verarbeitet werden, sowie für klassifizierte Dokumente, Informationen und Standorte. Es gilt ebenfalls für alle den Hafengesellschaften (NPorts & JWP) eigenen, informationsverarbeitenden Systeme und Netzwerke, Dokumente und Informationen.

Die Freigabe dieses Dokumentes ersetzt alle früheren Versionen und Ausgaben.

Sollten vertragliche oder gesetzliche Festlegungen dieses Dokuments oder Teile hiervon berühren, haben diese in jedem Fall Vorrang.

Die Einbindung von externen Parteien in die Geschäftsabläufe der Hafengesellschaften (NPorts & JWP) gehört zu den regelmäßigen Anforderungen, um effektiv, effizient und erfolgreich agieren zu können. Die Aufrechterhaltung der Sicherheit und der Schutz unserer Informationswerte darf hierbei jedoch nicht

negativ beeinflusst oder gefährdet werden. Hierzu beschreibt das vorliegende Dokument einige Aspekte und Faktoren, welche in die betrieblichen Abläufe und Prozesse integriert werden sollten. Es werden Hinweise und Anforderungen an Vereinbarungen und Verträge aufgezeigt, die bei geschäftsmäßigen Bindungen zwischen den Unternehmen der Hafengesellschaften (NPorts & JWP) und externen Organisationen und Unternehmen im weitesten Sinne Berücksichtigung finden können.

# 2. Stellenwert der Informationsverarbeitung und Informationssicherheit im Unternehmen

Die Informationsverarbeitung ist für die Aufgabenerfüllung der wesentlichen strategischen und operativen Funktionen, Aufgaben und Dienstleistungen maßgeblich. Nur durch den Einsatz von IT-Systemen können die Hafengesellschaften (NPorts & JWP) ihre Geschäftsziele erreichen. Fallen diese Systeme aus, sind gestört oder kompromittiert, stellt dies eine hohe Gefahr für das Unternehmen dar.

Informationen können elektronisch, auf Papier oder auch in Köpfen vorhanden sein. Ausschließlich technische Sicherheitslösungen sind aus diesem Grund unzureichend. Voraussetzung für ein angemessenes Sicherheitsniveau ist eine geplante, strukturierte und organisierte Vorgehensweise im Umgang mit Informationen. Diese Planungs-, Lenkungs- und Kontrollaufgabe wird als Informationssicherheitsmanagement oder auch kurz als ISMS bezeichnet.

Die Erfüllung der Dienstleistungsverträge und aller damit verbundenen Leistungen steht im Mittelpunkt der täglichen Arbeit. Informationen in jeglicher Form, elektronisch gespeichert, oder elektronisch übertragen, auf Papier ausgedruckt, geschrieben oder in Gesprächen weitergegeben, sind unabhängig ihrer gewählten Form, dem Medium der Weitergabe oder der Speicherung immer an-gemessen zu schützen.

Der Schutz der IT-Systeme, die Verfügbarkeit der zu verarbeiteten Daten, Vertraulichkeit und Integrität haben daher einen hohen Stellenwert.

# 3. Gefahren der Informationssicherheit und Sicherheitsziele

Die IT-Systeme und Anwendungen sind verschiedensten internen und externen Risiken ausgesetzt, die durch Vorsatz, Fahrlässigkeit, Umwelteinflüsse, technisches Versagen oder Unfälle Auswirkungen auf den Betrieb und die Verfügbarkeit, die Integrität und die Vertraulichkeit haben können.

- Die IT-Systeme des Unternehmens und die mit ihnen verarbeiteten Daten sind mit wirtschaftlich angemessenen Mitteln gegen die oben genannten Risiken zu schützen.
- Es muss jederzeit sichergestellt sein, dass Störungen, sei es aufgrund von Fehlern in den Systemen oder potenziellen Angriffen, erkannt und definierte Gegenmaßnahmen eingeleitet werden können.
- Darüber hinaus sind Zustände, die zu Störungen oder absehbar zu Störungen oder Verletzung der obigen Ziele führen werden, umgehend zu beheben.
- Sehr sorgfältiger, verantwortungsvoller und verlässlicher Umgang mit Informationen zum Schutz der Verfügbarkeit, Integrität und Vertraulichkeit dieser Informationen.

# 4. Auftragnehmer Prozess

**1. Marktzugang und Registrierung (Interessenbekundung)**

Die Aufnahme in den Kreis potenzieller Bieter erfolgt über die zentrale Vergabestelle / den Einkauf / die Bedarfsstelle der Hafengesellschaften (NPorts & JWP).

