



FSR 2026

TAPA Global Standard



TAPA Americas

1353 Riverstone Pkwy,
Ste 120-320
Canton, GA 30114 USA

www.tapaonline.org

TAPA Asia Pacific

10 Anson Rd, #33-15
International Plaza,
Singapore 079903

www.tapa-apac.org

TAPA EMEA

Kanaalpark 140
2321 JV Leiden
The Netherlands

www.tapaemea.org

1.0	Einführung	4
1.1	Zweck dieses FSR-Dokuments	4
1.2	Ressourcen zur Umsetzung der TAPA FSR	4
1.3	Schutz der Richtlinien und Verfahren der LSP	4
2.0	Über TAPA.....	5
2.1	Zweck von TAPA	5
2.2	TAPA's Mission	5
3.0	TAPA Standards	6
3.1	TAPA Sicherheitsstandards	6
3.2	Implementierung	6
4.0	Rechtliche Beratung.....	7
4.1	Umfang	7
4.2	Übersetzung	7
4.3	Die Marke "TAPA"	7
4.4	Haftungsbeschränkungen	7
5.0	Verträge und Unteraufträge	8
5.1	Verträge.....	8
5.2	Untervergabe	8
5.3	TAPA-Beschwerdeuntersuchung und -beilegung	8
6.0	Ausnahmegenehmigungen.....	9
7.0	Sicherheitsanforderungen für Einrichtungen	10
S1.	Allgemeine Anforderungen	10
S2.	Perimeter.....	12
2.1	Lager für externe Frachtabfertigung, Versand und Warenannahme	12
2.2	Physische Barrieren	12
2.3	Externe Rampenbereiche.....	13
2.4	Zugang für Privatfahrzeuge.....	14
S3.	Außenwände, Dach und Türen.....	15
3.1	Außenbereiche der Anlage: CCTV/VSS	15
3.2	Außenwände und Dach.....	15
S4.	Ein- und Ausgänge für Büro und Lager.....	18
4.1	Besuchereingang im Bürobereich	18
4.2	Eingang für Mitarbeiter	19
4.3	Fahrer- und Fahrzeugidentifizierung	19
S5.	Innenbereich Lager und Büro	21
5.1	Lagerbereich: Zwischenwände bei mehreren Mietern	21
5.2	Innere Lagerbereiche	21

5.3	Innere Rampentore und Rampenbereiche	22
5.4	Zugangskontrolle zwischen Büro und Rampe/Lager	22
5.5	Bereich für hochwertige Fracht (HVC)	23
5.6	Müllinspektion aus dem Lager	24
5.7	Vorverladung und Bereitstellung	24
5.8	Personenkontrollen und Ausgangskontrollen	25
5.9	Kontrolle der Frachtumschlaggeräte	25
5.10	Integrität des Containers oder Aufliegers: 7-Punkte-Inspektion	26
5.11	Frachtübergabeprozess; Plomben	26
5.12	Ladungsintegrität; Validierungsprozess für Be- und Entladung	27
5.13	Betrügerische Abholungen	27
S6.	Sicherheitssysteme: Gestaltung, Monitoring und Reaktion	28
6.1	Monitoring Zentrale	28
6.2	Einbrucherkennungssystem (IDS Intruder Detection System)	28
6.3	Automatisches Zutrittskontrollsystem (AACS Automatic Access Control System)	29
6.4	CCTV / Videoüberwachung (VSS)	30
6.5	Außen- und Innenbeleuchtung	31
S7.	Training und Prozeduren	32
7.1	Eskalationsverfahren	32
7.2	Managementverpflichtung	32
7.3	Schulungen	32
7.4	Zugang zu den Vermögenswerten des Käufers	33
7.5	Informationskontrolle	33
7.6	Meldung von Sicherheitsvorfällen	33
7.7	Wartungsprogramme	34
7.8	Verantwortung Auftragnehmer	34
7.9	Versand- und Empfangsaufzeichnungen	34
7.10	Avisierungsprozess	35
S8.	Integrität der Belegschaft	36
8.1	Überprüfung/Hintergrundprüfung (soweit nach lokalem Recht zulässig)	36
8.2	Kündigung oder Wiedereinstellung von Arbeitskräften	36
S9.	Zentrale Anforderungen (gültig für Zertifizierung mehrerer Standorte)	38
9.1	Allgemein	38
9.2	Richtlinien und Verfahren	39
9.3	Bericht zur Selbstbewertung für alle Standorte	39
9.4	Inspektionsberichte, Protokolle (Besucher-/Fahrerprotokolle), 7-Punkte-Inspektionen	40
9.5	Risikobewertung aller Standorte	40
9.6	CCTV-/VSS- und Alarmanlagenplan des Geländes	40
9.7	Protokolle zu Alarm- und Zutrittskontrolle	40
9.8	Schulungsunterlagen	41
9.9	Screening-/Überprüfungsakten	41
9.10	Managementbewertung zur Auswertung der Selbstprüfungen; festgestellte SCARs; etwaige Verluste, Diebstähle; Risikobewertungen	41
8.0	IT- und Cybersicherheitsbedrohung – Erweiterte Option	43
E8.	Obligatorische Anforderungen	43

1.0 Einführung

1.1 Zweck dieses FSR-Dokuments

Dieses Dokument zu den Sicherheitsanforderungen für Lagerstätten (Facility Security Requirements, FSR) ist der offizielle TAPA-Standard für sichere Lagerhaltung. Es handelt sich um einen weltweit anerkannten Standard, der in Geschäfts- und Sicherheitsvereinbarungen zwischen Käufern und Logistikdienstleistern (LSPs) bzw. anderen Zertifizierungsbewerbern Anwendung finden kann.

Bei der Entwicklung dieses Standards berücksichtigte TAPA die vielfältigen Unterschiede in der Bereitstellung von Lagerdienstleistungen auf globaler, regionaler und unternehmensinterner Ebene. Der FSR kann daher für alle oder einen Teil der von einem LSP/Bewerber erbrachten Dienstleistungen gelten. Je nach Komplexität und Größe der Lieferkette kann die Einhaltung der TAPA-Standards durch einen einzelnen LSP/Bewerber oder durch mehrere LSPs/Bewerber und qualifizierte Subunternehmer erreicht werden.

Umfang

TAPA bietet drei Optionen zur Unterstützung der Zertifizierung an:

- Zertifizierung eines einzelnen Standorts durch eine unabhängige Prüfstelle (IAB).
- Zertifizierung mehrerer Standorte durch eine IAB.
- Selbstprüfung durch autorisierte Auditoren (AA) des LSP/Antragstellers oder der IAB (die eine Selbstprüfung im Auftrag des LSP/Antragstellers durchführt).

Zielgruppe

Zu den typischen Nutzern der TAPA-Standards gehören:

- Einkäufer
- Logistikdienstleister/Antragsteller
- Strafverfolgungsbehörden oder andere Regierungsbehörden
- Professionelle Lieferkettenorganisationen
- Versicherer

1.2 Ressourcen zur Umsetzung der TAPA FSR

Die Ressourcen zur Erfüllung der Anforderungen der FSR liegen in der Verantwortung des LSP/Antragstellers und werden auf dessen eigene Kosten bereitgestellt, sofern nicht zwischen Käufer und LSP/Antragsteller etwas anderes ausgehandelt oder vereinbart wurde.

1.3 Schutz der Richtlinien und Verfahren der LSP

Kopien von Dokumenten zu Sicherheitsrichtlinien und -verfahren werden dem Käufer nur gemäß den zwischen LSP/Antragsteller und Käufer unterzeichneten Offenlegungsvereinbarungen übermittelt und sind als vertrauliche Informationen zu behandeln.

2.0 Über TAPA

2.1 Zweck von TAPA

Frachtdiebstahl stellt eine der größten Herausforderungen für Hersteller wertvoller und risikoreicher Produkte sowie deren Logistikdienstleister dar.

Die Bedrohung geht längst nicht mehr nur von Gelegenheitstätern aus. Organisierte Verbrecherbanden operieren heute weltweit und setzen immer raffiniertere Angriffe auf Fahrzeuge, Gebäude und Personal ein, um ihre Ziele zu erreichen. TAPA ist ein einzigartiges Forum, das globale Hersteller, Logistikdienstleister, Spediteure, Strafverfolgungsbehörden und weitere Akteure mit dem gemeinsamen Ziel vereint, Verluste in internationalen Lieferketten zu reduzieren. Der Schwerpunkt von TAPA liegt auf Diebstahlprävention durch Echtzeitinformationen und modernste Präventionsmaßnahmen.

2.2 TAPA's Mission

Die Mission von TAPA ist es, die Vermögenswerte ihrer Mitglieder durch die Minimierung von Frachtverlusten in der Lieferkette zu schützen. Dies erreicht TAPA durch die Entwicklung und Anwendung globaler Sicherheitsstandards, anerkannter Branchenpraktiken, Technologien, Schulungen, Benchmarking, Zusammenarbeit mit Regulierungsbehörden und die proaktive Identifizierung von Kriminalitätstrends und Bedrohungen der Lieferkettensicherheit.

3.0 TAPA Standards

3.1 TAPA Sicherheitsstandards

Die folgenden globalen TAPA-Sicherheitsstandards wurden entwickelt, um den sicheren Transport und die Lagerung von wertvollen, diebstahlgefährdeten Gütern zu gewährleisten:

- Die Anforderungen an die Standortsicherheit (FSR) stellen Mindeststandards speziell für die sichere Lagerung von Waren, auch transportbedingte Zwischen-Lagerung, innerhalb einer Lieferkette dar.
- Die Anforderungen an die Lkw-Sicherheit (TSR) konzentrieren sich ausschließlich auf den Lkw-Transport und stellen Mindeststandards speziell für den Straßentransport von Produkten innerhalb einer Lieferkette dar.
- Die Cybersicherheitsstandards (CSS) bieten Unternehmen ein Instrument, um die Mindestanforderungen an das IT-Management in ihren Lieferkettenabläufen zu verstehen und digitale Anlagen vor Cyberangriffen und Betriebsstörungen zu schützen.

Die globalen TAPA-Sicherheitsstandards werden alle drei Jahre überprüft und bei Bedarf überarbeitet.

