FACILITY SECURITY REQUIREMENTS

TAPA
Transported Asset Protection Association

Transported Asset Protection Association

Facility Security Requirements
FSR 2020

TAPA Standards

TAPA Americas
5030 Champion Blvd,
G-11 #266 Boca Raton,
Florida 33496
U.S.A.
www.tapaonline.org
Tel. (561) 617-0096

TAPA Asia Pacific
1 Gateway Drive, Westgate
Tower #07-01,
Singapore 608531

www.tapa-apac.org
Tel. (65) 6514 9648

TAPA EMEA
Rhijngeesterstraatweg 40D
2341 BV Oegstgeest
The Netherlands

www.tapaemea.org
Tel. +44 1633 251325

FSR Inhaltsverzeichnis

FSR Inhaltsverzeichnis (Fortsetzung)

□□□

1. Einführung

1.1 Zweck dieses FSR Dokumentes

Dieses Facility Security Requirements (FSR) (*Sicherheitsanforderungen für Betriebsstätten)* Dokument ist der offizielle TAPA Standard für sichere Lagerung und Einlagerung. Es ist ein gemeinsamer weltweiter Standard, welcher in Geschäfts-/Sicherheitsabkommen zwischen Käufern und Logistikdienstleistern (LSP) und/oder anderen Antragstellern, die sich zertifizieren lassen wollen, genutzt werden kann.

Bei der Entwicklung dieses Standards hat TAPA anerkannt, dass es große Unterschiede darin gibt, wie die Lagerdienste global, regional und sogar innerhalb von einem Unternehmen bereitgestellt werden und dass die FSR für alle oder einen Teil der von einem LSP/Antragsteller erbrachten Dienstleistungen gelten kann. Abhängig von der Komplexität und Größe der Lieferkette kann die Einhaltung der TAPA Standards durch einen einzigen LSP/Antragsteller oder mehrere LSP/Bewerber und qualifizierte Subunternehmer erreicht werden.

Umfang

TAPA hat drei Optionen entwickelt um die Zertifizierung zu unterstützen:

• Zertifizierung eines einzelnen Standortes durch Zertifizierungsgesellschaft (IAB).

• Zertifizierung mehrerer Standorte durch Zertifizierungsgesellschaft (IAB).

• Selbstaudit-Zertifizierung durch autorisierte Auditoren (AA) durch den LSP / Antragsteller oder IAB

Zielgruppe

Typische Nutzer der TAPA-Standards sind:

- Käufer
- LSP/Antragsteller
- Strafverfolgungsbehörden oder andere Regierungsorganisationen
- Unternehmen, die Teil einer professionellen Lieferkette sind
- Versicherungsgesellschaften

1. Einführung

1.2 Mittel zur Implementierung des TAPA FSR

Die Mittel zur Erfüllung der Anforderungen des FSR liegen in der Verantwortung des LSP / Antragstellers und auf eigene Kosten des LSP / Antragstellers, sofern dies nicht zwischen dem Käufer und LSP / Antragsteller ausgehandelt oder anderweitig vereinbart wurde.

1.3 Schutz der LSP-Richtlinien und Verfahren

Kopien von Sicherheitsrichtlinien und -verfahren werden dem Käufer nur in Übereinstimmung mit den unterzeichneten Offenlegungsvereinbarungen zwischen LSP / Antragsteller und Käufer übermittelt und als vertrauliche Informationen behandelt.

2. Über TAPA

2.1 TAPA's Absicht

Frachtkriminalität ist eine der größten Herausforderungen in der Lieferkette für Hersteller wertvoller Produkte mit hohem Risiko und deren Logistikdienstleister.

Die Bedrohung geht nicht mehr nur von opportunistischen Kriminellen aus. Heutzutage sind Ringe der organisierten Kriminalität weltweit tätig und setzen immer ausgefeiltere Angriffe auf Fahrzeuge, Räumlichkeiten und Personal ein, um ihre Ziele zu erreichen.

TAPA ist ein einzigartiges Forum, das globale Hersteller, Logistikdienstleister, Frachtunternehmen, Strafverfolgungsbehörden und andere Interessengruppen zusammenbringt, um die Verluste aus internationalen Lieferketten zu reduzieren. Das Hauptaugenmerk von TAPA liegt auf der Diebstahlprävention durch den Einsatz von Echtzeitinformationen und den neuesten Präventionsmaßnahmen.

2.2 TAPA's Mission

Die Mission von TAPA ist es, zum Schutz der Vermögenswerte der Mitglieder beizutragen, indem Frachtverluste aus der Lieferkette minimiert werden. TAPA erreicht dies durch die Entwicklung und Anwendung globaler Sicherheitsstandards, anerkannter Branchenpraktiken, Technologie, Bildung, Benchmarking, Zusammenarbeit bei der Regulierung und die proaktive Identifizierung von Kriminalitätstrends und Sicherheitsbedrohungen in der Lieferkette.

3. TAPA Standards

3.1 TAPA Sicherheits-Standards

Die folgenden globalen TAPA-Sicherheitsstandards wurden erstellt, um den sicheren Transport und die Lagerung hochwertiger und diebstahlgefährdeter Fracht zu gewährleisten:

- Die Facility Security Requirements (FSR) stellen Mindeststandards dar, die speziell für die *sichere Lagerung oder die beförderungsbedingte Zwischenlagerung* während des Transports innerhalb einer Lieferkette gelten.
- Die Trucking Security Requirements (TSR) konzentrieren sich ausschließlich auf den Transport per LKW und stellen Mindeststandards für den *Transport von Produkten auf der Straße* innerhalb einer Lieferkette dar.

Die globalen Sicherheitsstandards von TAPA werden alle drei Jahre nach Bedarf überprüft und überarbeitet.

Dieses Dokument behandelt nur die FSR-Anforderungen.

- Der Zertifizierungsprozess für TAPA FSR ist im Dokument TAPA FSR Zertifizierungsrahmenbedingungen beschrieben.
- Um den TAPA FSR-Zertifizierungsstatus zu erreichen, müssen sowohl die aktuellen Versionen des TAPA FSR- als auch die des TAPA FSR Zertifizierungs-Rahmenbedingungen-Dokuments befolgt werden.

3.2 Umsetzung

Die erfolgreiche Umsetzung der TAPA-Sicherheitsstandards hängt davon ab, dass LSPs (Logistikdienstleister) / Antragsteller, Käufer (Eigentümer der Ladung) und von TAPA autorisierte Prüfer zusammenarbeiten.

4. Rechtliche Leitlinie

4.1 Umfang

Der FSR ist ein globaler Standard und alle Abschnitte des Standards sind obligatorisch, es sei denn, eine Ausnahme wird durch das offizielle Verzichtsverfahren gewährt. (Siehe Abschnitt 6.).

4.2 Übersetzung

In geografischen Gebieten, in denen Englisch nicht die Muttersprache ist und in denen eine Übersetzung erforderlich und anwendbar ist, liegt es in der Verantwortung des LSP / Antragstellers und seiner Vertreter sicherzustellen, dass jede Übersetzung des FSR oder eines seiner Teile genau den Absichten von TAPA entspricht, die bei der Entwicklung und Veröffentlichung dieses Standards zugrunde gelegt wurden.

4.3 Das Markenzeichen "TAPA"

TAPA" ist eine eingetragene Marke der Transported Asset Protection Association und darf ohne die ausdrückliche schriftliche Genehmigung von TAPA durch seine offiziell anerkannten Regionen nicht verwendet werden. TAPA-Standards und zugehöriges Material werden durch und von TAPA veröffentlicht und dürfen ohne die ausdrückliche schriftliche Genehmigung von TAPA von keiner Partei überarbeitet, bearbeitet oder geändert werden. Der Missbrauch der Marke TAPA kann zur Aufhebung der Zertifizierung oder zu rechtlichen Schritten führen.

4.4 Haftungsgrenzen

Durch die Veröffentlichung dieser Standards bietet TAPA keine Garantie oder Zusicherung, dass alle Ladungsdiebstahlereignisse verhindert werden, unabhängig davon, ob die Standards vollständig und ordnungsgemäß implementiert sind oder nicht. Jegliche Haftung, die sich aus einem Diebstahl von eingelagerter Ladung oder einem anderen Verlust von eingelagerter Ladung gemäß den FSR-Standards ergeben kann, geht zu Lasten des LSP / Antragstellers und / oder des Käufers gemäß den Bestimmungen und Bedingungen in seinem Vertrag miteinander und mit allen Gesetzen oder Statuten, die innerhalb der jeweiligen Gerichtsbarkeit gelten können.

5. Verträge und Unterauftragsvergabe

5.1 Verträge

Der sichere Transport, die Lagerung und der Umgang mit den Wirtschaftsgütern des Käufers liegen in der Verantwortung des LSP / Antragstellers, seiner Vertreter und Subunternehmer während der gesamten Abholung, des Transports, der Lagerung und der Lieferung, wie in einer Freigabe oder einem Vertrag angegeben.

Soweit sich im Vertrag zwischen dem LSP/Antragsteller und dem Käufer auf die FSR bezogen wird oder diese in den Vertrag aufgenommen wurden, muss auf diese auch im Sicherheitsprogramm des LSP/Antragstellers verwiesen werden.