- **Transparenz:** Interessierte Unternehmen registrieren sich über das genutzte Vergabeportal.
- **Informationspflicht:** Bereits in dieser Phase werden Auftragnehmer über die geltenden ISMS-Rahmenbedingungen informiert, die als wesentliche Vertragsbedingungen im späteren Verfahren gelten.

**2. Eignungsprüfung und Sicherheitsqualifizierung (Eignungskriterien)**

Im Rahmen des formalen Vergabeverfahrens (z. B. UVgO) erfolgt eine Prüfung der fachlichen Eignung. Die ISMS-Anforderungen können hierbei als Mindestkriterien oder Eignungsnachweise definiert werden:

- **Selbstauskunft & Nachweise:** Einreichung von Zertifikaten (z. B. ISO/IEC 27001, TISAX) oder vergleichbaren Nachweisen zur Informationssicherheit.
- **Prozessprüfung:** Validierung, ob der Auftragnehmer über Prozesse verfügt, die den Schutzbedarf der Unternehmens-Daten (Vertraulichkeit, Integrität, Verfügbarkeit) sicherstellen.
- **Personelle Sicherheit:** Nachweis über regelmäßige Sensibilisierungsschulungen der eingesetzten Mitarbeiter.
- **Umgang mit Dritten:** Nachweis über das Management von Unterauftragnehmern (Supply Chain Security).

**3. Vergabeentscheidung und ISMS-Freigabe**

Die finale Auswahl erfolgt nach den Kriterien der Wirtschaftlichkeit und der technischen Eignung.

- **Fachliche Votierung:** Die Bedarfsabteilung trifft die Entscheidung nach bedarfsgerechter Beratung mit dem ISMS-Team.
- **Risikobewertung:** Bestehen Restrisiken bezüglich der Informationssicherheit, werden diese vor Zuschlagserteilung bewertet und ggf. durch zusätzliche vertragliche Sicherheitsklauseln (Besondere Vertragsbedingungen) minimiert.

**4. Laufende Überwachung und Lieferantenbewertung (Monitoring)**

Nach Vertragsschluss wird die Leistungserbringung kontinuierlich auf Basis von Annex 5.22 der ISO 27001 überwacht:

- **Leistungsfähigkeit:** Regelmäßige Bewertung der Servicequalität und Einhaltung der vereinbarten Sicherheitsvorgaben.
- **Re-Auditierung:** NPorts & JWP behalten sich vor, bei besonders wichtigen Dienstleistungen anlassbezogene oder zyklische Audits (Self-Assessments oder Vor-Ort-Audits) durchzuführen.
- **Risikoidentifikation:** Änderungen in der Auftragnehmerstruktur oder Sicherheitsvorfälle führen zu einer sofortigen Neubewertung des Risikos.

**5. Onboarding und operative Integration**

Mit Erteilung des Zuschlags und Vertragsunterzeichnung wird der Auftragnehmer in die Geschäftsprozesse integriert:

- **Einweisung:** Verpflichtende Einweisung in die relevanten Sicherheitsrichtlinien für externe Parteien.
- **Asset-Management:** Übergabe von notwendigen Zugängen oder Informationen erfolgt erst nach Bestätigung der Kenntnisnahme der Sicherheitsrichtlinien.

# 5. Mitarbeit des Auftragnehmers im Rahmen des ISMS

Die Mitarbeit des Auftragnehmers dient dem Schutz von Informationen und Systemen des Unternehmens, seiner Kunden, Mitarbeiter und Partner. Dazu müssen klare Zuständigkeiten des Informationseigentümers und Informationsnutzers definiert sein. Die Klassifizierung von Informationen obliegt dem Informationseigner oder von diesen beauftragten Personen. Bei der Autorisierung von Berechtigungen bzw. Personen ist nach dem Prinzip Need-to-know vorzugehen. Hiermit ist „Kenntnis nur bei Bedarf“ gemeint. Zugang zu Informationen erhält nur, wer die Information zur Erfüllung seiner Aufgaben benötigt.

Der Auftragnehmer verpflichtet sich zur Mitarbeit im Rahmen des ISMS der Hafengesellschaften (NPorts & JWP). Dies bedeutet im einzeln:

- Einhaltung des Informationsklassifizierungsschema
- Einhaltung der Hafenbenutzungsvorschrift (HBV)
- Einhaltung der Anforderungen an die Informationsübertragung
- Verschwiegenheitspflicht
- Einhaltung der Sicherheitsanforderungen
- Einhaltung der rechtlichen und organisatorischen Anforderungen, inkl. Datenschutz-, Urheberschutzrecht- etc.
- Melden von Informationssicherheitsvorfällen an die Hafengesellschaften (NPorts & JWP)
- Hinweisen auf Schwachstellen die für die Informationssicherheit aufgrund der gemeinsamen Tätigkeit entstehen können (Wartung an Systemen, Notwendige Sicherheitsmaßnahmen, …)
- Beachtung der Unternehmens-Richtlinien, die zum Tragen kommen
- Verfahren zum Berichtswesen
- Je nach Art des Zugriffs auf die Unternehmens-Informationen müssen Mitarbeiter entsprechend geschult werden