Dieses Dokument behandelt ausschließlich die FSR-Anforderungen!

- Der Zertifizierungsprozess für TAPA FSR ist im TAPA FSR Certification Framework-Dokument beschrieben.
- Sowohl die aktuelle Fassung des TAPA FSR-Dokuments als auch des TAPA FSR Certification Framework-Dokument müssen eingehalten werden, um den TAPA FSR Zertifizierungsstatus zu erreichen.

3.2 Implementierung

Die erfolgreiche Umsetzung der TAPA-Sicherheitsstandards hängt von der Zusammenarbeit zwischen Logistikdienstleistern/Antragstellern, Einkäufern (Eigentümern der Fracht) und von TAPA autorisierten Prüfern ab.

4.0 Rechtliche Beratung

4.1 Umfang

Der FSR ist ein globaler Standard, und alle Abschnitte des Standards sind obligatorisch, es sei denn, eine Ausnahme wird im Rahmen des offiziellen Ausnahmegenehmigungsverfahrens gewährt (siehe Abschnitt 6 des FSR-Standards und Abschnitt 7 des FSR-Zertifizierungsrahmendokuments).

4.2 Übersetzung

In geografischen Gebieten, in denen Englisch nicht die Muttersprache ist und in denen eine Übersetzung notwendig und angebracht ist, liegt es in der Verantwortung des LSP/Antragstellers und seiner Beauftragten, sicherzustellen, dass jede Übersetzung des FSR oder eines seiner Teile die Absichten von TAPA bei der Entwicklung und Veröffentlichung dieser Standards genau widerspiegelt.

4.3 Die Marke "TAPA"

"TAPA" ist eine eingetragene Marke der Transported Asset Protection Association und darf ohne die ausdrückliche schriftliche Genehmigung von TAPA über deren offiziell anerkannte Regionalverbände nicht verwendet werden. Die TAPA-Standards und zugehörigen Materialien werden von TAPA veröffentlicht und dürfen ohne die ausdrückliche schriftliche Genehmigung von TAPA von keinem Beteiligten überarbeitet, bearbeitet oder geändert werden. Missbrauch der Marke TAPA kann zum Entzug der Zertifizierung oder zu rechtlichen Schritten führen.

4.4 Haftungsbeschränkungen

Mit der Veröffentlichung dieser Standards übernimmt TAPA keine Garantie dafür, dass alle Ladungsdiebstähle verhindert werden können, unabhängig davon, ob die Standards vollständig und ordnungsgemäß umgesetzt werden. Jegliche Haftung, die sich aus einem Diebstahl von Lagergut oder einem anderen Verlust von Lagergut gemäß den FSR-Standards ergibt, liegt beim Logistikdienstleister/Antragsteller und/oder Käufer gemäß den Vertragsbedingungen und den geltenden Gesetzen und Bestimmungen des jeweiligen Gerichtsstands.

5.0 Verträge und Unteraufträge

5.1 Verträge

Die sichere Beförderung, Lagerung und Handhabung der Vermögenswerte des Käufers obliegt dem Logistikdienstleister/Antragsteller, seinen Beauftragten und Subunternehmern während der gesamten Abwicklung – von der Abholung über den Transport und die Lagerung bis hin zur Auslieferung – wie in einer Freigabeerklärung oder einem Vertrag festgelegt.

Sofern die Sicherheitsrichtlinien (FSR) im Vertrag zwischen dem Logistikdienstleister/Antragsteller und dem Käufer erwähnt oder aufgeführt sind, müssen sie auch im Sicherheitsprogramm des Logistikdienstleisters/Antragstellers aufgeführt werden.

Der Logistikdienstleister legt dem Käufer einen Nachweis über die Zertifizierung nach den Sicherheitsrichtlinien (FSR) und gegebenenfalls einen Nachweis über die Einhaltung der Anforderungen vor. Jegliche behauptete Nichterfüllung der Anforderungen nach den Sicherheitsrichtlinien (FSR) durch den Logistikdienstleister/Antragsteller wird gemäß den Bestimmungen des zwischen dem Käufer und dem Logistikdienstleister/Antragsteller ausgehandelten Vertrags geregelt.

5.2 Untervergabe

Bei der Beauftragung von Subunternehmern muss vertraglich festgelegt sein, dass diese alle genannten FSR-Anforderungen erfüllen. Die internen, autorisierten Prüfer des LSP müssen bestätigen, dass der Subunternehmer die FSR-Anforderungen auf gleichem Niveau erfüllt.

5.3 TAPA-Beschwerdeuntersuchung und -beilegung

Geht bei TAPA eine formelle Beschwerde über die Leistung eines zertifizierten LSP/Antragstellers ein, kann TAPA (vorbehaltlich der Überprüfung) verlangen, dass der LSP/Antragsteller auf eigene Kosten eine erneute Prüfung in Auftrag gibt. Besteht der LSP/Antragsteller die Prüfung nicht oder verweigert er die Einhaltung des Verfahrens, kann ihm die Zertifizierung entzogen werden.

6.0 Ausnahmegenehmigungen

Eine Ausnahmegenehmigung ist eine schriftliche Genehmigung, die eine Einrichtung von einer bestimmten TAPA-Anforderung befreit und die Akzeptanz einer alternativen Lösung zur Einhaltung der Vorschriften ermöglicht. Eine Ausnahmegenehmigung kann beantragt werden, wenn ein LSP/Antragsteller eine bestimmte Anforderung der FSR nicht erfüllen kann und alternative Maßnahmen begründen kann. Ausnahmegenehmigungen gelten für den Zeitraum der Zertifizierung.

TAPA Copyright © Do Not Copy

7.0 Sicherheitsanforderungen für Einrichtungen

S1. Allgemeine Anforderungen

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
1.1.1	Alle in diesem Standard vorgeschriebenen Verfahren und Richtlinien müssen dokumentiert und mindestens alle zwei Jahre aktualisiert werden.	Ⓐ	Ⓑ	Ⓒ
1.1.2	Die Geschäftsleitung muss formell eine Person (AA) für die Sicherheit vor Ort ernennen, die für die Einhaltung der TAPA FSR-Vorgaben, den Abschluss von SCARS, die Risikobewertung, den Managementbericht und die Sicherheitsanforderungen der Lieferkette des Unternehmens verantwortlich ist. Eine weitere Person (möglicherweise dieselbe) ist ebenfalls für die Überwachung des FSR-Programms zuständig. Dies umfasst die Planung von Compliance-Prüfungen, die Kommunikation mit den Sicherheitsbeauftragten, die Rezertifizierung, Änderungen des FSR-Standards usw. Diese Personen können Mitarbeiter oder externe Dienstleister sein, die im Rahmen eines Vertrags mit der Wahrnehmung dieser Aufgaben betraut sind.	Ⓐ	Ⓑ	Ⓒ
1.1.3	Interne Audits (durch ein funktionsübergreifendes Team) des Sicherheitsmanagementsystems, Selbstbewertungsberichte des internen Sicherheitsbeauftragten und der Abschluss des SCARS-Verfahrens müssen abgeschlossen und dokumentiert werden.	Ⓐ	Ⓑ	Ⓒ
1.1.4	Für physische Schlösser, Zugangskarten und/oder Schlüssel, die die physischen und elektronischen Schlüssel verwalten und kontrollieren, ist ein Verfahren, ein Protokoll und/oder ein Schlüsselplan erforderlich. Das Verfahren sollte Prozesse für die Duplizierung, die Aufbewahrung und den Umgang mit fehlenden/verlorenen Schlüsseln umfassen.	Ⓐ	Ⓑ	Ⓒ

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
1.1.5	Eine dokumentierte Risikoanalyse, die die Wahrscheinlichkeit und die Auswirkungen sicherheitsrelevanter Bedrohungen berücksichtigt, muss mindestens jährlich durchgeführt und aktualisiert werden. Das Management muss überprüfen und bestätigen, dass die identifizierten Risiken bewertet und geeignete Kontrollmaßnahmen zur Minderung oder Beseitigung der Risiken auf ein akzeptables Maß implementiert wurden. Mindestens die folgenden häufigen internen/externen Ereignisse müssen bewertet werden: Diebstahl von Fracht oder Informationen, unbefugter Zutritt zu Einrichtungen oder Fracht, Manipulation/Zerstörung von Sicherheitssystemen, fingierte Frachtabholungen, Aufrechterhaltung der Sicherheit bei Personalmangel oder Naturkatastrophen, Bedarf an Rammschutzbarrieren für ebenerdig zugängliche Fenster oder Laderampentore usw. Weitere Bedrohungen können auf Grundlage lokaler/nationaler Risiken berücksichtigt werden.	Ⓐ	Ⓑ	Ⓒ
1.1.6	Die Person, die interne oder jährliche Audits für den Antragsteller/LSP durchführt (im Folgenden LSP-AA genannt), muss geschult sein. Diese Person kann dieselbe sein wie unter Punkt 1.1.2 erwähnt oder ein externer Dienstleister, der vertraglich mit dieser Aufgabe betraut ist.	Ⓐ	Ⓑ	Ⓒ
1.1.7	Um den FSR zu verstehen und alle seine Anforderungen umsetzen zu können, müssen alle Antragsteller/LSP AAs die entsprechende Prüfung für den TAPA-Standard und die Version, nach der sie auditieren sollen, abgelegt und bestanden haben.	Ⓐ	Ⓑ	Ⓒ