Der LSP stellt dem Käufer einen Nachweis über die FSR-Zertifizierung zur Verfügung und liefert, falls notwendig, den Nachweis, dass die FSR Anforderungen erfüllt worden sind. Ferner wird die Frage ob ein angebliches Versäumnis des LSP/Antragstellers die FSR-Anforderungen umzusetzen vorliegt gemäß den Vertragsbedingungen, die zwischen dem Käufer und dem LSP/Antragsteller ausgehandelt wurden, entschieden.

5.2 Unterauftragsvergabe

Der Vertrag für Unterauftragnehmer für die Lagerung enthält eine Anforderung, dass alle angegebenen FSR-Standards vom Subunternehmer ebenfalls zu erfüllen sind.

5.3 TAPA Untersuchung und Lösung von Beschwerden

Wenn TAPA eine formelle Beschwerde über die Leistung eines zertifizierten LSP / Antragstellers erhält, kann TAPA (vorbehaltlich der Validierung) verlangen, dass dieser LSP / Antragsteller auf eigene Kosten eine erneute Auditierung beauftragt und durchführt. Wenn der LSP / Antragsteller das Audit nicht besteht oder sich weigert diesen Prozess einzuhalten, kann sein Zertifikat entzogen werden.

6. Außerkraftsetzung (Verzichtserklärung)

6. 1 Überblick

Eine Verzichtserklärung ist eine schriftliche Genehmigung, mit der entweder ein Standort von einer bestimmten TAPA-Anforderung befreit oder eine alternative Compliance-Lösung akzeptiert wird. Eine Verzichtserklärung kann beantragt werden, wenn ein LSP / Antragsteller eine bestimmte Anforderung im FSR nicht erfüllen kann, dafür jedoch eingeführte alternative Maßnahmen dies rechtfertigen können. Ausnahmen gelten für den Zeitraum der Zertifizierung.

Alle Ausnahmeanträge für eine bestimmte Sicherheitsanforderung (ganz oder teilweise) müssen über ein TAPA-Ausnahmeantragsformular (auf der TAPA Webseite zu finden) vom LSP / Antragsteller an den Auditor (IAB) / Authorized Auditor (AA) gesendet werden. Der anfragende LSP / Antragsteller übernimmt die volle Verantwortung für die Richtigkeit der in der Verzichtserklärung angegebenen Informationen.

Jeder Verzichtsantrag muss dann über das IAB / AA der regionalen TAPA-Verzichtserklärungskommission zur Genehmigung vorgelegt werden. Es liegt in der Verantwortung des IAB / AA, zu entscheiden, ob die Anfrage vollständig ist und die Bearbeitung durch TAPA rechtfertigt. Dies umfasst die Überprüfung von Ausgleichsmaßnahmen und / oder alternativen Sicherheitskontrollen.

Sollten TAPA-Vertreter und/oder Käufer diese Verzichtserklärung in Frage stellen, wird TAPA eine formelle Untersuchung durchführen und dem LSP/Antragsteller zu verstehen geben, dass die Verzichtserklärung von TAPA widerrufen werden kann.

6. 2 Ablaufprozess

Wenn ein LSP eine bestimmte Anforderung im FSR nicht erfüllen kann, wird der folgende Prozess ausgeführt.

Tabelle 1: Verantwortlichkeiten: Verzichtserklärung Antrag / Evaluierung

Schritt	Verantwortlich	Maßnahme
1.	LSP/Antragsteller	Ermittelt die Ausgleichsmaßnahmen und weist die Wirksamkeit nach
2.	LSP/Antragsteller	Füllt einen TAPA Antrag auf Verzichtserklärung aus und übermittelt es an IAB / AA.
3.	IAB/AA	Prüft und verifiziert die Vollständigkeit der Informationen die im TAPA Verzichtserklärungsformular übermittelt wurden.
4.	IAB/AA	Übermittelt das TAPA Verzichtserklärungsformular an die TAPA regionale Verzichtserklärungskommission.
5.	TAPA regionale Verzichtserklärungs-kommission	Überprüft den Antrag und genehmigt oder verweigert die Verzichtserklärung.

6. Außerkraftsetzung (Verzichtserklärung)

Wenn die Verzichtserklärung verweigert worden ist

Wenn die regionale TAPA Verzichtserklärungskommission die Verzichtserklärung nicht genehmigt, ist der LSP/Antragsteller verpflichtet die vollständigen Sicherheitsanforderungen des FSR umzusetzen

Wenn die Verzichtserklärung genehmigt worden ist

Wenn die regionale TAPA Verzichtserklärungskommission die Verzichtserklärung genehmigt hat, werden die folgenden Maßnahmen ergriffen:

Tabelle 2: Genehmigung

Schritt	Verantwortlich	Aktion
1.	TAPA regionale Verzichtserklärungs-kommission	Dokumentiert und unterschreibt die Details der Verzichtserklärung.
2.	TAPA regionale Verzichtserklärungs-kommission	Gibt die Laufzeit der Verzichtserklärung an (bis maximal drei Jahre) und sendet eine Kopie an den AA.
3.	AA	Teilt dem LSP/Antragsteller das Ergebnis des Verzichtserklärungsantrages mit.
4.	LSP/Antragsteller	Entspricht den Anforderungen der Verzichtserklärung. Wenn dies nicht der Fall ist, wird die Freistellung ungültig.

6.3 Außerkraftsetzung von physischen Barrieren (unter Kapitel 1) und der Sicherheitskäfige für hochwertige Fracht (HVC, unter Kapitel 4.5)

TAPA wird einen Verzicht ganz oder teilweise auf die Umgrenzungsbarriere-Anforderungen und / oder für den HVC in Betracht ziehen, wenn alle folgenden Voraussetzungen erfüllt sind:

General:

- Der Verzichtsantrag wird über das offizielle TAPA-Antragsformular für Verzichtserklärungen eingereicht und vom IAB / AA gebilligt.
- Der Antrag auf Verzicht enthält Einzelheiten zu Ausgleichsmaßnahmen, um sicherzustellen, dass gefährdete Waren keinem unnötigen Diebstahl- oder Verlustrisiko ausgesetzt sind.
- Eine Risikobewertung muss ausgefüllt und zusammen mit dem Antrag auf Verzicht eingereicht werden. Alle in der Risikobewertung festgestellten signifikanten Schwachstellen müssen im Verzicht separat aufgeführt und die Maßnahmen ergriffen werden, um das Risiko auf ein akzeptables Maß zu reduzieren.

6. Außerkraftsetzung (Verzichtserklärung)

Ausgleichsmaßnahmen müssen vorhanden und in der Einreichung des Verzichtsantrags dokumentiert sein:

- **Umgrenzungsbarrieren:**
  - Zusätzliche Vorrichtungen, Ressourcen und Verfahren, die eingeführt wurden, um die rechtzeitige Erkennung nicht autorisierter Personen oder Fahrzeuge zu unterstützen, dies können unter anderem zusätzliche Beleuchtung, Videoüberwachung, verbesserte Verfahren zur Durchsetzung von Personen- und Fahrzeug Identifizierung, für bestimmte Bereiche Zugang nur mit LSP-Weste oder Uniform.
  - Sichtbare Begrenzungsschilder müssen in der Landessprache installiert sein und "Kein unbefugter Zutritt", "Kein unbefugtes Parken" anzeigen.
  - An den Außentüren oder -Wänden sind sichtbare Schilder anzubringen, die Fahrer, Besucher usw. anweisen, zum entsprechenden Eingang oder Sicherheitskontrolle zu gehen.
  - Bestätigung, dass Verfahren vorhanden sind die sicherstellen, dass die Bereiche für Frachtumschlag, Versand und Empfang von Waren mindestens wöchentlich überprüft werden und den Verzichtsbedingungen entsprechen.
- **HVC:**
  - Für HVC-Verzichtserklärungen müssen die geeigneten Ausgleichsmaßnahmen zur Risikominimierung (sofern kein HVC verfügbar ist) in der jährlichen Risikobewertung berücksichtigt und dokumentiert werden.
  - Der Verzichtsantrag enthält eine beigefügte Erklärung, die vom LSP / Antragsteller unterzeichnet wurde und besagt, dass kein Käufer einen HVC benötigt.