# 6. Klassifizierung der Informationen

Zur Klassifizierung der Informationen wird die Folgende Einteilung vorgenommen:

| **„Öffentlich“**<br>**TLP:CLEAR** | **„Intern“**<br>**TLP:AMBER** | **„Vertraulich“**<br>**TLP:AMBER+STRICT** | **„Streng Vertraulich“**<br>**TLP:RED** |
|---|---|---|---|
| ***"Darf Jede/r sehen."*** | ***"Dürfen alle KollegInnen sehen."*** | ***"Dürfen nur Kolleginnen mit bestimmten Aufgaben sehen."*** | ***"Darf niemand außer den Empfängern sehen."*** |
| ***„Darf uneingeschränkt verteilt werden.“***<br><br>*→ „Unbegrenzte Weitergabe“* | ***„Darf intern und nur wenn nötig extern weitergegeben werden. (Die Externen dürfen das nicht weitergeben.)“***<br><br>*→ „Eingeschränkte interne und organisationsübergreifende Weitergabe“* | ***„Darf nur intern weitergegeben werden.“***<br><br>*→ „Eingeschränkte interne Weitergabe“* | ***„Darf nicht weitergegeben werden.“***<br><br>*→ „Keine Weitergabe. Persönlich, nur für bekannte Empfänger“* |
| Abgesehen von urheberrechtlichen Aspekten, die das TLP explizit nicht adressiert, dürfen Informationen der Stufe TLP:CLEAR **ohne Einschränkungen** frei weitergegeben werden. | **Es gilt „Kenntnis nur, wenn nötig“, s**owohl in der eigenen Organisation als auch innerhalb der Partnerorganisation.<br><br>Eine **Weitergabe von den Partnern an Dritte ist nicht erlaubt.**<br><br>Der **Empfänger darf** die Informationen, welche als TLP:AMBER gekennzeichnet sind**, an seine Partner weitergeben**, soweit diese die Informationen zur Schadensreduktion oder dem eigenen Schutz benötigen.<br><br>Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen, diese müssen eingehalten werden. | **Es gilt „Kenntnis nur, wenn nötig“.**<br><br>Die Einstufung von Informationen als TLP:AMBER+STRICT **beschränkt die Weitergabe ausschließlich auf die Organisation des Empfängers**, jegliche Weitergabe darüber hinaus ist untersagt.<br><br>Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen, diese müssen eingehalten werden. | **Eine Weitergabe ist untersagt.**<br><br>Informationen dieser Stufe sind **auf** den **Kreis der Anwesenden** in einer Besprechung oder Video-/ Audiokonferenz **bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt.**<br><br>TLP:RED eingestufte Informationen sollten möglichst mündlich oder persönlich übergeben werden. |

**Es gilt der Grundsatz: Dokumente sind grundsätzlich und im Zweifel als Intern (TLP:AMBER) eingestuft anzusehen.** Eine unbegrenzte Veröffentlichung nicht gekennzeichneter Informationen (i.S.d. TLP:CLEAR) ist **erst nach expliziter Freigabe** durch Dokumenteneigner gestattet.

## 6.1 Öffentliche Information

Sind Informationen die keinem besonderen Schutzbedarf und keiner Kennzeichnung unterliegen, eine Offenlegung ist gefahrlos möglich.

z. B. Flyer, Logos, Prospekte, Informationsblätter, allgemeine Beschreibungen ohne Detailinformationen.

## 6.2 Interne Information

Sind Informationen die ausschließlich innerhalb der Hafengesellschaften (NPorts & JWP) oder durch Geschäftspartner als schutzbedürftig klassifiziert und gekennzeichnet wurden, weitergegeben werden dürfen, deren Offenlegung führt zu geringfügiger Verlegenheit oder Unannehmlichkeit, z.B. Angebote, Lieferscheine, Rechnungen, Intranet Meldungen.