S2. Perimeter

2.1 Lager für externe Frachtabfertigung, Versand und Warenannahme

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
2.1.1	CCTV (Closed-Circuit Television)/VSS (Video Surveillance System) zur Überwachung des gesamten Verkehrs auf dem äußeren Güterumschlags-, Versand- und Empfangsgelände (einschließlich Ein- und Ausfahrtpunkte), um sicherzustellen, dass alle Fahrzeuge und Personen jederzeit erkennbar sind, es sei denn, es kommt zu einer vorübergehenden Behinderung aufgrund betrieblicher Erfordernisse (z.B. Be- und Entladen von Lkw in Echtzeit).	Ⓐ	Ⓑ	
2.1.2	Adäquate Beleuchtung in Lade- und Entladebereichen sollte als grundlegende Abschreckung gegen Kriminalität dienen und die Möglichkeit bieten, die Abläufe in diesen Bereichen während der Nacht zu überwachen. <i>Hinweis: Die Beleuchtung kann dauerhaft sein oder durch Alarm, Bewegung, Geräuscherkennung usw. aktiviert werden, wobei eine sofortige Ausleuchtung gewährleistet sein muss.</i>	Ⓐ	Ⓑ	Ⓒ
2.1.3	Es muss ein Verfahren vorliegen, das den Umgang mit unbefugten Fahrzeugen und Personen auf dem äußeren Güterumschlags-, Versand- und Empfangsgelände regelt. Die relevanten Mitarbeiter, einschließlich der Wachleute, müssen über dieses Verfahren informiert werden.	Ⓐ	Ⓑ	Ⓒ
2.1.4	Die Frachtabfertigung, der Versand und der Empfangsbereich müssen angemessen kontrolliert werden, um unbefugten Zutritt zu verhindern.		Ⓑ	Ⓒ
2.1.5	Bei ebenerdigen, zugänglichen Fenstern oder Laderampentoren muss die jährliche Risikobewertung den Bedarf an Einbruchschutzvorrichtungen prüfen. Zusätzlich sollte die Verwendung von Fensterabdeckungen zum Schutz vor unbefugter Einsicht in die Innenräume bewertet werden (siehe Risikobewertung, Anforderung 1.1.5).	Ⓐ		

2.2 Physische Barrieren

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
2.2.1	Eine physische Barriere umschließt den Bereich für Güterumschlag, Versand und Warenannahme.	Ⓐ		

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
2.2.2	Die physische Barriere um den Güterumschlag-, Versand- und Empfangsbereich muss mindestens 1,8 Meter hoch sein. Hinweis: Die physische Barriere, die unbefugten Zutritt verhindern soll, muss über ihre gesamte Länge, einschließlich tiefer gelegener Bereiche, eine Höhe von 1,8 Metern aufweisen.	Ⓐ		
2.2.3	Die physische Barriere um den Güterumschlag-, Verschiffungs- und Empfangsbereich wird in gutem Zustand gehalten.	Ⓐ		
2.2.4	Die Tore innerhalb des Güterumschlags-, Versand- und Empfangsbereichs sind entweder bemannt oder elektronisch gesteuert.	Ⓐ		
2.2.5	Die physische Barriere um den Güterumschlag-, Versand- und Empfangsbereich wird mindestens wöchentlich auf Unversehrtheit und Beschädigungen überprüft.	Ⓐ		

2.3 Externe Rampenbereiche

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
2.3.1	Die Außenbereiche der Rampen werden durch farbige oder „Tag/Nacht“-Außenkameras (CCTV/VSS) überwacht.	Ⓐ	Ⓑ	Ⓒ
2.3.2	CCTV-/VSS-Kameras sind so montiert, dass sie alle Vorgänge und Bewegungen im Außenbereich der Rampen jederzeit überwachen können, es sei denn, es kommt aufgrund betrieblicher Erfordernisse (z.B. Be- und Entladen von Lkw in Echtzeit) zu vorübergehenden Behinderungen.	Ⓐ	Ⓑ	Ⓒ
2.3.3	Alle Fahrzeuge und Personen im Außenbereich der Rampen müssen mit CCTV-/VSS-Kameras überwacht werden, die die Fahrzeugidentifikation deutlich anzeigen und die Gesichtsmerkmale des Personals erkennen können.	Ⓐ		
2.3.4	Fahrzeuge und Personen im Außenbereich der Rampen müssen in mindestens 75 % der Fälle innerhalb eines Tages von Überwachungskameras (CCTV/VSS) erfasst und sichtbar sein.		Ⓑ	Ⓒ

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
2.3.5	Alle Außenbereiche rund um die Rampentore sind vollständig beleuchtet.	Ⓐ	Ⓑ	Ⓒ

2.4 Zugang für Privatfahrzeuge

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
2.4.1	Privatfahrzeuge dürfen nur dann in die Bereiche für Frachtabfertigung, Versand und Warenannahme, wenn dies vorher genehmigt wurde und in einer dokumentierten Richtlinie festgelegt ist.	Ⓐ	Ⓑ	Ⓒ
2.4.2	Innerhalb von 25 m Fußweg zu den Außenrampenbereichen gibt es keine privaten Parkplätze.	Ⓐ	Ⓑ	Ⓒ

S3. Außenwände, Dach und Türen

3.1 Außenbereiche der Anlage: CCTV/VSS

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
3.1.1	Farbige oder „Tag/Nacht“-Außenkameras (CCTV/VSS) sind installiert, die alle Außenseiten des Gebäudes erfassen.	Ⓐ		
3.1.2	Ein Farb- oder „Tag/Nacht“-Außenkamerasystem (CCTV/VSS) ist installiert, das die Außenseiten des Gebäudes mit Türen, Fenstern und anderen Öffnungen erfasst.		Ⓑ	
3.1.3	Alle Sichtfelder des externen CCTV/VSS-Kamerasystems sind jederzeit frei, es sei denn, es kommt aufgrund betrieblicher Erfordernisse (z.B. Be- und Entladen von LKW in Echtzeit) zu vorübergehenden Sichtbehinderungen.	Ⓐ		
3.1.4	Alle Fahrzeuge und Personen im Außenbereich der Anlage werden von CCTV-/VSS-Kameras erfasst, die die Fahrzeugidentifikation deutlich anzeigen und die Gesichtsmerkmale des Personals erkennen können.	Ⓐ		
3.1.5	Fahrzeuge und Personen sind auf mindestens 75 % der Aufnahmen der Außenkameras (CCTV/VSS) innerhalb eines Tages sichtbar.		Ⓑ	

3.2 Außenwände und Dach

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
3.2.1	Außenwände und Dach müssen so konstruiert und instand gehalten werden, dass sie dem Eindringen widerstehen und einen robusten physischen Schutz bieten. Die Materialien sollten ausreichende Festigkeit und Haltbarkeit aufweisen, um Versuchen eines gewaltsamen Eindringens standzuhalten. (Beispiele: Ziegel, Betonblöcke, vorgefertigte Betonpaneele oder hochfeste Sandwichpaneele mit einer Gesamtstärke von 7mm starken Innen- und Außenplatten). <i>Hinweis: Werden leichte oder nicht tragende Materialien verwendet, müssen zusätzliche Schutzmaßnahmen (wie internes Stahlgitter oder Einbruchmeldesysteme) umgesetzt werden, um ein gleichwertiges Sicherheitsniveau zu erreichen.</i>	Ⓐ	Ⓑ	Ⓒ

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
3.2.2	Alle Fenster, die geöffnet werden können, Lüftungsöffnungen oder andere Öffnungen in den Außenwänden des Gebäudes sowie alle versiegelten Fenster, die in den Außenwänden des Gebäudes unterhalb von 3 Metern / 9 Fuß 10 Zoll über dem Arbeitsboden installiert sind, müssen eine physische Barriere aufweisen oder mit einem Alarmsystem ausgestattet und an das Hauptalarmsystem angeschlossen sein.	Ⓐ	Ⓑ	
3.2.3	Alle zu öffnenden Fenster, Dachfenster, Lüftungsöffnungen, Dachluken und sonstige Dachöffnungen müssen gesichert sein durch: (a) eine stabile physische Barriere (z.B. Sicherheitsgitter, -stäbe oder verstärkte Abdeckungen) oder (b) eine in die primäre Alarmanlage des Gebäudes integrierte Einbruchmeldeanlage. <i>Hinweis: Physische Barrieren müssen so konstruiert sein, dass sie nicht entfernt oder manipuliert werden können. Alarmgesicherte Öffnungen müssen bei unbefugtem Zutritt sofort einen Alarm auslösen.</i>	Ⓐ		
3.2.4	Der Zugang zum Dach von außen (Leiter oder Treppe) muss: physisch gesichert und videoüberwacht sein (Farb- oder Tag-/Nachtkameras) oder physisch gesichert und alarmgesichert sein.	Ⓐ		
3.2.5	Der Zugang zum Dach von außen (Leiter oder Treppe) ist physisch verschlossen.		Ⓑ	Ⓒ
3.2.6	Alle äußeren Fußgängertüren des Lagers und der Büros sind mit Alarmanlagen zur Erkennung unbefugten Öffnens ausgestattet und an die Hauptalarmanlage angeschlossen. <i>Hinweis: Laderampentore fallen nicht unter diese Anforderung; siehe Anforderung 3.2.12 für die Alarmanforderungen an Laderampentore.</i>	Ⓐ	Ⓑ	Ⓒ
3.2.7	Jede Außentür des Lagers, jede Bürotür oder sonstige Öffnung der Anlage muss innerhalb des Hauptalarmsystems eindeutig pro Tür oder pro Zone gekennzeichnet sein.	Ⓐ		
3.2.8	Alle Außentüren des Lagers sind stets geschlossen und gesichert, wenn sie nicht genutzt werden. Gegebenenfalls werden Schlüssel/Codes verwendet.	Ⓐ	Ⓑ	