7. Facility Security Requirements

Kapitel	Allgemeine Anforderungen:	A	B	C
7.0				
7.0.1	Alle in dieser Norm geforderten Verfahren oder Richtlinien müssen dokumentiert werden.	✔	✔	✔
7.0.2	Für physische Schlösser, Zugangskarten und / oder Schlüssel, die die physischen und elektronischen Schlüssel verwalten und steuern, ist ein Verfahren, ein Protokoll und / oder ein Schlüsselplan erforderlich.	✔	✔	✔

Kapitel	Perimeter / Umgrenzung	A	B	C
7.1				
Lagerhalle Außenbereich Frachtumschlag, Versand und Annahme (Allgemein)				
7.1.1	Die Videoüberwachung muss in der Lage sein, den gesamten Verkehr auf dem Betriebsgelände im Be- und Entladebereich (einschließlich Ein- und Ausfahrt) zu sehen und sicherstellen, dass alle Fahrzeuge und Einzelpersonen jederzeit erkennbar sind, es sei denn, dass eine vorübergehende Einschränkung der Sicht aufgrund von Betriebsanforderungen besteht (z.B. LKW Be- und Entladen in Echtzeit).	✔	✔	
7.1.2	Die Beleuchtung in Be- und Entladebereichen muss angemessen sein. *Hinweis: Die Beleuchtung kann konstant sein oder wird durch Alarm, Bewegung, Geräusche, etc. sofort ausgelöst und aktiviert.*	✔	✔	✔
7.1.3	Verfahren, das beschreibt, wie mit nicht autorisierten Fahrzeugen und Personen innerhalb der externen Frachtumschlag-, Versand- und Empfangsbereiche verfahren werden soll. Anweisungen zum Verfahren müssen den relevanten Mitarbeitern, einschließlich der Wachen, ausgehändigt werden.	✔	✔	✔
7. 1.4	Frachtumschlags- und Wareneingangsbereich ist hinreichend kontrolliert, um unbefugten Zutritt zu verhindern		✔	✔
7.1.5	Für ebenerdig zugängliche Fenster oder Tore muss die jährliche Risikobewertung die Notwendigkeit von Einbruchschutz-Pollern beinhalten. (Siehe Risikobewertung, Abschnitt 7.6.5.)	✔		
Physische Barrieren (Zäune/Tore)				
7.1.6	Physische Barrieren umschließen die Bereiche Frachtumschlag, Versand- und Annahmehof.	✔		
7.1.7	Die physischen Barrieren um die Bereiche Frachtumschlag, Versand- und Annahmehof sind mindestens 6 Fuß / 1.80m hoch. *Anmerkung: Die physische Barriere, die konzipiert ist um unbefugten Zutritt zu verhindern, muss eine Höhe von 6 Fuß / 1,8 Metern über ihre gesamte Länge erreichen, einschließlich der Bereiche, in denen sich das Bodenniveau ändert; d.h. niedriger ist.*	✔		
7.1.8	Die physischen Barrieren um die Bereiche Frachtumschlag, Versand- und Annahmehof müssen in einem guten Zustand gehalten werden.	✔		
7.1.9	Zutrittstore für die Bereiche Frachtumschlag, Versand- und Annahmehof müssen entweder bewacht oder elektronisch kontrolliert werden.	✔		

Kapitel	Perimeter / Umgrenzung	A	B	C
7.1.10	Die physischen Barrieren um die Bereiche Frachtumschlag, Versand- und Annahmehof müssen mindestens 1x wöchentlich auf Unversehrtheit und Beschädigung überprüft werden.	✔		
Äußere Ladebereiche				
7.1.11	Der äußere Ladebereich wird durch Farb- oder Tag/Nacht-Kameras abgedeckt	✔	✔	✔
7.1.12	Die installierten Kameras müssen in der Lage sein, jederzeit alle Tätigkeiten und Bewegungen rund um den Außenbereich der Ladetore zu sehen, es sei denn, dass eine vorübergehende Einschränkung der Sicht aufgrund von Betriebsanforderungen (z.B. LKW Be- und Entladen in Echtzeit) besteht.	✔	✔	✔
7.1.13	Alle Fahrzeuge und Personen im Bereich äußere Ladetore sind klar erkennbar	✔		
7.1.14	Alle Fahrzeuge und Personen im Bereich äußere Ladetore sind meistens sichtbar		✔	✔
7.1.15	Alle Bereiche um die Ladetore sind vollständig beleuchtet	✔	✔	✔
Zugang Privatfahrzeuge				
7.1.16	Privatfahrzeuge im Bereich Frachtumschlag, Versand- und Annahmehof sind nur dann erlaubt, wenn dies vorab genehmigt wurde und auf gekennzeichnete / ausgewiesene Parkbereiche beschränkt ist. Kein persönlicher Parkplatz darf innerhalb von 25 m zu Fuß zu externen Ladebereichen liegen. Die Prozesse für die Vorabgenehmigung und Einschränkungen sind vorhanden.	✔	✔	✔

Kapitel	Außenwände, Dach, Türen	A	B	C
7.2				
Außenseiten des Gebäudes: CCTV/Kameraüberwachung				
7.2.1	Farb- oder Tag / Nacht-Außenkamerasystem vorhanden, das alle Außenseiten des Gebäudes abdeckt.	✔		
7.2.2	Farb- oder Tag / Nacht-Außenkamerasystem vorhanden, das alle Außenseiten des Gebäudes mit Türen, Fenster oder sonstigen Öffnungen abdeckt.		✔	
7.2.3	Alle Bilder sind jederzeit deutlich, es sei denn, dass eine vorübergehende Einschränkung der Sicht aufgrund von Betriebsanforderungen (z.B. LKW-Be- und Entladen in Echtzeit) besteht.	✔		
7.2.4	Alle Fahrzeuge und Personen sind im Kamerasystem deutlich erkennbar	✔		
7.2.5	Fahrzeuge und Personen sind im Kamerasystem in den meisten Fällen sichtbar		✔	
Außenwände und Dach				
7.2.6	Außenwände und Dach sind so konstruiert und instandgehalten, dass sie dem Eindringen von außen standhalten (Beispiel: Ziegel, Block, Kippbetonplatte, Sandwichplattenwände).	✔	✔	✔
7.2.7	Alle zu öffnenden Fenster, Lüftungsöffnungen oder sonstigen Öffnungen in den Außenwänden der Anlage oder Fenster, die sich nicht öffnen lassen und die weniger als 3 Meter vom Arbeitsboden entfernt in den Außenwänden der Anlage installiert sind, müssen eine physische Barriere aufweisen oder alarmgesichert und mit dem Hauptalarmsystem verbunden sein.	✔	✔	
7.2.8	Alle zu öffnenden Fenster, Oberlichter, Lüftungsschlitze, Zugangsklappen oder sonstigen Öffnungen im Dach der Anlage müssen eine physische Barriere aufweisen oder alarmgesichert und mit dem Hauptalarmsystem verbunden sein.	✔		

Kapitel	Außenwände, Dach, Türen	A	B	C
7.2.9	Der Außenzugang zum Dach (Leiter oder Treppe) muss: Physisch gesichert und durch Videoüberwachung (Farb- oder Tag / Nacht-Kameras) abgedeckt sein oder physisch gesichert und alarmgesichert sein.	✔		
7.2.10	Der Außenzugang zum Dach (Leiter oder Treppe) ist physisch gesichert.		✔	✔
7.2.11	Alle Außentüren zum Lager und den Büros am Gebäude müssen alarmgesichert sein um nicht autorisierte Öffnung zu erkennen und müssen mit der Hauptalarmanlage verbunden sein. *Hinweis: Rampentüren fallen nicht unter diese Anforderung. Siehe Abschnitt 7.2.17 für Anforderungen an Türenalarme für Rampen.*	✔	✔	✔
7.2.12	Jede Außentür zum Lager, jede Bürotür oder andere Öffnung am Gebäude kann eindeutig innerhalb der Hauptalarmanlage per Tür oder per Zone zugeordnet werden.	✔		
7.2.13	Alle Außentüren zum Lager müssen immer verschlossen und gesichert sein, wenn sie nicht aktiv genutzt werden. Schlüssel oder Code gesteuert.	✔	✔	
7.2.14	Lager Fußgängertüren und Rahmen können nicht leicht durchbrochen werden. Wenn Scharniere außen angebracht sind, müssen sie verankert oder punktgeschweißt werden. Glastüren sind nicht akzeptabel, es sei denn, Glasbruchmelder sind angebracht oder eine andere Erkennungsvorrichtung ist installiert (z. B. PIR/Passiv-Infrarot-Sensorik) und alarmiert direkt das Überwachungszentrum oder das Glas wird durch Gitterstäbe / Drahtgeflecht geschützt.	✔	✔	✔
7.2.15	Notausgänge, die auch nur im Notfall genutzt werden (z.B. bei Feuer) müssen jederzeit mit einem akustischen Alarmgeber, einzeln oder per Zone, gesichert sein	✔	✔	
7.2.16	Alle Ladetore müssen stark genug ausgelegt sein um den gewaltsamen Zutritt mit Hilfe von kleinen tragbaren Handwerkzeugen zu verhindern und/oder zu verzögern.	✔	✔	✔
7.2.17	**Ladetore** **Außerhalb der Öffnungszeiten:** Ladetore sind geschlossen, gesichert (z.B. elektronisch deaktiviert oder physisch verschlossen). Um unerlaubtes Eindringen zu erkennen sind die Ladetore alarmgesichert und mit dem Hauptalarmsystem verbunden. **Während der Öffnungszeiten:** Ladetore müssen geschlossen sein, wenn sie nicht aktiv genutzt werden. Falls Scherengitter-Tore genutzt werden, müssen diese durch mechanische Schiebe- / Verriegelungsschlösser gesichert sein und mindestens 8 Fuß / 2,4 Meter hoch sein.	✔	✔	✔