- Der Zugriff Externer ist nur mit Erlaubnis des Informationseigners gestattet.
- **Es gilt der Grundsatz: Dokumente sind grundsätzlich und im Zweifel als Intern (TLP:AMBER) eingestuft anzusehen.**

## 6.3 Vertrauliche Information

Sind Informationen, die bei einer Veröffentlichung der Hafengesellschaften (NPorts & JWP) signifikante, kurzfristige Entwicklung des Unternehmens Schaden zufügen können, z.B. Personalunterlagen, Entwicklungs- oder Konstruktionsunterlagen, Berichte, Protokolle, Arbeitsunfähigkeitsbescheinigung, Arbeits- und Rahmenverträge, Verträge und Schriftverkehre mit Dritten.

**Personenbezogene Daten sind grundsätzlich als vertraulich zu klassifizieren.**

- Der Zugriff auf vertrauliche Informationen ist nur dem Informationseigner oder der von ihm legitimierten Personen gestattet.
- Vertrauliche Informationen dürfen nicht auf externe Systeme ohne entsprechende Sicherheitsmaßnahmen übertragen werden. (siehe hierzu auch Lieferantenrichtlinie).

## 6.4 Streng Vertrauliche Information

Sind Informationen, die bei einer Offenlegung schwerwiegende Auswirkungen auf langfristige strategische Zielsetzungen und den Bestand der Hafengesellschaften (NPorts & JWP) gefährden, z. B. PFSO-Unterlagen, Gefahrenabwehrpläne, PO-Ereignismeldungen, Admin-Zugänge.

- Der Zugriff auf geheime Informationen ist auf eine geringe und namentlich genau festgelegte Anzahl von Personen begrenzt.
- Jede Person mit Einsicht ist der Geheimhaltung verpflichtet
- Anlagen dürfen nicht unverschlüsselt per Mail versendet werden / E-Mail-Verschlüsselung.

Alle Dokumente der Hafengesellschaften (NPorts & JWP) haben in der Fußzeile einen expliziten Klassifizierungshinweis oder sind implizit klassifiziert. Ausgenommen hiervon sind öffentliche Dokumente.

# 7. Aspekte im Umgang mit externen, betriebsfremden Parteien

Unterschiedliche Aspekte und Faktoren können Einfluss auf die Geschäftstätigkeiten der Hafengesellschaften (NPorts & JWP) haben. Um den Umgang und die Behandlung sachgerecht analysieren und beurteilen zu können, sollen folgende Aspekte beachtet werden:

## 7.1 Risiken im Zusammenhang mit externen Mitarbeitern, Parteien und Kunden

Werden externe Parteien oder Mitarbeiter bzw. Kunden aktiv in die Geschäftsprozesse der Hafengesellschaften (NPorts & JWP) eingebunden, dürfen diese die Informationswerte und Abläufe nicht negativ beeinflussen oder gefährden. Bei der Beurteilung, wann, wie und in welchem Ausmaß Externe zur Leistungserbringung herangezogen werden, sollen diese einer Risikobetrachtung unterzogen werden.

Die folgenden Kriterien dienen als Hilfe bei der Bewertung eines möglichen Risikos:

- Benötigen Externe Zugriff auf informationsverarbeitende Systeme?
- Wie ist die Art des Zugriffs
    - Wird ein physischer Zugang, z.B. zu Büros, Computerräumen, Aktenschränken benötigt?
    - Wird ein logischer Zugang z.B. zu den Datenbanken oder Informationssystemen benötigt?
    - Werden Datenverbindungen zu oder von externen Parteien benötigt?

- Wie hoch ist der Wert und die Sensitivität der involvierten Informationen, und deren Kritikalität für den Geschäftsbetrieb?
- Wie hoch sind die notwendigen Aufwendungen und erforderlichen Maßnahmen zum Schutz derjenigen Informationen, die für Externe nicht zugänglich sein sollen?
- Wie können Mitarbeiter von externen Parteien identifiziert, wie kann die Berechtigung verifiziert und wie häufig muss oder sollte diese überprüft und bestätigt werden?
- Welche verschiedenen Mittel und Maßnahmen werden durch Externe bei der Speicherung, Verarbeitung, Kommunikation und Weitergabe, sowie beim Austausch von Informationen eingesetzt und sind diese angemessen?
- Wie hoch sind die Auswirkungen, wenn Externe bei Bedarf oder unvorhersehbaren Situationen kein Zugang zu den relevanten Informationen oder Systemen haben oder dieser entzogen wurde?
- Wie hoch sind die Auswirkungen, wenn Externe inkorrekte oder irreführende Informationen eingeben oder erhalten?
- Wie sind die Bedingungen für den weiteren Zugang für Externe nach Informationssicherheitsvorfällen zu bewerten und welche Auswirkungen haben diese auf die relevanten Geschäftsprozesse?
- Wie beeinflussen gesetzliche und behördliche Anforderungen und andere vertragliche Verpflichtungen, die im Zusammenhang mit Externen zu berücksichtigen sind, die relevanten Geschäftsprozesse?
- Werden Interessen anderer Stakeholder durch den Einsatz von Externen berührt?
- Wie werden die relevanten Geschäftsprozesse bei abrupter Beendigung oder Unterbrechung beeinflusst und können hierdurch ggf. geschäftsgefährdende Situationen entstehen?