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
3.2.9	Außentüren und -rahmen von Lagerhallen dürfen nicht leicht zu durchbrechen sein. Außenliegende Scharniere müssen vernietet oder punktgeschweißt werden. Voll- oder Teilglastüren in Lagerhallen sind nur zulässig, wenn Glasbruchmelder installiert sind oder ein anderes lokales Detektionssystem (z.B. passive Infrarot-Sensoren) installiert ist, das direkt an die Alarmzentrale angeschlossen ist, ODER wenn das Glas durch Gitterstäbe/Netze geschützt ist. TAPA gestattet bestehenden Zertifikatsinhabern, die diese Anforderung nicht erfüllen können, ihre aktuelle Konfiguration bis zur nächsten Überarbeitung beizubehalten. Neue Zertifikatsinhaber oder neue Standorte müssen die neue Anforderung erfüllen.	Ⓐ	Ⓑ	Ⓒ
3.2.10	Notausgänge, die ausschließlich für Notfälle genutzt werden (z.B. Feuerausgänge), sind permanent mit einem individuellen oder zonenbezogenen akustischen Signalgeber ausgestattet.	Ⓐ	Ⓑ	
3.2.11	Alle Rampentore sind so robust, dass sie ein gewaltsames Eindringen mit kleinen elektrischen/batteriebetriebenen Handwerkzeugen verhindern bzw. verzögern.	Ⓐ	Ⓑ	Ⓒ
3.2.12	Laderampentore Außerhalb der Betriebszeiten: Die Laderampentore sind geschlossen und gesichert (z.B. elektronisch deaktiviert oder physisch verriegelt). Die Laderampentore sind mit einer Alarmanlage ausgestattet, die unbefugtes Eindringen erkennt und einen Alarm auslöst, der mit der Hauptalarmanlage verbunden ist. Betriebszeiten: Die Laderampentore müssen geschlossen sein, wenn sie nicht in Betrieb sind. Scherentore müssen, falls verwendet, mit einem mechanischen Schiebe-/Riegelschloss gesichert sein und eine Mindesthöhe von 2,4 Metern aufweisen.	Ⓐ	Ⓑ	Ⓒ

S4. Ein- und Ausgänge für Büro und Lager

4.1 Besuchereingang im Bürobereich

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
4.1.1	Die Besuchereingänge werden von einem Mitarbeiter/Wachmann/Empfangsmitarbeiter kontrolliert, der in Bezug auf die Ausstellung von Besucherausweisen, Kontrollen, Protokollierung, Besucher, Begleitpflichten usw. geschult wurde (Verfahren vorhanden für den Fall, dass Mitarbeiter ihre eigenen Gäste einchecken und für Besuche außerhalb der Betriebszeiten).	Ⓐ	Ⓑ	Ⓒ
4.1.2	Der/Die Besuchereingang/-punkte im Bürobereich ist/sind videoüberwacht (Farb- oder Tag/Nacht-Kameras), sodass die Personen jederzeit klar erkennbar sind.	Ⓐ	Ⓑ	
4.1.3	Ein Notrufalarm ist im Besuchereingangsbereich des Büros vorhanden und wird wöchentlich getestet.	Ⓐ	Ⓑ	
4.1.4	Alle Besucher des Bürobereichs müssen sich mit einem amtlichen Lichtbildausweis (z.B. Führerschein, Reisepass oder Personalausweis) ausweisen. Sollten digitale Ausweise von der Einrichtung akzeptiert und durch die lokale Gesetzgebung zugelassen sein, muss ein zuverlässiges Verifizierungsverfahren (einschließlich der gesamten erforderlichen technischen Infrastruktur) vorhanden sein.	Ⓐ	Ⓑ	Ⓒ
4.1.5	Alle Besucher des Bürobereichs werden registriert und die Daten mindestens 30 Tage lang protokolliert. Besuchsdetails, wie z.B. welche Person besucht wird und warum der Besuch stattfindet, müssen anhand der im Besucherprotokoll erfassten Informationen nachvollziehbar sein.	Ⓐ	Ⓑ	Ⓒ
4.1.6	Alle Besucherausweise müssen beim Verlassen des Geländes abgeglichen und das vollständige Besucherprotokoll täglich überprüft werden.	Ⓐ	Ⓑ	
4.1.7	Alle Besucher tragen gut sichtbar Ausweise oder Zutrittskarten und werden von Firmenpersonal begleitet.	Ⓐ	Ⓑ	

4.2 Eingang für Mitarbeiter

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
4.2.1	Alle Zugänge zum Betriebsgelände sind rund um die Uhr zugangskontrolliert.		Ⓑ	Ⓒ
4.2.2	Alle Zugangspunkte für die Mitarbeiter werden rund um die Uhr über ein elektronisches Zugangskontrollsystem überwacht. Die Zutritte werden protokolliert.	Ⓐ		
4.2.3	Die Eingänge für die Mitarbeiter werden durch Videoüberwachung (Farb- oder Tag/Nacht-Kameras) erfasst.	Ⓐ	Ⓑ	
4.2.4	Alle Mitarbeiter müssen nach Abschluss des Überprüfungsprozesses einen Firmenausweis mit Foto erhalten.	Ⓐ	Ⓑ	
4.2.5	Alle übrigen Mitarbeiter müssen mit einem Firmenausweis ausgestattet werden, damit sie innerhalb des Betriebsgeländes erkennbar sind.	Ⓐ	Ⓑ	
4.2.6	Alle Mitarbeiterausweise werden deutlich sichtbar angebracht.	Ⓐ	Ⓑ	
4.2.7	Mitarbeiterausweise dürfen unter keinen Umständen weitergegeben werden, und es muss eine Richtlinie für die Ausweisausgabe vorhanden sein.	Ⓐ	Ⓑ	

4.3 Fahrer- und Fahrzeugidentifizierung

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
4.3.1	Alle Fahrer müssen sich anhand eines amtlichen Lichtbildausweises (z.B. Führerschein, Reisepass oder Personalausweis) ausweisen, und es wird eine Fahrerliste geführt. Sollten digitale Ausweise von der Einrichtung akzeptiert und durch die lokale Gesetzgebung zugelassen sein, muss ein zuverlässiges Verifizierungsverfahren (einschließlich der gesamten erforderlichen technischen Infrastruktur) vorhanden sein.	Ⓐ	Ⓑ	Ⓒ

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
4.3.2	Überprüfung, ob der Führerschein gültig ist und mit dem Fahrer übereinstimmt. Wenn digitale Führerscheine von der Einrichtung akzeptiert werden und dies nach lokalem Recht zulässig ist, muss ein zuverlässiges Verifizierungsverfahren (einschließlich der gesamten erforderlichen technischen Infrastruktur) vorhanden sein.	Ⓐ	Ⓑ	Ⓒ
4.3.3	Fahrzeugidentifikationsmerkmale werden manuell (d.h. schriftlich) oder mithilfe von Kameras erfasst. Mindestens Kennzeichen und Fahrzeugtyp sind anzugeben.	Ⓐ		

S5. Innenbereich Lager und Büro

5.1 Lagerbereich: Zwischenwände bei mehreren Mietern

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
5.1.1	In Lagerhallen mit mehreren Mietern sind Innenwände, die vom Boden bis zur Decke reichen, und das Dach so konstruiert und instand gehalten, dass sie Durchdringungen widerstehen (Beispiel: Ziegel-, Block-, Kippbetonplatten-, Sandwichpaneelwände mit einer Mindeststärke von 7 mm).	Ⓐ	Ⓑ	Ⓒ
5.1.2	Wenn in Lagerhallen mit mehreren Mietern Innenwände, die vom Boden bis zur Decke reichen, aus Sicherheitsdrahtgitter oder einer anderen branchenüblichen Sicherheitsbarriere bestehen, müssen sie ebenfalls mit einer Alarmanlage zur Einbruchserkennung ausgestattet sein. <i>Hinweis 1: Netze, minderwertige Zäune oder Drahtgitter ohne Sicherheitsstandard sind nicht zulässig.</i> <i>Hinweis 2: Wenn in Lagerhallen mit mehreren Mietern die Innenwände aus massivem Material vom Boden bis zur Decke bestehen, entfällt diese Anforderung.</i>	Ⓐ	Ⓑ	Ⓒ

5.2 Innere Lagerbereiche

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
5.2.1	Zur Überwachung der internen Lagerbereiche ist eine Einbruchmeldeanlage (z.B. Infrarot-, Bewegungs-, Schall- oder Vibrationserkennung) erforderlich. Die Alarmer müssen außerhalb der Betriebszeiten (d.h. bei Lagerschluss) aktiviert und mit dem Hauptalarmsystem verbunden sein. <i>Hinweis 1: Bei einem Lagerbetrieb rund um die Uhr (24/7/366) kann diese Anforderung entfallen, sofern die Risiken und Gegenmaßnahmen in der lokalen Risikobewertung dokumentiert sind. (Siehe Anforderung 1.1.5)</i> <i>Hinweis 2: Unabhängig von den Betriebszeiten ist eine Perimeterüberwachung oder die Installation physischer Barrieren an Außentüren und Fenstern im Erdgeschoss von Büro und Lager stets erforderlich. (Siehe Anforderungen 3.2.2 und 3.2.6)</i>	Ⓐ		

5.3 Innere Rampentore und Rampenbereiche

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
5.3.1	Alle internen Rampentore und Rampenbereiche sind mit Kamera-/Videoüberwachung (CCTV/VSS) ausgestattet (Farb- oder „Tag/Nacht“-Kameras).	Ⓐ	Ⓑ	Ⓒ
5.3.2	Die Sicht auf das Be- und Entladen von Fracht an allen internen Rampentoren und Rampenbereichen, ist jederzeit frei, es sei denn, es kommt aufgrund betrieblicher Erfordernisse (z.B. Be- und Entladung von Lkw in Echtzeit) zu vorübergehenden Behinderungen.	Ⓐ	Ⓑ	Ⓒ
5.3.3	Die Vermögenswerte des Käufers werden in den Bereichen Warenvorbereitung/-bereitstellung (z.B. Palettenbau-/Aufbaubereiche, Wege zu und von den Lagerregalen, Rampen, Transitzkorridore) zu 100 % videoüberwacht.	Ⓐ	Ⓑ	
5.3.4	Eine Analyse der toten Winkel für eine 100%ige Videoüberwachung der Warenbewegungen muss mindestens jährlich durchgeführt werden, es sei denn, es finden betriebliche und/oder bauliche Änderungen im Lager statt.	Ⓐ		