Kapitel	Büro und Lagerhaus Eingänge und Ausgänge	A	B	C
7.3				

Kapitel	Büro und Lagerhaus Eingänge und Ausgänge	A	B	C
Bürobereich Besuchereingang				
7.3.1	Der Zugang zu Besuchereingängen im Bürobereich, wird von einem Mitarbeiter / Wachmann / Empfangsmitarbeiter kontrolliert, der / die in Bezug auf die Ausstellung von Ausweisen, Kontrollen, Protokollierung, Besucher, Begleitanforderungen usw. geschult wurde (ein Verfahren für Besuche außerhalb der Öffnungszeiten liegt vor).	✔	✔	✔
7.3.2	Die Eingangsbereiche für Besucher im Büro sind durch Überwachungskameras (Farb- oder Tag/Nacht-Kamera) abgedeckt. Personen sind jederzeit deutlich erkennbar.	✔	✔	
7.3.3	In den Eingangsbereichen für Besucher im Büro ist ein Alarm bei Bedrohung installiert, dieser wird wöchentlich getestet.	✔	✔	
7.3.4	Alle Besucher des Bürobereichs müssen anhand eines behördlich ausgestellten Lichtbildausweises identifiziert werden (z. B. Führerschein, Reisepass oder Personalausweis usw.).	✔	✔	✔
7.3.5	Alle Besucher müssen registriert werden, die Protokolle müssen mindestens 30 Tage aufbewahrt werden.	✔	✔	✔
7.3.6	Wenn der Besucher das Gelände verlässt muss der Besucherausweis abgegeben werden und das vollständige Protokoll ist täglich zu kontrollieren.	✔	✔	
7.3.7	Alle Besucher müssen ihren Besucherausweis gut sichtbar tragen und von Firmenmitarbeitern begleitet werden.	✔	✔	
Personaleingänge				
7.3.8	Personaleingänge sind 24/7 zugangskontrolliert		✔	✔
7.3.9	Personaleingänge werden 24/7 durch ein elektronisches Zutrittskontrollsystem kontrolliert. Jeder Zutritt ist protokolliert.	✔		
7.3.10	Personaleingänge sind durch Videoüberwachungskameras abgedeckt. (Farb- oder Tag/Nacht Kameras).	✔	✔	
7.3.11	Nach Abschluss der Sicherheitsüberprüfung müssen allen Mitarbeitern Firmenfotoausweise ausgestellt werden.	✔	✔	
7.3.12	Alle anderen Mitarbeiter müssen mit einem Firmenausweis ausgestattet sein, damit sie innerhalb des Betriebes erkennbar sind.	✔	✔	
7.3.13	Alle Mitarbeiterausweise müssen gut sichtbar getragen werden	✔	✔	
7.3.14	Firmenausweise dürfen unter keinen Umständen gemeinsam benutzt werden und die Richtlinien zur Ausstellung von Firmenausweisen müssen dokumentiert sein.	✔	✔	
Fahrer- und Fahrzeugidentifikation				
7.3.15	Alle Fahrer müssen mittels behördlich ausgegebenen Lichtbildausweisen identifiziert werden (z.B. Führerschein, Pass oder Personalausweis) und ein Fahrerprotokoll muss geführt werden.	✔	✔	✔
7.3.16	Überprüfung, dass der Führerschein gültig ist, dass der Lichtbildausweis nicht abgelaufen ist und dass die Unterlagen zum Fahrer passen.	✔	✔	✔
7.3.17	Fahrzeugerkennungen werden von Hand protokolliert (d.h. schriftlich) oder mit Hilfe von Kameras. Diese müssen mindestens das Kfz-Kennzeichen und den Fahrzeugtyp beinhalten.	✔		

Kapitel	Innerhalb des Lager und der Büros	A	B	C
7.4				
Lagerbereich: Trennwände in einem Multi-Lager				
7.4.1	Im Lagerbereich für verschiedene Mieter sind die raumhohen Innentrennwände und das Dach so ausgelegt/gebaut und instandgehalten, dass sie Schutz vor Eindringen von außen bieten (Beispiel: Ziegel, Block, Kippbetonplatte, Sandwichplattenwände).	✔	✔	✔
7.4.2	Wenn die raumhohen Trennwände aus Drahtgeflecht mit Sicherheitsqualität oder einer anderen branchenweit anerkannten sicheren Barriere bestehen, muss auch ein Alarm ausgelöst werden, um ein Eindringen zu erkennen. Hinweis: Netze, minderwertige Zäune oder Maschendraht ohne Sicherheitsqualität sind nicht zulässig.	✔	✔	✔
Lagerbereich innen				
7.4.3	Einbruchmeldung (z. B. Infrarot-, Bewegungs-, Ton- oder Vibrationserkennung) ist erforderlich, um den internen Lagerbereich zu überwachen. Die Alarme müssen aktiviert und außerhalb der Öffnungszeiten mit der Hauptalarmanlage verbunden sein (d.h. wenn das Lager geschlossen ist). *Hinweis: Wenn das Lager ein echter 24/7/366 Betrieb ist, kann diese Anforderung N/A sein, wenn die Risiken und Abhilfemaßnahmen in der örtlichen Risikobewertung dokumentiert sind.* *Unabhängig von Öffnungszeiten sind Einbruchmelder oder physische Barrieren an der Umgrenzung an den Außentüren sowie ebenerdigen Fenstern, sowohl im Büro- als auch im Lagerbereich, erforderlich. (siehe Kapitel 7.2.11).*	✔		
Interne Ladetore und Ladebereiche				
7.4.4	Alle internen Ladetore und Ladebereiche werden durch die Videoüberwachungskameras abgedeckt (Farb- oder Tag/Nacht Kameras).	✔	✔	✔
7.4.5	Zu jeder Zeit uneingeschränkte Sicht auf die geladene-/entladene Fracht es sei denn, dass eine vorübergehende Einschränkung der Sicht aufgrund von Betriebsanforderungen (d.h. LKW-Be- und Entladen in Echtzeit) besteht.	✔	✔	✔
7.4.6	Das Eigentum des Käufers ist in Lagerbewegungs- und Zwischenlagerbereich (d.h. Bereiche in denen die Ware auf oder von Paletten bewegt wird, Wege von und zu Lagerregalen, Laderampen, Durchgängen) zu 100% unter Videoüberwachung.	✔	✔	
Zutrittskontrolle zwischen Büro und Lager/Ladebereich				
7.4.7	Zutritt zwischen Büro und Ladebereich oder Lagerhalle ist kontrolliert.	✔	✔	
7.4.8	Türalarme für Zutritt mit Karte oder Türsprechanlage zwischen Büro und Ladebereich/Lager sind örtlich hörbar **und** erzeugen einen Alarm zur Reaktion, wenn die Tür für mehr als 60 Sekunden offengehalten wird oder sofort, wenn sie gewaltsam geöffnet wird.	✔		
7.4.9	Türalarme für Türen zwischen Büro und Ladebereich/Lager sind örtlich hörbar **oder** erzeugen einen Alarm zur Reaktion, wenn die Tür für mehr als 60 Sekunden offengehalten wird oder wenn sie gewaltsam geöffnet wird.		✔	
7.4.10	Der Zutritt zum Lager ist beschränkt und nur berechtigten Mitarbeitern des LSP/Antragsteller sowie begleiteten Besuchern, basierend auf Geschäftsanforderungen, erlaubt.	✔	✔	✔

Kapitel	Innerhalb des Lager und der Büros	A	B	C
7.4.11	Die Zutrittsliste zum Lager/Verladebereich wird mindestens vierteljährlich überprüft um zu begrenzen/zu überprüfen, dass die Zugriffsberechtigung nur dem benannten/autorisierten Personal gewährt wird.	✔	✔	
Sicherheitskäfige / -bereich für hochwertige Fracht (HVC)				
7.4.12	Die Größe und Nutzung von HVC (Sicherheitskäfig für hochwertige Fracht) kann durch die Käufer - LSP/Antragsteller Vereinbarung vorgeschrieben werden. Wenn es eine solche Vereinbarung nicht gibt, dann muss der HVC mindestens ein Stauvolumen von 6 Kubikmetern für Produkte haben.	✔	✔	
7.4.13	Gitterumzäunung oder harte Wände von allen Seiten, inklusive Deckel/Dach.	✔	✔	
7.4.14	Verriegelungsvorrichtung an der Tür/Tor.	✔	✔	
7.4.15	Komplette Abdeckung sowohl des Eingangs- als auch des Innenbereiches des HVC durch die Videoüberwachungsanlage (Farb- oder Tag/Nacht Kameras). *Hinweis: Falls der HVC zu klein ist um eine Kamera innen anzubringen ist es ausreichend, wenn der Eingangsbereich abgedeckt ist*	✔		
7.4.16	Eingangsbereich des HVC ist durch die Videoüberwachungsanlage (Farb- oder Tag/Nacht Kamera) abgedeckt.		✔	
7.4.17	Wenn mehr als 10 Personen Zutritt zum HVC benötigen, dann ist der Zutritt elektronisch per Karte/Transponder zu kontrollieren. Wenn 10 oder weniger Personen Zugang benötigen, reicht ein Hochleistungsschloss oder ein Vorhängeschlosssystem, das von einem kontrollierten Schlüsselausgabesystem unterstützt wird. Schlüssel können an eine Einzelperson für die Dauer einer Schicht abgegeben werden, dürfen aber nicht ohne Genehmigung weitergegeben werden und müssen im Schlüsselprotokoll aufgezeichnet sein. Bei Nichtbenutzung müssen alle Schlüssel zurückgegeben und im Bestand wieder aufgeführt werden.	✔		
7.4.18	HVC Türen/Tore sind alarmgesichert um gewaltsames Eindringen festzustellen. Alarme können durch Türkontakte und/oder Nutzung des Bewegungsmelders der Videoüberwachungsanlage generiert werden um nicht genehmigten Zutritt zu erkennen.	✔		
7.4.19	Alle Wände/Umzäunungen des HVC werden in gutem Zustand erhalten und einmal monatlich auf Unversehrtheit und Beschädigung untersucht.	✔		
7.4.20	LSP/Applicant to ensure that access to the HVC is only granted to designated/authorized personnel. Die genehmigte Zugangsliste für den HVC wird monatlich überprüft und unverzüglich aktualisiert, wenn ein Mitarbeiter das Arbeitsverhältnis beendet oder keinen Zugriff mehr benötigt. Das Verfahren für den HVC-Zugang ist dokumentiert.	✔	✔	
Müllinspektion vom Lager				
7.4.21	Interne und/oder externe Lagerhaus-Müllsammelbehälter / Müllsammelstellen werden von der Videoüberwachungsanlage überwacht.	✔		
7.4.22	Wenn Müllsäcke im Lager genutzt werden, sind diese transparent.		✔	✔