Besonders bei Gewährung von Kundenzugriffen auf Informationswerte sollten die in “Logische Anbindung” beschriebenen Maßnahmen berücksichtigt werden. Dies gilt auch für Zugriffe auf sensitive Systeme, Netzwerke und Informationen durch externe Unternehmen oder Dienstleistern. Dort sollte das Risiko betrachtet und die entsprechenden Maßnahmen bewertet werden.

Beim Zugriff von Kunden auf Daten und IT Systeme sollten ergänzend folgende Aspekte Berücksichtigt werden:

- Schutz von Werten:
  - Umgang mit bekannten Schwachstellen
  - Verfahren, um festzustellen, ob die Werte kompromittiert wurden, z. B. in Form von Datenverlust oder -veränderung
  - Einschränkungen bzgl. des Kopierens und der Freigabe von Informationen
- Beschreibung des zur Verfügung gestellten Produkts oder der bereitgestellten Dienstleistung
- die verschiedenen Gründe, Anforderungen und Vorteile des Kundenzugangs;
- Richtlinie zur Zugangskontrolle, einschließlich:
- Vereinbarungen für Berichte, Mitteilungen und Untersuchungen von informationssicherheitsvorfällen
- eine Beschreibung jeder bereitgestellten Dienstleistung
- der angestrebte Service-Level und nicht akzeptable Service-Levels;
- das Recht, jegliche Aktivitäten in Zusammenhang mit den Werten zu überwachen und zu widerrufen
- die Haftungsregelungen zwischen den Unternehmen und dem Kunden
- Verantwortlichkeiten zur Gesetzeskonformität, und Sicherstellung der Erfüllung gesetzlicher Anforderungen

## 7.2 Adressieren von Sicherheit in Vereinbarungen mit Dritten

Verträge und Vereinbarungen mit Dritten sollten sicherstellen, dass beim Zugriff, bei der Verarbeitung, bei der Kommunikation, der Administration oder der technischen Betreuung von Informationen oder informationsverarbeitenden Einrichtungen der Hafengesellschaften (NPorts & JWP) alle relevanten Sicherheitsanforderungen Berücksichtigung finden, und der Schutzbedarf sensitiver Informationen hinreichend berücksichtigt wird.

Die Aufnahme der folgenden Bedingungen in der Vereinbarung sollte erwogen werden, um die identifizierten Sicherheitsanforderungen zu erfüllen:

- die Informationssicherheitsleitlinie;
- Maßnahmen zur Sicherstellung des Schutzes von organisationseigenen Werten (Assets), einschließlich:
  - Verfahren zum Schutz organisationseigener Werte (Assets), einschließlich Informationen, Software und Hardware;
  - alle notwendigen Maßnahmen und Mechanismen für den physischen Schutz;
  - Maßnahmen, die den Schutz vor bösartigen Codes sicherstellen;
  - Verfahren zur Bestimmung, ob eine Kompromittierung von Werten stattgefunden hat, z. B. in Form von Verlust oder Veränderung der Informationen, Software und Hardware;

- Maßnahmen, um die Rückgabe oder Vernichtung von Informationen und Werten bei Vertragsende oder zu einem vereinbarten Zeitpunkt innerhalb der Vertragslaufzeit sicherzustellen;
- Vertraulichkeit, Integrität, Verfügbarkeit und alle anderen wichtigen Eigenschaften von organisationseignen Werten;
- Einschränkungen bzgl. des Kopierens und der Freigabe von Informationen sowie die Verwendung von Vertraulichkeitsverpflichtungen;

- Benutzer- und Administratorschulung in Methoden, Verfahren und Sicherheit;
- sicherstellen, dass die Benutzer ihrer Verantwortung für Informationssicherheit bewusst sind. Dazu Mitarbeiter Sensibilisierungen auch für Externe/Dritte.
- gegebenenfalls Vorkehrungen für die Übernahme von Personal;
- Verantwortlichkeiten in Bezug auf Installation und Wartung von Hardware und Software;
- eine eindeutige Berichtsstruktur und festgelegte Berichtsformate;
- ein eindeutiger und festgelegter Prozess für die Handhabung von Anpassungen;
- Richtlinie zur Zugangskontrolle, einschließlich:
  - die unterschiedlichen Gründe, Anforderungen und Vorteile, die den Zugang von Dritten notwendig machen;
  - zulässige Zugangsmethoden, und die Kontrolle und Benutzung eindeutiger Kennungen wie Benutzerkennungen und Passwörtern;
  - ein Berechtigungsprozess für Benutzerzugriff und -privilegien;
  - die Anforderung, eine Liste zu pflegen, welche Personen zur Benutzung der zur Verfügung gestellten Dienste berechtigt sind, und welches ihre Rechte und Privilegien im Rahmen dieser Benutzung sind;
  - eine Erklärung, dass jeglicher Zugang verboten ist, der nicht ausdrücklich erlaubt ist;
  - einen Prozess, Zugangs- und Zugriffsrechte zu entziehen oder die Verbindung zwischen Systemen zu unterbrechen;