5.4 Zugangskontrolle zwischen Büro und Rampe/Lager

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
5.4.1	Der Zugang zwischen Büro und Rampe/Lager ist kontrolliert.	Ⓐ	Ⓑ	
5.4.2	Die Türalarme für Zutrittskarten oder Gegensprechanlagen an Türen zwischen Büro und Laderampe/Lager sind lokal hörbar und lösen einen Alarm aus, wenn die Türen länger als 60 Sekunden offen gehalten werden oder sofort, wenn sie gewaltsam geöffnet werden.	Ⓐ		
5.4.3	Türalarme für Türen zwischen Büro und Laderampe/Lager sind lokal hörbar oder lösen einen Alarm aus, der eine Reaktion erfordert, wenn die Türen länger als 60 Sekunden offen gehalten oder gewaltsam geöffnet werden.		Ⓑ	
5.4.4	Der Zugang zu den Rampen-/Lagerbereichen ist den autorisierten Mitarbeitern des LSP/Antragstellers und den begleiteten Besuchern nur nach geschäftlichem Bedarf und unter Auflagen gestattet.	Ⓐ	Ⓑ	Ⓒ
5.4.5	Die Zugangsliste für Rampen-/Lagerbereiche wird mindestens vierteljährlich überprüft, um sicherzustellen, dass die Zugangsberechtigung nur dem dafür vorgesehenen/autorisierten Personal erteilt wird.	Ⓐ	Ⓑ	

5.5 Bereich für hochwertige Fracht (HVC)

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
5.5.1	Die Größe und Nutzung des HVC Bereichs können durch eine Vereinbarung zwischen Käufer, Logistikdienstleister und Antragsteller festgelegt werden. Liegt keine solche Vereinbarung vor, muss der HVC Bereich ein Mindestlagervolumen von 6 Kubikmetern Produkt aufweisen.	Ⓐ	Ⓑ	
5.5.2	HVC/ Bereichsumfang allseitig eingezäunt oder mit festen Wänden versehen, einschließlich Oberseite/Dach.	Ⓐ	Ⓑ	
5.5.3	HVC/ Bereich hat eine Verriegelungsvorrichtung an Tür/Tor.	Ⓐ	Ⓑ	
5.5.4	Vollständige Videoüberwachung (Farb- oder Tag-/Nachtkameras) des Eingangsbereichs und des Inneren des HVC Bereichs. <i>Hinweis: Ist das HVC zu klein für eine Innenkamera, genügt die Videoüberwachung des Eingangsbereichs.</i>	Ⓐ		
5.5.5	Videoüberwachung (Farb- oder Tag-/Nachtkameras) am Eingang des HVC Bereichs.		Ⓑ	
5.5.6	Benötigen mehr als 10 Personen Zugang zum HVC Bereich, erfolgt die Zugangskontrolle elektronisch per Karte/Transponder. Bei 10 oder weniger Personen ist ein robustes Schloss- oder Vorhängeschlosssystem mit kontrollierter Schlüsselausgabe erforderlich. Schlüssel können schichtweise an einzelne Personen ausgegeben werden, dürfen jedoch nur mit Genehmigung weitergegeben und im Schlüsselprotokoll vermerkt werden. Alle Schlüssel sind nach Gebrauch zurückzugeben und zu dokumentieren.	Ⓐ		
5.5.7	Türen/Tore des HVC Bereichs sind mit einem Alarm zur Erkennung von Einbruchsversuchen ausgestattet. Alarmer können durch Türkontakte und/oder durch Videoüberwachung/Bewegungsmelder ausgelöst werden, um unbefugten Zutritt zu erkennen.	Ⓐ		
5.5.8	Der Außenbereich des HVC Bereichs wird in gutem Zustand gehalten und monatlich auf Unversehrtheit und Beschädigungen überprüft.	Ⓐ		

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
5.5.9	Der LSP/Antragsteller stellt sicher, dass der Zugriff auf den HVC Bereich nur autorisierten Mitarbeitern gewährt wird.			
	Die Liste der genehmigten Zugriffsberechtigten für die HVC Zone wird monatlich überprüft und in Echtzeit aktualisiert, wenn ein Mitarbeiter das Unternehmen verlässt oder keinen Zugriff mehr benötigt.	Ⓐ	Ⓑ	
	Ein Verfahren für den HVC-Zugriff ist vorhanden.			

5.6 Müllinspektion aus dem Lager

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
5.6.1	Die Müllsammelbehälter und Verdichtungsbereiche im Lager und/oder auf der Außenfläche werden per Videoüberwachung (CCTV/VSS) überwacht.	Ⓐ		
5.6.2	Sofern verwendet, sind die im Lager verwendeten Müllsäcke transparent.		Ⓑ	Ⓒ

5.7 Vorverladung und Bereitstellung

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
5.7.1	Das Vorladen oder Parken von FTL-/speziellen Käufer-Lkw außerhalb des Lagergeländes ist außerhalb der Betriebszeiten nur nach vorheriger Absprache zwischen Käufer und Spediteur/Antragsteller gestattet.			
	Es sind alternative Sicherheitsmaßnahmen zu ergreifen (z.B. zusätzliche Sicherheitsvorrichtungen an Fahrzeugen/Laderäumen).	Ⓐ	Ⓑ	Ⓒ
	<i>Hinweis: „Außerhalb des Lagergeländes“ bezeichnet Bereiche, die zwar vom Lagergelände getrennt, aber innerhalb des Geländes/der Umzäunung des Spediteurs/Antragstellers liegen.</i>			

5.8 Personenkontrollen und Ausgangskontrollen

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
5.8.1	Schriftliche Sicherheitsrichtlinien legen fest, wie „persönliche Behälter“ im Lager kontrolliert werden. Zu den persönlichen Behältern gehören beispielsweise Brotdosen, Rucksäcke, Kühlboxen und Handtaschen.	Ⓐ	Ⓑ	
5.8.2	Sofern es nach lokalem Recht zulässig ist, muss der Logistikdienstleister/Antragsteller ein dokumentiertes Verfahren für Ausgangskontrollen entwickeln und pflegen. Die Aktivierung dieses Verfahrens liegt im Ermessen des Logistikdienstleisters/Antragstellers und/oder richtet sich nach der Vereinbarung zwischen Käufer, Logistikdienstleister und Antragsteller. Das Verfahren muss mindestens die Kriterien für das Recht des Logistikdienstleisters/Antragstellers auf Durchsuchungen festlegen, falls diese erforderlich werden, obwohl sie normalerweise nicht vorgeschrieben sind (z.B. bei Verdacht auf Diebstahl durch Mitarbeiter). Mitarbeiter, Sicherheitsbeauftragte, Subunternehmer und Besucher müssen vor Betreten des Lagers über diese Richtlinie informiert werden.	Ⓐ		

5.9 Kontrolle der Frachtumschlaggeräte

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
5.9.1	Ein Verfahren, das vorschreibt, dass alle Gabelstapler und andere motorisierte Flurförderzeuge außerhalb der Betriebszeiten außer Betrieb genommen werden müssen, existiert. <i>Hinweis: Dies gilt nicht für Hubwagen/Palettenhubwagen.</i>	Ⓐ	Ⓑ	

5.10 Integrität des Containers oder Aufliegers: 7-Punkte-Inspektion

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
5.10.1	Alle ausgehenden, dem Käufer zugeordneten Container oder Auflieger werden einer 7-Punkte-Prüfung unterzogen. Diese umfasst: Vorderwand, linke Seite, rechte Seite, Boden, Decke/Dach, Innen-/Außentüren und Verriegelungsmechanismus, Außenseite/Unterboden. <i>Hinweis: Dies gilt für alle Arten von Aufliegern und Containern mit Schloss und/oder Plombe (d.h. nicht nur für Seefrachtcontainer).</i>	Ⓐ	Ⓑ	Ⓒ

5.11 Frachtübergabeprozess; Plomben

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
5.11.1	Sofern vom Käufer nicht ausdrücklich anders vereinbart, werden bei allen direkten, nonstop Sendungen manipulationssichere Plomben verwendet. Die Plomben müssen gemäß ISO 17712 (Klassifizierung I, S oder H) zertifiziert sein. <i>Hinweis: Bei Sendungen mit mehreren Zwischenstopps sind keine Plomben erforderlich, da dies mit der Komplexität und dem Risiko verbunden ist, dass Fahrer mehrere Plomben mitführen müssen.</i>	Ⓐ	Ⓑ	Ⓒ
5.11.2	Der LSP/Antragsteller muss über dokumentierte Verfahren für die Verwaltung und Kontrolle von Sicherheitsplomben, Anhänger-(Container-)Türschlössern, Bolzenschlössern und anderer Sicherheitsausrüstung verfügen.	Ⓐ	Ⓑ	Ⓒ
5.11.3	Sicherheitsplomben werden ausschließlich von autorisiertem Personal, d.h. Lagerpersonal, angebracht oder entfernt. Dieses Personal ist angewiesen, beschädigte Plomben zu erkennen und zu melden. Der Fahrer darf die Plomben nur mit Genehmigung des Käufers anbringen oder entfernen.	Ⓐ	Ⓑ	Ⓒ
5.11.4	Es gibt Verfahren zur Erkennung und Meldung kompromittierter Sicherheitsplomben.	Ⓐ	Ⓑ	Ⓒ

5.12 Ladungsintegrität; Validierungsprozess für Be- und Entladung

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
5.12.1	Es sind robuste Verfahren implementiert, die sicherstellen, dass alle vom Käufer versandten und empfangenen Güter bei der Übergabe durch eine manuelle und/oder elektronische Stückzählung geprüft werden. Der Prozess muss gewährleisten, dass Abweichungen konsequent erkannt, dokumentiert und dem Logistikdienstleister/Antragsteller und/oder Käufer gemeldet werden. Die manuellen und/oder elektronischen Aufzeichnungen müssen beweissicher sein. Falls keine Fahrer anwesend sind, um diese Prüfung zu bezeugen, müssen Käufer/Logistikdienstleister/Antragsteller alternative Zählnachweise wie Scans und/oder Videoaufnahmen (CCTV/VSS) sicherstellen, die speziell für diesen Zweck erfasst und aufbewahrt werden. <i>Hinweis: Neben fehlender Ware können Abweichungen auch Beschädigungen, fehlende Gurte oder Klebebänder, Schnitte oder andere offensichtliche Öffnungen umfassen, die auf Diebstahl oder Entwendung hindeuten.</i>	Ⓐ	Ⓑ	Ⓒ