Vorladung und Bereitstellung				
7.4.23	Außerhalb der Öffnungszeiten ist das Abstellen oder Vorladen von FTL / für den Käufer bestimmte LKW außerhalb des Lagerhauses nicht erlaubt, es sei denn, dass dieses ausdrücklich zwischen Käufer und LSP/Antragsteller vereinbart worden ist. Alternative Sicherheitsmaßnahmen müssen implementiert werden (z. B. zusätzliche Sicherheitseinrichtungen an dem Transportbehälter). *Hinweis: „Außerhalb des Lagerhauses" sind die Bereiche, die von der Einrichtung getrennt sind, sich jedoch noch innerhalb des Hofbereiches / des eingezäunten Geländes des LSP / Antragstellers befinden.*	✔	✔	✔
Persönliche Behälter und Kontrollen am Ausgang				
7.4.24	Schriftliche Sicherheitsverfahren definieren, wie "persönliche Behälter" innerhalb des Lagers kontrolliert werden. Zu den persönlichen Behältern gehören Brotdosen, Rucksäcke, Kühltaschen, Handtaschen usw.	✔	✔	
7.4.25	Wenn dies nach örtlichem Recht zulässig ist, muss der LSP / Antragsteller ein dokumentiertes Verfahren für Ausgangskontrollen entwickeln und aufrechterhalten. Die Aktivierung des Verfahrens liegt im Ermessen des LSP / Antragstellers und / oder gemäß der Vereinbarung zwischen Käufer / LSP / Antragsteller. Das Verfahren muss mindestens das Recht des LSP / Antragstellers auf Suchkriterien berücksichtigen, falls die Notwendigkeit besteht Durchsuchungen durchzuführen, wenn diese normalerweise nicht erforderlich sind (z. B. wenn der Verdacht auf Diebstahl durch Mitarbeitern besteht).	✔		
Kontrolle der Frachtumschlagausrüstung				
7.4.26	Es muss ein dokumentiertes Verfahren vorliegen, welches festlegt, dass alle Gabelstapler und sonstige Güterumschlagsgeräte außerhalb der Öffnungszeiten deaktiviert sein müssen. *Hinweis: Dieses schließt Handhubwagen nicht mit ein.*	✔	✔	
Unversehrtheit von Container und Auflieger/Anhänger; 7 Punkte Überprüfung				
7.4.27	Für alle für einen Käufer bestimmte ausgehenden Container, Auflieger oder Anhänger wird eine 7-Punkte-physische Kontrolle durchgeführt: Vorderwand, linke Seite, rechte Seite, Boden, Decke/Dach, Türen und Verriegelung von innen/außen und Außenseite Fahrgestell. Die Vorgehensweise muss dokumentiert sein. *Hinweis: Dieses ist anwendbar für alle Typen von Container oder Auflieger/Anhänger mit Schloss und/oder Plombe (d.h. nicht beschränkt auf Seefrachtcontainer).*	✔	✔	✔
Frachtübergabeprozess: Sicherheitsplomben				
7.4.28	Sofern vom Käufer nicht ausdrücklich von dieser Verpflichtung befreit, werden bei allen direkten Nonstop-Lieferungen manipulationssichere Sicherheitsplomben verwendet. Die Plomben müssen nach ISO 17712 (I-, S- oder H-Klassifizierung) zertifiziert sein. *Hinweis: Sicherheitsplomben müssen für Transporte mit Zwischenstopps auf Grund der Unübersichtlichkeit und des Aufwands für den Fahrer durch das Mitführen mehrerer Plomben, nicht verwendet werden.*	✔	✔	✔
7.4.29	LSP/Antragsteller muss ein dokumentiertes Verfahren für die Verwaltung und Kontrolle von Plomben, Anhängern (Containern) Türschlössern, Königszapfen-Schlösser und anderer Sicherheitsausrüstung haben.	✔	✔	✔

7.4.30	Sicherheitsplomben werden nur von autorisiertem Personal, d. h. Lagerpersonal, das unterwiesen ist, beschädigte Plomben zu erkennen und zu melden, angebracht oder entfernt werden. Die Plomben dürfen niemals vom Fahrer angebracht oder entfernt werden, es sei denn diese Ausnahme ist mit dem Käufer vereinbart.	✔	✔	✔
7.4.31	Ein Verfahren zur Erkennung und Meldung beschädigter Sicherheitsplomben ist vorhanden.	✔	✔	✔
Unversehrtheit der Fracht; Validierungsprozess beim Laden / Entladen				
7.4.32	Es gibt zuverlässige Verfahren die sicherstellen, dass alle transportierten und erhaltenen Vermögenswerte des Käufers zum Zeitpunkt der Übergabe validiert werden, indem eine manuelle und / oder elektronische Stückzählung durchgeführt wird. Der Prozess muss sicherstellen, dass Unregelmäßigkeiten lückenlos erkannt, dokumentiert und dem LSP / Antragsteller und / oder Käufer gemeldet werden. Manuelle und / oder elektronische Aufzeichnungen müssen von Beweisqualität sein. Wenn kein Fahrer anwesend ist, um diese Tätigkeit zu bezeugen, muss der Käufer / LSP / Antragsteller eine alternative Überprüfung der Anzahl sicherstellen, z. B. Scans und / oder CCTV-Bilder, die speziell für diesen Zweck gesammelt und aufbewahrt werden. Hinweis: Zusätzlich zu fehlenden Teilen können Unregelmäßigkeiten sein: Schäden, fehlende Bänder oder Klebebänder, Schnitte oder andere offensichtliche Öffnungen, die auf einen möglichen Diebstahl hinweisen.	✔	✔	✔
Betrügerische Abholung				
7.4.33	Die ID des LKW-Fahrers, Dokumentation zur Abholung der Ladung und die Angaben der kundenbezogenen Voravise werden vor dem Laden überprüft. Ein dokumentiertes Verfahren muss vorhanden sein.	✔	✔	✔

Kapitel	Sicherheitssysteme; Ausgestaltung, Überwachung und Reaktion.	A	B	C
7.5				
Überwachungsstelle				
7.5.1	Überwachung von Alarmereignissen 24x7x366 über eine interne oder externe Überwachungsstelle, geschützt vor unbefugtem Zutritt. *Hinweis: Überwachungsstellen können sich innerhalb oder außerhalb der Betriebsstätte befinden und können firmeneigen oder eine Fremdfirma sein. In allen Fällen muss der Zutritt durch die Verwendung eines elektronischen Zutrittskontrollsystems (Ausweis), Schlössern oder biometrischen Scannern gesteuert werden.*	✔	✔	✔
7.5.2	Überwachungsstelle reagiert auf alle Alarme des Sicherheitssystems in Echtzeit 24x7x366	✔	✔	✔
7.5.3	Die Überwachungsstelle bestätigt die Alarmaktivierung und reagiert (informiert die nächsthöhere Stelle) in weniger als drei Minuten.	✔	✔	✔