- Vereinbarungen für Berichte, Mitteilungen und Untersuchungen von Informationssicherheitsvorfällen und Sicherheitsverstößen, genauso wie Vertragsverstöße;
- eine Beschreibung des bereitgestellten Produkts oder der Dienstleistung, und eine Beschreibung der zur Verfügung gestellten Informationen, einschließlich ihrer Sicherheitsklassifizierung;
- das angestrebte Service-Level und nicht akzeptable Service-Levels;
- die Definition überprüfbarer Leistungskriterien, deren Überwachung und Berichterstattung;
- das Recht, jegliche Aktivitäten in Zusammenhang mit den Werten der Organisation zu überwachen und zu widerrufen;
- das Recht, die vertraglich festgelegten Verantwortlichkeiten zu überprüfen, diese Prüfungen durch unabhängige Dritte durchführen zu lassen, und die satzungsgemäßen Rechte der Prüfer zu benennen;
- Einrichtung eines Eskalationsprozesses zur Problemlösung;
- Anforderungen an die Kontinuität der Dienstleistung, einschließlich von Messgrößen für Verfügbarkeit und Verlässlichkeit, die im Einklang mit den geschäftlichen Prioritäten der Organisation sind;
- die vereinbarte Verpflichtung der jeweiligen Parteien;

- Verantwortlichkeiten zur Gesetzeskonformität, und Sicherstellung der Erfüllung gesetzlicher Anforderungen, z. B. Datenschutzgesetze; insbesondere unter Berücksichtigung unterschiedlicher nationaler Rechtssysteme, wenn die Vereinbarung die Zusammenarbeit mit Organisationen im Ausland einschließt;
- geistiges Eigentum und die Zuweisung von Urheberrechten, und der Schutz jeglicher gemeinschaftlicheren Arbeit.
- Einbeziehung Dritter mit Subunternehmern, sowie die Sicherheitsmaßnahmen, die diese Subunternehmer umsetzen müssen;
- Bedingungen für die Neuverhandlung/Beendigung von Vereinbarungen:
    - für den Fall, dass eine Partei die Geschäftsbeziehung vor Vertragslaufzeitende beenden möchte, sollte ein Notfallplan existieren;
    - Neuverhandlung von Vereinbarungen, wenn sich die Sicherheitsanforderungen der Organisation ändern;
    - laufende Dokumentation von Listen über organisationseigene Werte, Lizenzen, Vereinbarungen oder die daraus resultierenden Rechte.

- Bevor Änderungen durchgeführt werden, sollten gemeinsam mit dem Dienstleister Rückfall-Lösungen erarbeitet werden
- Im Notfallvorsorgekonzept sollten die Zuständigkeiten, Ansprechpartner und Abläufe zwischen den Hafengesellschaften (NPorts & JWP) und den Dienstleistern geregelt sein, dazu sollten Notfallübungen durchgeführt werden.
- Im bestimmten Fällen sollte mit Dienstleistern vereinbart sein, dass eine mögliche Sicherheitsüberprüfung des eingesetzten Personals geeignet überprüft wird.
- Wird die Fernwartung von Externen durchgeführt, sollten alle Aktivitäten von internen Mitarbeitern beobachtet werden. Alle Fernwartungsvorgänge sollen aufgezeichnet werden.

Es sollte sichergestellt werden, dass sich Externe ihrer Verpflichtungen bewusst sind und die Verantwortlichkeiten und Haftung akzeptieren, die der Zugriff, die Verarbeitung, die Kommunikation oder die Verwaltung von Informationen und informationsverarbeitenden Einrichtungen mit sich bringen.

Alle Vereinbarungen, die einen Zugriff Dritter auf Prozesssteuerungssysteme beinhalten, müssen auf die Notwendigkeit dieses Zugriffs geprüft werden.