5.13 Betrügerische Abholungen

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
5.13.1	Die Fahreridentifikation des Lkw, die Dokumentation zur Frachtabholung und die vom Käufer angegebenen Vorabinformationen werden vor dem Verladen überprüft. Ein entsprechendes Verfahren muss vorhanden sein. Wenn digitale Identitäten vom Betrieb akzeptiert werden und dies nach lokaler Gesetzgebung zulässig ist, muss ein umfassendes Verifizierungsverfahren (einschließlich der gesamten erforderlichen technischen Infrastruktur) implementiert sein.	Ⓐ	Ⓑ	Ⓒ

S6. Sicherheitssysteme: Gestaltung, Monitoring und Reaktion

6.1 Monitoring Zentrale

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
6.1.1	Die Überwachung von Alarmereignissen erfolgt rund um die Uhr an 366 Tagen im Jahr über eine interne oder externe Überwachungszentrale, die vor unbefugtem Zugriff geschützt ist. <i>Hinweis: Die Überwachungszentralen können sich auf dem Firmengelände oder außerhalb befinden und vom Unternehmen oder einem Drittanbieter betrieben werden. In jedem Fall muss der Zugang durch ein elektronisches Zutrittskontrollsystem (Ausweise), Schlösser oder biometrische Scanner geregelt werden.</i>	Ⓐ	Ⓑ	Ⓒ
6.1.2	Die Überwachungszentrale reagiert in Echtzeit auf alle Alarme des Sicherheitssystems, rund um die Uhr, 366 Tage im Jahr.	Ⓐ	Ⓑ	Ⓒ
6.1.3	Die Überwachungsstelle bestätigt die Alarmauslösung und eskaliert die Meldung in weniger als 3 Minuten.	Ⓐ	Ⓑ	Ⓒ
6.1.4	Alarmüberwachungsprotokolle sind verfügbar.	Ⓐ	Ⓑ	Ⓒ
6.1.5	Prozeduren für die Alarmzentrale zur Reaktion auf Störungen liegen vor.	Ⓐ	Ⓑ	Ⓒ

6.2 Einbrucherkennungssystem (IDS Intruder Detection System)

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
6.2.1	Alle Einbruchmeldeanlagen werden außerhalb der Betriebszeiten aktiviert und sind mit dem Hauptalarmsystem verbunden.	Ⓐ	Ⓑ	Ⓒ
6.2.2	Alarmaufzeichnungen des IDS werden 90 Tage lang gespeichert.	Ⓐ	Ⓑ	
6.2.3	Die Alarmaufzeichnungen des IDS werden sicher gespeichert und mindestens wöchentlich gesichert.	Ⓐ	Ⓑ	

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
6.2.4	Ein Verfahren zur Sicherstellung des beschränkten Zugriff auf das IDS für autorisierte Personen oder Systemadministratoren ist vorhanden. Dies umfasst Server, Konsolen, Controller, Bedienfelder, Netzwerke und Daten. Die Zugriffsrechte für das IDS müssen umgehend aktualisiert werden, wenn Personen das Unternehmen verlassen oder ihre Rolle wechseln und daher keinen Zugriff mehr benötigen.	Ⓐ	Ⓑ	Ⓒ
6.2.5	Alarm wird bei Stromausfall/Verlust des IDS ausgelöst. <i>Hinweis: Bei Systemen mit unterbrechungsfreier Stromversorgung (USV) wird der Alarm ausgelöst, wenn die USV-Batterie ausfällt.</i>	Ⓐ	Ⓑ	Ⓒ
6.2.6	Eine Überprüfung der IDS-Alarmaktivierung wird durchgeführt. <i>Hinweis: Verfahren zur Überprüfung der Aktivierung der Alarmanlage außerhalb der Betriebszeiten.</i>	Ⓐ	Ⓑ	Ⓒ
6.2.7	Einbruchmeldeanlage (IDS): Alarmübertragung über Festnetz-, Funk- und/oder andere Kommunikationswege einschließlich Erkennung und Meldung von Kommunikationsausfällen.	Ⓐ	Ⓑ	
6.2.8	Backup-Kommunikationssystem auf dem IDS-Gerät und/oder Leitungsausfall vorhanden.	Ⓐ	Ⓑ	

6.3 Automatisches Zutrittskontrollsystem (AACS Automatic Access Control System)

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
6.3.1	AACS-Transaktionsdatensätze der letzten 90 Tage sind verfügbar. Daten sicher gespeichert und dupliziert.	Ⓐ	Ⓑ	
6.3.2	Verfahren zur Sicherstellung vorhanden, dass der Zugriff auf AACS auf autorisierte Personen oder Systemadministratoren beschränkt ist. Zugriffsrechte müssen umgehend aktualisiert werden, wenn Personen das Unternehmen verlassen oder ihre Rolle wechseln und daher keinen Zugriff mehr benötigen.	Ⓐ	Ⓑ	

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
6.3.3	Die Berichte des Zugangssystems werden mindestens vierteljährlich geprüft, um Unregelmäßigkeiten oder Missbrauch (z.B. mehrere erfolglose Zugriffsversuche, Fehlesungen (z.B. deaktivierte Karte), Hinweise auf Kartenweitergabe zum unbefugten Zugriff usw.) zu erkennen. Ein entsprechender Prozess ist eingerichtet.	Ⓐ	Ⓑ	

6.4 CCTV / Videoüberwachung (VSS)

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
6.4.1	Digitale Aufzeichnung von Videoüberwachungs- und Videoüberwachungssystemen ist vorhanden.	Ⓐ	Ⓑ	Ⓒ
6.4.2	Die Aufnahmegeschwindigkeit für CCTV/VSS ist auf mindestens 8 Bilder pro Sekunde (fps) pro Kamera eingestellt.	Ⓐ	Ⓑ	Ⓒ
6.4.3	Die digitale Aufzeichnungsfunktion wird an Betriebstagen täglich gemäß Verfahren überprüft. Aufzeichnungen sind verfügbar.	Ⓐ	Ⓑ	Ⓒ
6.4.4	Videoaufzeichnungen von Überwachungskameras/Videoüberwachungssystemen werden, sofern dies nach lokalem Recht zulässig ist, mindestens 30 Tage lang gespeichert. Der LSP/Antragsteller muss Nachweise über alle lokalen Gesetze vorlegen, die den Einsatz von Überwachungskameras verbieten und/oder die Speicherdauer der Videodaten auf weniger als 30 Tage beschränken.	Ⓐ	Ⓑ	Ⓒ
6.4.5	Der Zugang zum Videoüberwachungssystem (CCTV/VSS), einschließlich Hardware, Software und Daten-/Videospeicher, ist streng kontrolliert. Dieser Raum muss verschlossen sein, wenn sich das Videoüberwachungssystem (CCTV/VSS) mit Zugangskontrollen auf dem Gelände befindet.	Ⓐ	Ⓑ	Ⓒ
6.4.6	CCTV-/VSS-Bilder werden aus Sicherheitsgründen nur von autorisiertem Personal eingesehen.	Ⓐ	Ⓑ	Ⓒ

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
6.4.7	Es liegen Verfahren vor, die die Datenschutzrichtlinien für CCTV/VSS hinsichtlich der Verwendung von Echtzeit- und Archivbildern gemäß den geltenden Gesetzen detailliert beschreiben.	Ⓐ	Ⓑ	

6.5 Außen- und Innenbeleuchtung

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
6.5.1	Die Außen- und Innenbeleuchtung ist ausreichend, um CCTV/VSS-Bilder zu unterstützen, die eine Untersuchung und die Aufzeichnung von Beweismaterial ermöglichen.	Ⓐ	Ⓑ	
6.5.2	Die Außen- und Innenbeleuchtung ist ausreichend, um alle Fahrzeuge und Personen deutlich zu erkennen.	Ⓐ		

S7. Training und Prozeduren

7.1 Eskalationsverfahren

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
7.1.1	Es gelten lokale Verfahren für den Umgang mit den Vermögenswerten des Käufers, einschließlich des Prozesses zur zeitnahen Meldung von Verlust, Fehlen oder Diebstahl. Vorfälle sind vom Logistikdienstleister/Antragsteller innerhalb von 24 Stunden an den Käufer zu melden. Offensichtliche Diebstähle werden unverzüglich gemeldet. Der Prozess wird konsequent eingehalten.	Ⓐ	Ⓑ	Ⓒ
7.1.2	Notfallkontakte für Käufer und LSP/Antragsteller im Bereich Lager Management bei Sicherheitsvorfällen sind aufgelistet und verfügbar. Die Liste wird alle 6 Monate aktualisiert und enthält Notfallkontakte der Strafverfolgungsbehörden.	Ⓐ	Ⓑ	Ⓒ

7.2 Managementverpflichtung

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
7.2.1	Das Management muss eine Sicherheitsrichtlinie entwickeln, kommunizieren und aufrechterhalten, um sicherzustellen, dass alle relevanten Personen (d.h. Mitarbeiter und Auftragnehmer) die Sicherheitserwartungen des Anbieters klar kennen.	Ⓐ	Ⓑ	Ⓒ

7.3 Schulungen

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
7.3.1	Schulungen zur Sensibilisierung für Sicherheitsthemen/Bedrohungen sind allen Mitarbeitern innerhalb der ersten 60 Tage ihrer Beschäftigung und danach alle 2 Jahre anzubieten.	Ⓐ	Ⓑ	Ⓒ
7.3.2	Schulungen zur Sensibilisierung für Informationssicherheit mit Schwerpunkt auf dem Schutz der elektronischen und physischen Versanddaten des Käufers werden den Mitarbeitern angeboten, die Zugriff auf die Informationen des Käufers haben, und danach mindestens alle zwei Jahre oder gemäß den lokalen Gesetzen, falls ein kürzeres Auffrischungsintervall vorgeschrieben ist.	Ⓐ	Ⓑ	Ⓒ

7.4 Zugang zu den Vermögenswerten des Käufers

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
7.4.1	Es ist ein Verfahren vorhanden zum Schutz der Vermögenswerte des Käufers (z.B. Fracht) vor unbefugtem Zugriff durch Mitarbeiter, Besucher usw.	(A)	(B)	(C)