Kapitel	Sicherheitssysteme; Ausgestaltung, Überwachung und Reaktion.	A	B	C
7.5.4	Alarmüberwachungsberichte sind verfügbar.	✔	✔	✔
7.5.5	Die Reaktionsprozesse der Überwachungsstelle sind dokumentiert.	✔	✔	✔
Einbruchmeldeanlage (IDS)				
7.5.6	Die Einbruchmeldeanlage muss außerhalb der Öffnungszeiten aktiviert und mit der Hauptalarmanlage verbunden sein.	✔	✔	✔
7.5.7	Alarmaufzeichnungen der Sicherheitssysteme werden 60 Tage aufbewahrt.	✔	✔	
7.5.8	Die Alarmaufzeichnungen sind sicher gespeichert und es existiert eine Sicherheitskopie.	✔		
7.5.9	Die Alarmaufzeichnungen sind sicher gespeichert.		✔	
7.5.10	Es existiert ein dokumentiertes Verfahren das sicherstellt, dass der Zugriff auf die Einbruchmeldeanlage auf autorisierte Personen oder Systemadministratoren beschränkt ist. Dies umfasst Server, Konsolen, Controller, Panels, Netzwerke und Daten. Die Zugriffsrechte müssen umgehend aktualisiert werden, wenn Personen das Unternehmen verlassen oder sich die Funktion ändert und kein Zugriff mehr benötigt wird.	✔	✔	✔
7.5.11	Ein Alarm muss ausgelöst werden bei Stromausfall / Signalverlust *Hinweis: Bei Systemen mit unterbrechungsfreier Stromversorgung (USV) wird der Alarm gesendet, wenn die USV-Batterie ausfällt.*	✔	✔	✔
7.5.12	Überprüfungsprozess, dass der Alarm auch aktiviert ist. *Hinweis: Ein dokumentiertes Verfahren zur Überprüfung, ob Alarme außerhalb der Betriebszeiten aktiviert sind, ist vorhanden.*	✔	✔	✔
7.5.13	IDS Alarm wird bei Ausfall eines Gerätes oder Leitungsstörung über Festnetz übertragen.	✔	✔	
7.5.14	Es existiert ein Sicherungskommunikationssystem für den Fall eines Geräteausfalls oder einer Leitungsstörung.	✔	✔	
Automatisches Zugangskontrollsystem (AACS)				
7.5.15	90 Tage der Zugangskontrollaufzeichnungen sind verfügbar. Die Aufzeichnungen sind sicher gespeichert und es existiert eine Sicherheitskopie.	✔	✔	
7.5.16	Es existiert ein dokumentiertes Verfahren das sicherstellt, dass der Zugriff auf das Zugangskontrollsystem auf autorisierte Personen oder Systemadministratoren beschränkt ist. Die Zugriffsrechte müssen umgehend aktualisiert werden, wenn Personen das Unternehmen verlassen oder sich die Funktion ändert und kein Zugriff mehr benötigt wird.	✔	✔	
7.5.17	Die Berichte des Zugriffssystems werden mindestens vierteljährlich überprüft, um Unregelmäßigkeiten oder Missbrauch festzustellen (z.B. mehrere erfolglose Versuche, falsche Auslesung (z.B. durch deaktivierte Karte), Beweise für die gemeinsame Nutzung von Karten, um unbefugten Zugriff zu ermöglichen usw.). Prozess an Ort und Stelle.	✔	✔	
Überwachungskamerasysteme (CCTV)				

Kapitel	Sicherheitssysteme; Ausgestaltung, Überwachung und Reaktion.	A	B	C
7.5.18	Digitale Aufzeichnungen der Überwachungskameras sind vorhanden.	✔	✔	✔
7.5.19	Die Aufnahmegeschwindigkeit für die Überwachungskameras ist auf mindestens 8 Bilder pro Sekunde (fps) pro Kamera eingestellt. *Hinweis: TAPA erlaubt bestehenden Zertifizierungsinhaber ohne Upgrade auf 8 fps bis zur Revision 2023 mit vorhandenen 3 fps fortzufahren.* *Neue Zertifikatsinhaber müssen die neue Anforderung erfüllen.*	✔	✔	✔
7.5.20	Die digitale Aufzeichnungsfunktionalität wird an Betriebstagen täglich gemäß dem dokumentierten Verfahren überprüft. Aufzeichnungen sind verfügbar.	✔	✔	✔
7.5.21	Die Aufzeichnungen der Überwachungskameras werden mindestens 30 Tage lang gespeichert, sofern dies nach örtlichem Recht zulässig ist. LSP / Antragsteller muss lokale Gesetze nachweisen, die die Verwendung von Videoüberwachung verbieten und / oder die Speicherung von Videodaten auf weniger als 30 Tage beschränken.	✔	✔	✔
7.5.22	Der Zugriff auf das CCTV-System ist streng kontrolliert, einschließlich Hardware, Software und Daten- / Videospeicher.	✔	✔	✔
7.5.23	Lediglich autorisiertes Personal und nur aus Sicherheitsgründen darf die Kamerabilder ansehen.	✔	✔	✔
7.5.24	In Übereinstimmung mit den örtlichen Gesetzen ist ein Verfahren zur Datenschutzrichtlinie für Videoüberwachung in Bezug auf die detaillierte Verwendung von Echtzeit- und Archivbildern vorhanden.	✔	✔	
Außen- und Innenbeleuchtung				
7.5.25	Die Beleuchtungsstärke im Außen- und Innenbereich ist so ausreichend, dass sie die Bildaufzeichnung für eine Untersuchung in Beweisqualität ermöglicht.	✔	✔	
7.5.26	Die Beleuchtungsstärke im Außen- und Innenbereich ist so ausreichend, dass alle Fahrzeuge und Personen klar erkennbar sind	✔		

Kapitel	Schulung und Vorgehensweise	A	B	C
7.6				
Eskalationsverfahren				
7.6.1	Es sind dokumentierte Verfahren für den Umgang mit Vermögenswerten des Käufers örtlich vorhanden, einschließlich der Verfahren zur rechtzeitigen Meldung verlorener, fehlender oder gestohlener Vermögenswerte des Käufers. Dies sind Vorfälle, die der LSP / Antragsteller dem Käufer innerhalb von 24 Stunden melden muss. Offensichtliche Diebstähle müssen sofort gemeldet werden. Der Prozess wird konsequent verfolgt.	✔	✔	✔
7.6.2	Notfallkontaktdaten vom Käufer und LSP / Antragsteller für Sicherheitsvorfälle sind aufgelistet und verfügbar. Die Liste wird alle 6 Monate aktualisiert und enthält auch Notfallkontakte der Strafverfolgungsbehörden.	✔	✔	✔
Engagement der Geschäftsführung				

Kapitel	Schulung und Vorgehensweise	A	B	C
7.6.3	Die Geschäftsführung des Lieferanten muss offiziell eine verantwortliche Person für die Sicherheit vor Ort ernannt haben, die für die Einhaltung der Sicherheitsanforderungen für TAPA FSR und die Lieferkette des Unternehmens zuständig ist. Der Lieferant muss auch eine für die Überwachung des FSR-Programms verantwortliche Person (kann dieselbe sein) ernennen. Dies umfasst die Planung von Konformitätsprüfungen, die Kommunikation mit AAs, die Rezertifizierung, Änderungen des FSR-Standards usw. *Hinweis: Diese Personen können eigene Mitarbeiter oder Mitarbeiter von Fremdfirmen, die unter Vertrag stehen um diese Funktion zu übernehmen, sein.*	✔	✔	✔
7.6.4	Die Geschäftsführung muss eine Sicherheitsrichtlinie entwickeln, kommunizieren und aufrechterhalten, um sicherzustellen, dass alle relevanten Personen (d. h. Mitarbeiter und Auftragnehmer) die Sicherheitserwartungen des Unternehmens genau kennen.	✔	✔	✔
7.6.5	Eine Risikobewertung des Standortes, die die Wahrscheinlichkeit und die Auswirkungen sicherheitsrelevanter Ereignisse berücksichtigt, muss mindestens einmal jährlich durchgeführt / aktualisiert werden. Für den Risikobewertungsprozess muss das Management fundierte Entscheidungen über Schwachstellen und Schadensbegrenzung treffen. Zumindest müssen die folgenden gemeinsamen internen / externen Ereignisse bewertet werden: Diebstahl von Fracht oder Informationen, unbefugter Zugang zu Einrichtungen oder Fracht, Manipulation / Zerstörung von Sicherheitssystemen, fiktive Abholung von Fracht, Kontinuität der Sicherheit auch bei Arbeitskräftemangel oder Naturkatastrophen, etc. Zusätzliche Ereignisse können aufgrund lokaler / länderspezifischer Risiken in Betracht gezogen werden.	✔	✔	✔
Schulung				
7.6.6	Innerhalb der ersten 60 Arbeitstage und danach alle zwei Jahre muss allen Mitarbeitern eine Schulung zur Sicherheits- / Bedrohungsaufklärung angeboten werden.	✔	✔	✔
7.6.7	Mit allen Mitarbeitern, die Zugriff auf die elektronischen und physischen Versanddaten des Käufers haben, wird eine Schulung zur Sensibilisierung der Informationssicherheit durchgeführt.	✔	✔	
Zugang zu den Vermögenswerten des Käufers				
7.6.8	Ein dokumentiertes Verfahren ist vorhanden, um die Vermögenswerte des Käufers (z.B. Fracht) vor unbefugtem Zugriff durch Arbeitskräfte, Besucher usw. zu schützen.	✔	✔	
Informationskontrolle				
7.6.9	Der Zugriff auf Versanddokumente und Informationen zu den Vermögenswerten des Käufers, sind auf der Grundlage des „Need to Know“ Prinzips geregelt.	✔	✔	✔
7.6.10	Der Zugriff auf Versanddokumente und Informationen zu den Vermögenswerten des Käufers wird überwacht und protokolliert.	✔	✔	✔
7.6.11	Versanddokumente und Informationen zu den Vermögenswerten des Käufers sind bis zur Vernichtung geschützt.	✔	✔	✔
Berichterstattung von Sicherheitsvorfällen				