Zusätzlich sollten alle Verträge, die Telekommunikationsdienstleistungen beinhalten, spezielle Anforderungen in Bezug auf Krisen- und Notfallkommunikation wie Großereignisse, Naturkatastrophen, etc. erfüllen, um Ausfälle in Notfallsituationen zu vermeiden.

# 8. IKT Lieferkette

Es sollten Prozesse und Verfahren festgelegt und umgesetzt werden, um die mit der IKT-Produkt- und Dienstleistungslieferkette verbundenen Informationssicherheitsrisiken zu beherrschen. Die spezifischen Risikomanagementpraktiken für die IKT-Lieferkette bauen auf den allgemeinen Informationssicherheits-, Qualitäts-, Projektmanagement- und Systementwicklungspraktiken auf, ersetzen diese jedoch nicht.

Es sind Prozesse und Verfahren festgelegt und umgesetzt, um die mit der IKT-Produkt- und Dienstleistungslieferkette verbundenen Informationssicherheitsrisiken zu überwachen, u.a. auch in den Vereinbarungen mit Dritten.

# 9. Übersicht Informationsübertragung und Entsorgungshinweise

**Tab. 1:** Informationsübertragung und Entsorgungshinweise

| | **Öffentlich** | **Intern** | **Vertraulich** | **Streng vertraulich** |
|---|---|---|---|---|
| **Dokument** | | deutlich sichtbarer Vermerk auf dem Dokument | deutlich sichtbarer Vermerk auf dem Dokument | deutlich sichtbarer Vermerk auf dem Dokument |
| **Mail** | | | Empfohlen: Anhang Passwort geschützt | Anhang Passwort geschützt + Verschlüsselung |
| **Datenfile** | | | Empfohlen: Passwort geschützt | Passwort geschützt |
| **Datenablage** | | Berechtigungs-konzept, , Externe Datenträger: Verschlüsselt | Berechtigungs-konzept, Externe Datenträger: Verschlüsselt | Berechtigungs-konzept, Externe Datenträger: Verschlüsselt |
| **Datentransfer** | | Empfohlen: verschlüsselt | Empfohlen: verschlüsselt | verschlüsselt |
| **Dokumenten-Entsorgung** | Papier-container | Datentonne zertifizierter Entsorger mechanisch zerstört nach DIN 66399 Möglichst Schutzklasse 2 – hoher Schutzgrad | Datentonne zertifizierter Entsorger mechanisch zerstört nach DIN 66399 Mind. Schutzklasse 2 – hoher Schutzgrad | Datentonne zertifizierter Entsorger mechanisch zerstört nach DIN 66399 Mind. Schutzklasse 3 – sehr hoher Schutzgrad |
| **Datenträgerentsorgung** | | mechanisch zerstört zertifizierter Entsorger Möglichst Schutzklasse 2 – hoher Schutzgrad | mechanisch zerstört zertifizierter Entsorger Mind. Schutzklasse 2 – hoher Schutzgrad | mechanisch zerstört zertifizierter Entsorger Mind. Schutzklasse 3 – sehr hoher Schutzgrad |

| | | | | |
|---|---|---|---|---|
| **Schadensgröße** | klein | gering | Mittel | Groß bis existenzgefährdend |
| **Schaden für das Unternehmen** | Kein Schaden, da Information für die Öffentlichkeit bestimmt | Keine weit reichenden Konsequenzen | Betroffen ist ein Unternehmens-bereich: Erheblicher finanzieller Schaden / Rechtliche Konsequenzen bis hin zu Ordnungs-widrigkeiten und Geldstrafen / Verärgerung und Imageverlust bei einzelnen Kunden oder Lieferanten / Personenbezogene Daten gem. Bundesdatenschutzgesetz | Betroffen ist das gesamte Unternehmen: sehr schwerer Schaden für die Geschäftszwecke und Ziele des Hauses / Gravierende rechtliche Konsequenzen bis hin zu Haftstrafen / Erheblicher Verlust von Ansehen und Vertrauen bei mehreren Kunden oder Lieferanten |

# 10. Externe Netzwerkverbindungen

Externe Netzwerkverbindungen sind Verbindungen der Netze der Hafengesellschaften (NPorts & JWP) mit den Netzen externer Unternehmen (Auftragnehmer). Beispiele für externe Netzwerkverbindungen sind:

- Extranets mit Kunden oder Auftragnehmern
- Wartungszugänge durch IT-Lieferanten oder Dienstleister
- Remote Access durch Berater, Wirtschaftsprüfer oder andere
- Verbindungen mit Outsourcing-Anbietern

Externe Netzwerkverbindungen sind durch einen Prozess zu autorisieren, der aus den folgenden Schritten besteht:

1. Der Zweck und die Vorteile für die Hafengesellschaften (NPorts & JWP) aus dieser Netzwerkverbindung sind anzugeben
   - z. B. unterstützte Geschäftsprozesse oder Anwendungssysteme
   - Art und Kritikalität der Informationen, die über die Verbindung ausgetauscht werden
   - Die Gruppe der Anwender bei dem externen Dritten, die diese Verbindung nutzen
   - Dauer der Verbindung
2. Vor der Installation der Verbindung ist eine Risikoanalyse durchzuführen und entsprechend weitere Sicherheitsmaßnahmen umzusetzen, sofern nicht bereits in Verbindung mit 6.1.2/1.3 erfolgt.