7.5 Informationskontrolle

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
7.5.1	Der Zugriff auf Versanddokumente und Informationen über die Vermögenswerte des Käufers wird nach dem Prinzip beschränkt, nur relevanten Mitarbeitern Kenntnis zu ermöglichen. Es muss ein Verfahren vorhanden sein, das den Schutz der Informationen des Käufers gewährleistet.	(A)	(B)	(C)
7.5.2	Der Zugriff auf Versanddokumente und Informationen zu den Vermögenswerten des Käufers wird überwacht und protokolliert. Die entsprechenden Prozesse und Aufzeichnungen sind vorhanden.	(A)	(B)	(C)
7.5.3	Versanddokumente und alle anderen Dokumente, einschließlich Informationen über das Vermögen des Käufers, werden bis zur Vernichtung aufbewahrt.	(A)	(B)	(C)

7.6 Meldung von Sicherheitsvorfällen

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
7.6.1	Ein System zur Meldung und Verfolgung von Sicherheitsvorfällen ist vorhanden und wird zur Umsetzung proaktiver Maßnahmen genutzt.	(A)	(B)	

7.7 Wartungsprogramme

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
7.7.1	Für alle technischen (physischen) Sicherheitsinstallationen/-systeme sind Wartungsprogramme vorhanden, um deren Funktionsfähigkeit jederzeit zu gewährleisten (z.B. Kameraüberwachung/Videoüberwachungssysteme, Zutrittskontrollen, Einbruchmeldeanlagen und Beleuchtung).	Ⓐ	Ⓑ	Ⓒ
7.7.2	Die vorbeugende Wartung wird einmal jährlich oder gemäß den Vorgaben des Herstellers durchgeführt.	Ⓐ	Ⓑ	Ⓒ
7.7.3	Funktionsprüfungen aller Systeme werden einmal wöchentlich durchgeführt und dokumentiert, es sei denn, ein Systemausfall wird sofort/automatisch gemeldet oder ausgelöst.	Ⓐ	Ⓑ	
7.7.4	Ein Reparaturauftrag muss innerhalb von 48 Stunden nach Feststellung des Fehlers erteilt werden. Dauert die Reparatur voraussichtlich länger als 24 Stunden, müssen alternative Maßnahmen ergriffen werden.	Ⓐ	Ⓑ	

7.8 Verantwortung Auftragnehmer

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
7.8.1	Der LSP/Antragsteller ist dafür verantwortlich, dass alle Subunternehmer/Lieferanten die relevanten Sicherheitsprogramme des LSP/Antragstellers kennen und einhalten.	Ⓐ	Ⓑ	Ⓒ

7.9 Versand- und Empfangsaufzeichnungen

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
7.9.1	Die Versand- und Empfangsdokumente müssen lesbar, vollständig und korrekt sein (d.h. Uhrzeit, Datum, Unterschriften, Fahrer, Versand- und Empfangspersonal, Sendungsdetails und -menge usw.). Die Namen von Fahrer und Versender müssen stets deutlich lesbar sein.	Ⓐ	Ⓑ	Ⓒ

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
7.9.2	Der LSP/Antragsteller ist verpflichtet, Aufzeichnungen über alle Abholungen und Liefernachweise für einen Zeitraum von mindestens zwei Jahren aufzubewahren und diese den Schadensermittlungen bei Bedarf zur Verfügung zu stellen.	Ⓐ	Ⓑ	Ⓒ
7.9.3	Der Liefernachweis muss gemäß der schriftlichen Vereinbarung zwischen dem Käufer und dem Logistikdienstleister/Antragsteller erbracht werden. Sofern es der Käufer verlangt, benachrichtigt der Bestimmungsort den Abgangsort innerhalb der vereinbarten Frist über den Erhalt der Sendung und gleicht die vorab mitgeteilten Sendungsdetails ab.	Ⓐ	Ⓑ	Ⓒ

7.10 Avisierungsprozess

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
7.10.1	Sofern vom Käufer gewünscht, ist ein Vorabbenachrichtigungsverfahren für eingehende und/oder ausgehende Sendungen eingerichtet. Die Details der Vorabbenachrichtigung müssen zwischen Käufer und Spediteur/Antragsteller vereinbart werden. Zu den empfohlenen Angaben gehören Abfahrtszeit, voraussichtliche Ankunftszeit, Spedition, Name des Fahrers, Kennzeichen, Sendungsinformationen (Stückzahl, Gewicht, Frachtbriefnummer usw.) und die Nummern der Plomben.	Ⓐ	Ⓑ	Ⓒ

S8. Integrität der Belegschaft

8.1 Überprüfung/Hintergrundprüfung (soweit nach lokalem Recht zulässig)

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
8.1.1	Der LSP/Antragsteller muss ein Screening-/Validierungsverfahren durchführen, das mindestens die Überprüfung der letzten fünf Jahre der Beschäftigung und des Strafregisters umfasst. Dieses Screening-/Validierungsverfahren gilt für alle Bewerber, einschließlich Angestellter und Auftragnehmer. Der LSP/Antragsteller muss zudem vertraglich vereinbart haben, dass ein gleichwertiges Verfahren bei den Vertragsunternehmen angewendet wird, die Zeitarbeiter bereitstellen.	Ⓐ	Ⓑ	Ⓒ
8.1.2	Der LSP/Antragsteller muss Vereinbarungen treffen, um die erforderlichen Überprüfungen/Hintergrundinformationen von der Agentur und/oder dem Subunternehmer, der Zeit-Arbeitskräfte bereitstellt, liefern zu lassen, oder diese Überprüfungen selbst durchführen. Die Überprüfung muss eine Kontrolle des Strafregisters und der Beschäftigungsnachweise umfassen.	Ⓐ	Ⓑ	Ⓒ
8.1.3	Ein Verfahren zum Umgang mit falschen Angaben von Bewerbern/Mitarbeitern vor und nach der Einstellung muss vorliegen.	Ⓐ	Ⓑ	Ⓒ

8.2 Kündigung oder Wiedereinstellung von Arbeitskräften

Hinweis: Der Begriff „Beendigung“ umfasst sowohl freiwillige als auch unfreiwillige Trennungen – also gekündigte und ausgeschiedene Mitarbeiter.

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
8.2.1	Physische Vermögenswerte ausgeschiedener Mitarbeiter, darunter Firmenausweise, Zutrittskarten, Schlüssel, Ausrüstung, IT-Geräte und sensible Informationen, müssen sichergestellt werden. Ein dokumentiertes Verfahren ist erforderlich.	Ⓐ	Ⓑ	Ⓒ
8.2.2	Schutz der Käuferdaten: Der Zugriff ausgeschiedener Mitarbeiter auf physische und elektronische Systeme, einschließlich solcher, die Käuferdaten enthalten, muss gesperrt werden. Ein dokumentiertes Verfahren ist erforderlich.	Ⓐ	Ⓑ	Ⓒ

Nr. Anforde rung	Anforderungen / Kontrollen	Anwendbares Niveau		
8.2.3	Eine Checkliste für die Einarbeitung und das Ausscheiden von Mitarbeitern muss zur Überprüfung vorhanden sein.	Ⓐ	Ⓑ	Ⓒ
8.2.4	Wiedereinstellung: Es bestehen Verfahren, die verhindern, dass der Personaldienstleister/Antragsteller Mitarbeiter wieder einstellt, wenn die Ablehnungs-/Kündigungskriterien weiterhin gültig sind. <i>Hinweis: Vor einer Wiedereinstellung werden die Unterlagen geprüft (z.B. Hintergrundinformationen von zuvor gekündigten Mitarbeitern oder abgelehnten Bewerbern).</i>	Ⓐ	Ⓑ	Ⓒ

S9. Zentrale Anforderungen (gültig für Zertifizierung mehrerer Standorte)

9.1 Allgemein

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
9.1.1	Es gibt eine zentrale Stelle zur Verwaltung des Sicherheitsmanagementsystems für alle Standorte, wie im Geltungsbereich der Multi-Site-Zertifizierung definiert.	Ⓐ	Ⓑ	Ⓒ
9.1.2	Alle Standorte müssen in einer rechtlichen oder vertraglichen Beziehung zur zentralen Stelle stehen. Diese Anforderung gilt nicht für Standorte von Unterauftragnehmern, die gemäß CFD-Klausel 4.2.2 in den Zertifizierungsbereich einbezogen werden.	Ⓐ	Ⓑ	Ⓒ
9.1.3	Es wird ein einheitliches Sicherheitsmanagementsystem eingerichtet, um sicherzustellen, dass alle Standorte innerhalb des Systems die Anforderungen des jeweils geltenden TAPA-Sicherheitsstandards erfüllen.	Ⓐ	Ⓑ	Ⓒ
9.1.4	Die zentrale Stelle und ihr Managementsystem unterliegen internen Audits, um die fortlaufende Einhaltung der TAPA-Standards sicherzustellen.	Ⓐ	Ⓑ	Ⓒ
9.1.5	Die zentrale Stelle führt Audits an den betreffenden Standorten durch, um sicherzustellen, dass jeder Standort die geltenden TAPA FSR Anforderungen erfüllt. Die Audits müssen anhand der entsprechenden TAPA Auditvorlagen durchgeführt werden. Alle jährlichen und erforderlichen Standort-Audits müssen abgeschlossen sein und dem Auditor vor dem Zertifizierungsprozess vorliegen.	Ⓐ	Ⓑ	Ⓒ
9.1.6	Die zentrale Stelle ist befugt und berechtigt, von allen Standorten die Einhaltung der TAPA-Sicherheitsstandards zu verlangen und gegebenenfalls Korrektur- und Präventivmaßnahmen durchzuführen. <i>Hinweis: Dies sollte gegebenenfalls in der formellen Vereinbarung zwischen der zentralen Stelle und den Standorten festgehalten werden.</i>	Ⓐ	Ⓑ	Ⓒ

9.2 Richtlinien und Verfahren

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
9.2.1	Die zentrale Stelle ist verpflichtet, dokumentierte Richtlinien und Verfahren für ihre Sicherheitsmanagementsysteme zu führen, die für alle ihre Standorte gelten.	Ⓐ	Ⓑ	Ⓒ
9.2.2	Die zentrale Stelle hat sicherzustellen, dass Richtlinien und Verfahren an allen Standorten bedarfsgerecht aktualisiert, kommuniziert, eingesetzt und implementiert werden.	Ⓐ	Ⓑ	Ⓒ
9.2.3	Die Richtlinien und Verfahren müssen stets aktuell sein und bei Bedarf von allen Standorten leicht zugänglich gemacht werden.	Ⓐ	Ⓑ	Ⓒ