Kapitel	Schulung und Vorgehensweise	A	B	C
7.6.12	Ein System zur Berichterstattung und Verfolgung von Sicherheitsvorfällen ist vorhanden, um dies zur Implementierung proaktiver Maßnahmen zu nutzen.	✔	✔	
Instandhaltungsprogramm				
7.6.13	Ein Wartungsprogramm für alle technischen (physischen) Sicherheitsinstallationen / -systeme ist vorhanden, um jederzeit die Funktionalität sicherzustellen (z. B. Videoüberwachung, Zugangskontrolle, Einbruchmeldeanlage und Beleuchtung).	✔	✔	✔
7.6.14	Vorbeugend wird die Wartung einmal im Jahr oder gemäß den Angaben des Herstellers durchgeführt.	✔	✔	✔
7.6.15	Funktionsüberprüfungen aller Systeme wird einmal pro Woche durchgeführt und dokumentiert, es sei denn, dass ein Systemfehler sofort / automatisch gemeldet oder alarmiert wird.	✔	✔	
7.6.16	Ein Reparaturauftrag muss innerhalb von 48 Stunden nach dem Entdecken der Störung veranlasst werden. Für jegliche Reparaturen, die die erwartete Reparaturzeit von 24 Stunden überschreiten, müssen alternative Risikominimierungen umgesetzt werden.	✔	✔	
Einarbeitung von Auftragnehmern				
7.6.17	LSP / Antragsteller hat sicherzustellen, dass alle Subunternehmer / Lieferanten die für sie relevanten Sicherheitsprogramme des LSP / Antragsteller kennen und einhalten.	✔	✔	✔
Versand- und Empfangsunterlagen				
7.6.18	Die Versand- und Empfangsdokumente müssen lesbar, vollständig und sorgfältig ausgefüllt sein z.B. Uhrzeit, Datum, Unterschriften, Namen von Fahrer, Versand- und Empfangspersonal, Frachtangaben und -menge usw.).	✔	✔	✔
7.6.19	LSP / Antragsteller muss Aufzeichnungen über alle Abholungen und Abliefernachweise für einen Zeitraum von mindestens zwei Jahren aufbewahren und diese bei Bedarf für Schadensuntersuchungen zur Verfügung stellen.	✔	✔	✔
7.6.20	Die Abliefernachweise müssen in Übereinstimmung mit der schriftlichen Vereinbarung zwischen dem Käufer und dem LSP / Antragsteller erbracht werden. Wenn vom Käufer gefordert, muss der Empfänger der Ware innerhalb des vereinbarten Zeitraumes den Absender über den Sendungseingang informieren und die Details des Voravis abgleichen.	✔	✔	✔
Voravis Prozess ist eingeführt				
7.6.21	Wenn vom Käufer gefordert, ist ein Voravis-Prozess für eingehende und / oder ausgehende Sendungen vorhanden. Die Einzelheiten für das Voravis müssen zwischen Käufer und vom LSP / Antragsteller vereinbart werden. Vorgeschlagene Einzelheiten sind: Abfahrtszeit, voraussichtliche Ankunftszeit, Transportunternehmen, Name des Fahrers, Kfz-Kennzeichen, Frachtinformationen (Stückzahl, Gewicht, Frachtbriefnummer usw.) und Nummer der Sicherheitsplombe am Auflieger.	✔	✔	✔

Kapitel	Mitarbeiterintegrität	A	B	C
7.7				

Kapitel	Mitarbeiterintegrität	A	B	C
7.1	Screening/Sicherheitsüberprüfung /Hintergrundprüfung (soweit gesetzlich zulässig)			
7.7.1	Der LSP / Antragsteller muss über ein Screening- / Überprüfungs- / Hintergrundverfahren verfügen, das mindestens frühere Beschäftigungsverhältnisse und die strafrechtliche Überprüfungen der Vergangenheit umfasst. Überprüfungen gelten für alle Bewerber, einschließlich Mitarbeiter und Subunternehmer. Der LSP / Antragsteller verlangt von seinen Vertragsunternehmen, die Zeitarbeiter vermitteln, ein gleichwertiges Verfahren durchzuführen.	✔	✔	✔
7.7.2	Der Zeitarbeits-Mitarbeiter muss eine Erklärung unterzeichnen, dass er keine aktuellen strafrechtlichen Verurteilungen hat und die Sicherheitsverfahren von LSP / Antragsteller befolgen wird.	✔	✔	✔
7.7.3	LSP / Antragsteller hat mit dem Dienstleister zur Vermittlung von Zeitarbeitern und / oder dem Subunternehmer eine Vereinbarung getroffen, wonach dieser die entsprechenden Informationen liefert oder er führt diese Überprüfungen selbst durch. Das Screening muss eine Überprüfung von Vorstrafen und der Beschäftigungsverhältnisse umfassen.	✔	✔	✔
7.7.4	Es besteht ein Verfahren für den Umgang mit den Bewerbern / Mitarbeitern, die falsche Angaben gemacht haben, vor & nach der Einstellung.	✔	✔	✔
Kündigung oder Wiedereinstellung von Mitarbeitern *Hinweis: Die Kündigung beinhaltet sowohl freiwillige als auch unfreiwillige Trennungen – gekündigte Mitarbeiter und die Mitarbeiter, die selbst gekündigt haben.*				
7.7.5	Von dem gekündigten Personal müssen die firmeneigenen Gegenstände wie Firmenausweise, Zugangsausweise, Schlüssel, Ausstattungsgegenstände oder auch vertrauliche Informationen zurückgefordert werden. Ein dokumentiertes Verfahren ist erforderlich.	✔	✔	✔
7.7.6	Die Käuferinformation muss geschützt werden: Löschen Sie den Zugang zu physischen oder elektronischen Systemen die Käuferinformation beinhaltet (Bestands-oder Zeitplan). Die Verfahrensweise muss dokumentiert sein.	✔	✔	✔
7.7.7	Eine Checkliste der Beschäftigten zur Überprüfung ist vorhanden.	✔	✔	✔
7.7.8	Wiedereinstellung: Es sind Verfahren vorhanden die verhindern, dass der LSP / Antragsteller Mitarbeiter wiedereinstellt, obwohl die Ablehnungs- / Kündigungskriterien noch gültig sind. Hinweis: Die Aufzeichnungen werden vor der Neueinstellung überprüft (Beispiel: Hintergrund von zuvor entlassenem Personal oder abgelehnten Bewerbern (deren Einstellung bereits schon einmal abgelehnt wurde).	✔	✔	✔

8. Anforderungen an eine Zentralfunktion (gilt nur für die Multi-Site-Zertifizierung)

Kapitel	Zentralfunktion	A	B	C
8.1	**Allgemein**			
8.1.1	Es gibt eine Zentralfunktion zur Verwaltung des Sicherheitsmanagementsystems für alle Standorte, die im Rahmen der Multi-Site-Zertifizierung festgelegt sind.	✔	✔	✔
8.1.2	Alle Standorte haben ein rechtliches oder vertragliches Verhältnis zur Zentralfunktion.	✔	✔	✔
8.1.3	Ein einziges Sicherheitsmanagementsystem ist eingeführt um sicherzustellen, dass alle Standorte innerhalb des Systems die Anforderungen des geltenden TAPA-Sicherheitsstandards erfüllen.	✔	✔	✔
8.1.4	Die Zentralfunktion und ihr Managementsystem werden internen Audits unterzogen, um die fortdauernde Einhaltung der TAPA-Standards sicherzustellen.	✔	✔	✔
8.1.5	Die Zentralfunktion führt Audits an den verschiedenen Standorten durch, um das Vertrauen und die Sicherheit zu gewährleisten, dass das Sicherheitsmanagementsystem an allen Standorten innerhalb des Systems die Anforderungen der geltenden Norm erfüllt und in der Lage ist, die beabsichtigten Ergebnisse für alle beteiligten Standorte zu erzielen. Die Audits müssen mit den entsprechenden TAPA-Auditvorlagen durchgeführt werden.	✔	✔	✔
8.1.6	Die Zentralfunktion hat die Befugnis und das Recht, von allen Standorten die Einhaltung der TAPA-Sicherheitsstandards zu verlangen und erforderlichenfalls Korrektur- und Vorbeugungsmaßnahmen zu ergreifen. *Hinweis: Gegebenenfalls sollte dies in der formellen Vereinbarung zwischen der zentralen Funktion und den Standorten festgelegt werden.*	✔	✔	✔
8.2	**Richtlinien und Verfahren**			
8.2.1	Die Zentralfunktion pflegt die dokumentierten Richtlinien und Verfahren für ihre Sicherheitsmanagementsysteme, die für alle ihre Standorte gelten.	✔	✔	✔
8.2.2	Die Zentralfunktion stellt sicher, dass die entsprechenden Richtlinien und Verfahren von allen Standorten wenn erforderlich aktualisiert, kommuniziert, bereitgestellt und angewandt werden.	✔	✔	✔
8.2.3	Die Richtlinien und Verfahren müssen aufrechterhalten werden und sind erforderlichenfalls für alle Standorte leicht zugänglich.	✔	✔	✔
8.3	**Selbstbewertungsprüfungsbericht für alle Standorte durchführen**			
8.3.1	Die Zentralfunktion beauftragt alle Standorte mit der Durchführung der Selbstbewertung und alle Selbstbewertungsberichte sind der Zentralfunktion zur Registrierung und Überprüfung vorzulegen.	✔	✔	✔
8.3.2	Die Zentralfunktion stellt sicher, dass alle SCARs aus der Selbstbewertung und den Audits angemessen geschlossen werden, um ihre Sicherheitsmanagementsysteme zu verbessern.	✔	✔	✔
8.3.3	Alle Standorte müssen der zentralen Funktion Fortschrittsberichte und Berichte über alle ausstehenden SCARs vorlegen. Die Zentralfunktion leitet an die Geschäftsführung des LSP / Antragstellers weiter, wenn die SCARs nicht vor dem Fälligkeitsdatum abgeschlossen werden.	✔	✔	✔
8.4	**Aufzeichnungen über Kontrollen, Protokolle (Besucherprotokolle, Fahrerprotokoll), 7-Punkte-Inspektionen**			
8.4.1	Die Zentralfunktion muss über Verfahren verfügen um sicherzustellen, dass an allen Standorten Aufzeichnungen über Kontrollen, Besucherprotokolle, Fahrerprotokolle und 7-Punkte-Inspektionen usw. geführt werden.	✔	✔	✔
8.5	**Risikobewertungen für alle Standorte**			