# 11. Überwachung, Überprüfung, Änderungsmanagement von Lieferantendienstleistungen

Ziel: Ein vereinbartes Niveau der Informationssicherheit und der Dienstleistungserbringung ist im Einklang mit Auftragnehmerverträgen aufrecht erhalten.

Die Hafengesellschaften (NPorts & JWP) müssen die Erbringung von Auftragnehmerdienstleistungen regelmäßig überwachen, überprüfen und ggf. auditieren. Darüber hinaus muss sichergestellt werden, dass sich auch die Auftragnehmer an die in dieser Richtlinie dargestellten Regeln halten. Es muss sichergestellt werden, dass der Dienstleister die Dienst-leistung in Übereinstimmung mit dem vereinbarten Service Level Agreement (SLA) anbietet. Zu diesem Zweck muss die Leistungserbringung (ggf. gemäß definierter KPI's) überwacht werden.

Lieferanten und Dienstleister werden gemäß den Vorgaben des Gesetzes gegen Wettbewerbsbeschränkungen (GWB) sowie den geltenden Vergabebestimmungen (z.B. VgV, VOL, VOB) bewertet und ausgewählt. Die Hafengesellschaften (NPorts & JWP) sind im Eigentum der Länder Niedersachsen / Bremen und somit auch öffentliche Auftraggeber. Sie unterliegen damit einem strengen Diskriminierungsverbot. Bei der Bewertung von Auftragnehmern sind die Hafengesellschaften (NPorts & JWP) daher in besonderem Maße an die genannten Vorgaben gebunden.

Im Zuge dessen basieren Vergabeentscheidungen an externe Auftragnehmer grundsätzlich auf einem vor der Vergabe festgelegten und kommunizierten Kriterien- und Leistungskatalog. Jeder externe Anbieter, der ein Angebot für eine zu vergebende Leistung abgibt, wird anhand des spezifischen Kriterienkataloges bewertet und auf Grundlage der Bewertung ausgewählt. Entsprechend der Vorgaben der jeweiligen Vergabeordnung wird ein externer Anbieter in jedem Vergabeverfahren anhand des Kriterienkataloges im Hinblick auf die Übereinstimmung mit den Anforderungen neu beurteilt.

Alle Vergabeverfahren (inklusive der Kriterien, der Ergebnisse der Bewertung und daraus folgender notwendiger Maßnahmen) werden in den Fachabteilungen umfänglich dokumentiert. Dadurch ist zusätzlich die Nachvollziehbarkeit gewährleistet, welche Fremddienstleister für die Hafengesellschaften (NPorts & JWP) tätig sind und waren.

# 12. Vertragliche Regelungen

Die mit den vertraglichen Regelungen getroffenen Vereinbarungen (NDA, Vertragsstrafen, SLA's, die aktuelle Datenschutzvereinbarung etc.) werden von den Auftragnehmern und Dienstleistern anerkannt und deren Einhaltung sichergestellt.

Über die Fachverantwortlichen wird gesteuert, welche Aufgaben der Dienstleister zu erfüllen hat. Für diese Aufgabe wird ein Einzelvertrag (z.B. Dienstleistungsvertrag) abgeschlossen. In Abhängigkeit dieser Aufgabe erhält er die Zugriffsberechtigungen für seine Tätigkeit. Die Freischaltung erfolgt über die Beauftragung der verschiedenen Fachabteilungen. Nach Beendigung der Vertragslaufzeit werden die Zugriffsrechte wieder entzogen.
Mit der Durchführung von Arbeiten innerhalb des Vertragsverhältnisses, ist dem Auftragnehmer bekannt und bewusst, dass dieser durch die Hafengesellschaften (NPorts & JWP) im Rahmen des ISMS einem Lieferantenaudit unterzogen werden kann.

Oldenburg, den 07.07.2026

Holger Banik

Geschäftsführer NPorts
Geschäftsführer JWP-R & JWP-M

Volker Weiß

Geschäftsführer NPorts
Technischer Leiter JWP-R