Kapitel	Zentralfunktion	A	B	C
8.5.1	Die Zentralfunktion muss über Verfahren verfügen um sicherzustellen, dass an allen Standorten angemessene Risikobewertungen und -managements durchgeführt werden. Diese Aufzeichnungen werden gepflegt.	✔	✔	✔
8.6	**Videokameraüberwachung und Alarmgestaltung der Standorte**			
8.6.1	Die Zentralfunktion muss über Verfahren verfügen die sicherstellen, dass alle Standorte Dokumente zu allen physischen Sicherheitssystemen, wie Videoüberwachung und Alarmgestaltung, überprüfen und pflegen.	✔	✔	✔
8.7	**Alarm- und Zugangskontrollaufzeichnungen**			
8.7.1	Die zentrale Funktion muss über Verfahren verfügen die sicherstellen, dass alle Alarm- und Zugangskontrollsysteme gewartet und getestet werden, um ihre Betriebsbereitschaft sicherzustellen.	✔	✔	✔
8.7.2	Die zentrale Funktion muss über Verfahren verfügen die sicherstellen, dass alle Standorte Aufzeichnungen über alle Tests zur Erkennung von Einbrüchen und der Zugangskontrollen sowie Vorfälle führen.	✔	✔	✔
8.8	**Schulungsaufzeichnungen**			
8.8.1	Die zentrale Funktion muss über Verfahren verfügen um sicherzustellen, dass an allen Standorten ordnungsgemäße Schulungsunterlagen über die Sicherheitsmanagementschulungen ihrer Mitarbeiter geführt werden.	✔	✔	✔
8.8.2	Die zentrale Funktion muss über Verfahren verfügen um sicherzustellen, dass alle Standorte Aufzeichnungen über Sicherheitsschulungen aller Mitarbeiter des Standortes führen.	✔	✔	✔
8.9	**Aufzeichnungen über Sicherheitsüberprüfungen**			
8.9.1	Die zentrale Funktion muss über Verfahren verfügen um sicherzustellen, dass alle Standorte in regelmäßigen Abständen die Aufzeichnungen überprüfen, um die Integrität und Wirksamkeit der Sicherheitsmanagementsysteme sicherzustellen.	✔	✔	✔
8.9.2	Die zentrale Funktion muss über Verfahren verfügen um sicherzustellen, dass Aufzeichnungen über Überprüfungen einschließlich ihrer Ergebnisse und Korrektur- / Vorbeugungsmaßnahmen geführt werden.	✔	✔	✔
8.10	**Managementbewertungen zur Auswertung von Selbstaudits; SCARs; Verluste und Diebstähle; Risikobewertung.**			
8.10.1	Die zentrale Funktion führt regelmäßige Managementbewertungen durch, um die Einhaltung, Wirksamkeit und Verbesserung ihrer Sicherheitsmanagementsysteme sicherzustellen.	✔	✔	✔
8.10.2	Die Managementbewertungen umfassen, unter anderem, die Wirksamkeit von Selbstaudits, Schließungen von SCAR's, Risikobewertungen, Vorfälle und Verbesserungsmaßnahmen.	✔	✔	✔
8.10.3	Die zentrale Funktion führt Aufzeichnungen über alle Managementbewertungen.	✔	✔	✔

9.0. IT- und Internet(Cyber)sicherheitsbedrohung - Erweiterte Option

FSR enthält optionale Verbesserungen der Cybersicherheitsbedrohung, die als höheres Schutzniveau erachtet werden und zusätzlich zu den Modulen verwendet werden können. Diese optionale Erweiterung soll vom LSP / Antragsteller und / oder seinem Käufer als zusätzliche Anforderungen für seine betrieblichen Sicherheitsanforderungen ausgewählt werden. Wenn diese optionale Erweiterung in der Bewertung vor der Zertifizierung als Teil des Zertifizierungsaudits ausgewählt wird, sind alle Anforderungen zwingend erforderlich.

Kapitel	IT- und Cybersicherheitsbedrohung – Erweiterte Option
9.	***Zwingend erforderliche Anforderungen***
9.1	Der LSP / Antragsteller muss über Sicherheitsrichtlinien für IT- und Cyber-Bedrohungen verfügen. Die Richtlinien können separat oder in einem kombinierten Dokument vorliegen. Die Richtlinien müssen erklären: - 1. Die Maßnahmen des LSP / Antragstellers zur Identifizierung und Reaktion auf Bedrohungen. 2. Die Richtlinien und Verfahren zum Schutz, Erkennen, Testen und Reagieren auf Sicherheitsereignisse. 3. Die Methoden zur Wiederherstellung von IT-Systemen und / oder Daten. 4. Das Kommunikationsprotokoll an Käufer / Kunden, um die Auswirkungen auf die Lieferkette innerhalb von 24 Stunden nach Kenntnis des Vorfalls zu verringern. 5. Wie die Richtlinien jährlich überprüft und soweit erforderlich aktualisiert werden.
9.2	Der LSP / Antragsteller muss allen Mitarbeitern eine Informationsbewusstseinsschulung anbieten. Diese Schulung muss: - 1. Abdecken der Rollen und Verantwortlichkeiten, die Computernutzer haben in der Aufrechterhaltung der Sicherheit und dem daraus entstehenden Nutzen 2. Es existiert ein System das sicherstellt, dass Aufzeichnungen über Personen, die eine Schulung erhalten haben, gepflegt und mindestens 2 Jahre lang aufbewahrt werden.
9.3	Der LSP / Antragsteller muss über eine schriftliche Richtlinie verfügen um sicherzustellen, dass Cybersicherheitsmaßnahmen mit Subunternehmern und / oder Lieferanten getroffen werden, die Folgendes sicherstellen: 1. Die Cyber-Sicherheitsanforderungen des LSP / Antragsteller werden den Subunternehmern und / oder Lieferanten bekannt gegeben und in den Vereinbarungen mit eingeschlossen. 2. Wenn Subunternehmer und / oder Lieferanten die Cyber-Sicherheitsanforderungen des LSP / Antragsteller nicht anerkennen oder ablehnen, werden Maßnahmen dokumentiert und sind vorhanden, die die Risiken für die Cyber-Sicherheitsanforderungen des LSP / Antragsteller und deren Kunden minimieren.
9.4	Der LSP / Antragsteller muss über einen Plan für Maßnahmen zur Schadensminimierung bei einer Stromunterbrechung verfügen (z. B. eine alternative Stromversorgung oder ein Notstromaggregat) der sicherstellt, dass maßgebliche IT-Systeme (in der örtlichen Risikobewertung aufgeführt) mindestens 48 Stunden lang mit Strom versorgt werden.
9.5	In den IT-Systemen des LSP / Antragsteller muss lizenzierte Antiviren- und Anti-Malware-Software installiert sein. Die Antiviren- und Anti-Malware-Software müssen die neuesten Updates enthalten.
9.6	LSP / Antragsteller muss über einen geeigneten Notfallplan (IT Disaster Recovery Plan) für die Wiederherstellung eines gehackten Systems, einschließlich, aber nicht beschränkt auf, alle erforderlichen Vorkehrungen für die Sicherung und Wiederherstellung von Daten und Software verfügen.
9.7	Die IT-Systeme des LSP / Antragsteller müssen gesichert werden. Solche Sicherungen müssen regelmäßig getestet werden. Die Sicherungsdaten müssen verschlüsselt und an einen zweiten, externen Standort übertragen werden.

Kapitel	IT- und Cybersicherheitsbedrohung – Erweiterte Option
9.8	LSP / Antragsteller muss eine Richtlinie für alle Benutzerkonten implementieren, um den Zugriff auf Informationssysteme mithilfe eindeutiger persönlichen Kennungen und sicherer Passwörter zu verwalten und zu steuern. Folgende Verfahren zur Sicherstellung sind vorhanden: 1. Ein Programm zur Prüfung der Kennwortkonformität ist vorhanden. 2. Zum Zeitpunkt der Erstellung muss jedem neuen Konto ein eindeutiges Kennwort zugewiesen werden. 3. Anfangskennwörter dürfen weder den Namen noch die Identifikationsnummer des Benutzers enthalten oder auf andere Weise einem Standardmuster, basierend auf Benutzerinformationen, folgen. 4. Passwörter werden den Benutzern auf sichere Weise und erst nach Überprüfung der Identität des Benutzers mitgeteilt. 5. Die Benutzer müssen aufgefordert werden, die Kennwörter bei der ersten Anmeldung zu ändern. 6. Passwörter müssen mindestens alle 90 Tage geändert werden.

Publikationsgeschichte der Originalversion (in englischer Sprache)

Erstveröffentlichung im Januar 2020

Erste (aktuelle) Ausgabe im Januar 2020 veröffentlicht

Diese öffentlich zugängliche Spezifikation tritt am 1. Juli 2020 in Kraft