9.3 Bericht zur Selbstbewertung für alle Standorte

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
9.3.1	Die zentrale Stelle verpflichtet alle Standorte zur Durchführung einer Selbstbewertung. Alle Berichte zur Selbstbewertung sind der zentralen Stelle zur Archivierung und Überprüfung vorzulegen. Die Unterlagen sind mindestens zwei (2) Jahre lang aufzubewahren.	Ⓐ	Ⓑ	Ⓒ
9.3.2	Die zentrale Stelle soll sicherstellen, dass alle SCARs aus der Selbstbewertung und den Audits ordnungsgemäß abgeschlossen werden, um die Sicherheitsmanagementsysteme zu verbessern.	Ⓐ	Ⓑ	Ⓒ
9.3.3	Alle Standorte müssen der zentralen Stelle regelmäßig Fortschrittsberichte und Meldungen zu allen noch offenen SCARs übermitteln. Die zentrale Stelle informiert die Geschäftsleitung des LSP/Antragstellers, falls SCARs nicht fristgerecht bearbeitet werden. Die Unterlagen sind mindestens zwei (2) Jahre lang aufzubewahren.	Ⓐ	Ⓑ	Ⓒ

9.4 Inspektionsberichte, Protokolle (Besucher-/Fahrerprotokolle), 7-Punkte-Inspektionen

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
9.4.1	Die zentrale Stelle muss über Verfahren verfügen, die sicherstellen, dass an allen Standorten Aufzeichnungen über Inspektionen, Besucherlisten, Fahrerprotokolle und die 7-Punkte-Inspektion usw. geführt werden.	Ⓐ	Ⓑ	Ⓒ

9.5 Risikobewertung aller Standorte

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
9.5.1	Die zentrale Stelle muss über Verfahren verfügen, die sicherstellen, dass an allen Standorten angemessene Risikobewertungen und -Managementmaßnahmen durchgeführt werden, und ihre Aufzeichnungen müssen mindestens zwei (2) Jahre lang aufbewahrt werden.	Ⓐ	Ⓑ	Ⓒ

9.6 CCTV-/VSS- und Alarmanlagenplan des Geländes

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
9.6.1	Die zentrale Stelle muss über Verfahren verfügen, die sicherstellen, dass alle Standorte die Dokumente zu allen physischen Sicherheitssystemen wie Videoüberwachung und Alarmanlagen überprüfen und pflegen.	Ⓐ	Ⓑ	Ⓒ

9.7 Protokolle zu Alarm- und Zutrittskontrolle

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
9.7.1	Die zentrale Stelle muss über Verfahren verfügen, die sicherstellen, dass alle Alarm- und Zutrittskontrollsysteme gewartet und getestet werden, um ihre Betriebssicherheit zu gewährleisten.	Ⓐ	Ⓑ	Ⓒ
9.7.2	Die zentrale Stelle muss über Verfahren verfügen, die sicherstellen, dass an allen Standorten Aufzeichnungen über alle Tests und Vorfälle im Bereich der Einbruchserkennung und Zugangskontrolle geführt werden.	Ⓐ	Ⓑ	Ⓒ

9.8 Schulungsunterlagen

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
9.8.1	Die zentrale Stelle muss über Verfahren verfügen, um sicherzustellen, dass an allen Standorten ordnungsgemäße Schulungsnachweise über die Sicherheitsschulungen ihrer Mitarbeiter geführt werden.	Ⓐ	Ⓑ	Ⓒ
9.8.2	Die zentrale Stelle muss über Verfahren verfügen, um sicherzustellen, dass an allen Standorten Schulungsnachweise über die Sicherheitsausbildung aller Mitarbeiter geführt werden. Diese Nachweise sind mindestens zwei (2) Jahre lang aufzubewahren.	Ⓐ	Ⓑ	Ⓒ

9.9 Screening-/Überprüfungsakten

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
9.9.1	Die zentrale Stelle muss über Verfahren verfügen, die sicherstellen, dass alle Standorte in regelmäßigen Abständen eine Überprüfung der Screening Aufzeichnungen durchführen, um die Integrität und Effektivität der Sicherheitsmanagementsysteme zu gewährleisten.	Ⓐ	Ⓑ	Ⓒ
9.9.2	Die zentrale Stelle muss über Verfahren verfügen, die die Aufbewahrung von Aufzeichnungen über Überprüfungen einschließlich ihrer Ergebnisse und der Korrektur-/Präventivmaßnahmen gemäß Punkt 9.1.6 gewährleisten. Die Aufzeichnungen werden mindestens zwei (2) Jahre lang aufbewahrt.	Ⓐ	Ⓑ	Ⓒ

9.10 Managementbewertung zur Auswertung der Selbstprüfungen; festgestellte SCARs; etwaige Verluste, Diebstähle; Risikobewertungen

Nr. Anforderung	Anforderungen / Kontrollen	Anwendbares Niveau		
9.10.1	Die zentrale Stelle führt mindestens regelmäßige Managementüberprüfungen durch, um die Einhaltung, Effektivität und Verbesserung ihrer Sicherheitsmanagementsysteme sicherzustellen.	Ⓐ	Ⓑ	Ⓒ
9.10.2	Die Managementbewertungen umfassen unter anderem die Wirksamkeit von Selbstbewertungen, den Abschluss von SCARs, Risikobewertungen, Vorfällen und Verbesserungsmaßnahmen.	Ⓐ	Ⓑ	Ⓒ

Nr. Anforde rung	Anforderungen / Kontrollen	Anwendbares Niveau		
9.10.3	Die zentrale Stelle hat Aufzeichnungen über alle Managementbewertungen mindestens zwei (2) Jahre lang aufzubewahren.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

8.0 IT- und Cybersicherheitsbedrohung – Erweiterte Option

Die FSR umfassen optionale Erweiterungen zum Schutz vor IT- und Cybersicherheitsbedrohungen, die ein höheres Schutzniveau bieten und zusätzlich zu den Modulen eingesetzt werden können. Diese optionale Erweiterung kann vom LSP/Antragsteller bzw. dessen Auftraggeber als zusätzliche Anforderung für die betriebliche Sicherheit ausgewählt werden. Wird diese optionale Erweiterung in der Vorprüfung für das Zertifizierungsaudit ausgewählt, werden alle Anforderungen verbindlich.

Die erweiterte Option im Rahmen von TAPA FSR bietet grundlegende IT- und Cybersicherheitskontrollen auf Standortebene. Mitgliedern wird dringend empfohlen, die Cybersecurity Standards (CSS) anzuwenden, um ein umfassenderes und robusteres Cybersicherheitsgerüst zu erreichen.

E8. Obligatorische Anforderungen

Nr. Anforderung	Anforderungen / Kontrollen
E8.1.1	Der LSP/Antragsteller muss über Sicherheitsrichtlinien für IT und Cyberbedrohungen verfügen. Diese Richtlinien können separat oder in einem gemeinsamen Dokument vorliegen. Sie müssen Folgendes erläutern: 1. Die Maßnahmen des LSP/Antragstellers zur Identifizierung und Abwehr von Bedrohungen. 2. Die bestehenden Richtlinien und Verfahren zum Schutz vor, zur Erkennung, Prüfung und Reaktion auf Sicherheitsvorfälle. 3. Die Methoden zur Wiederherstellung von IT-Systemen und/oder Daten. 4. Das Kommunikationsprotokoll mit Käufern/Kunden, um die Auswirkungen auf die Lieferkette innerhalb von 24 Stunden nach Bekanntwerden eines Vorfalls zu minimieren. 5. Wie die Richtlinien jährlich überprüft und gegebenenfalls aktualisiert werden.
E8.1.2	Der LSP/Antragsteller ist verpflichtet, allen Mitarbeitern eine Schulung zur Informationssicherheit anzubieten. Diese Schulung muss: 1. Die Rollen und Verantwortlichkeiten der Computernutzer bei der Aufrechterhaltung der Sicherheit sowie die damit verbundenen Vorteile behandeln. 2. Ein System implementieren, das sicherstellt, dass die Schulungsnachweise der Teilnehmer mindestens zwei Jahre lang aufbewahrt werden.

Nr. Anforde rung	Anforderungen / Kontrollen
E8.1.3	Der LSP/Antragsteller muss über eine schriftliche Richtlinie verfügen, die sicherstellt, dass bei Subunternehmern und/oder Lieferanten Cybersicherheitsmaßnahmen umgesetzt werden, die Folgendes gewährleisten: 1. Die Cybersicherheitsanforderungen des LSP/Antragstellers werden an Subunternehmer und/oder Lieferanten kommuniziert und in Verträgen verankert. 2. Falls Subunternehmer und/oder Lieferanten die Cybersicherheitsanforderungen des LSP/Antragstellers nicht anerkennen oder deren Umsetzung ablehnen, müssen Maßnahmen dokumentiert und implementiert sein, die die Risiken für die Cybersicherheitsanforderungen des LSP/Antragstellers und dessen Kunden minimieren.
E8.1.4	Der LSP/Antragsteller muss über einen Plan zur Minderung von Stromausfällen verfügen (z.B. alternative Stromversorgung oder Notstromaggregat), der sicherstellt, dass die Stromversorgung kritischer IT-Systeme (die in der lokalen Risikobewertung identifiziert wurden) für mindestens 48 Stunden gewährleistet ist.
E8.1.5	Die Informationssysteme des LSP/Antragstellers müssen mit lizenzierter Antiviren- und Anti-Malware-Software ausgestattet sein. Diese Software muss über die neuesten Updates verfügen.
E8.1.6	Der LSP/Antragsteller muss über einen geeigneten IT-Notfallplan (DRP) zur Wiederherstellung nach Angriffen auf kompromittierte Systeme verfügen, einschließlich, aber nicht beschränkt auf, alle notwendigen Daten- und Software-Backup- und Wiederherstellungsmaßnahmen.
E8.1.7	Die Informationssysteme des LSP/Antragstellers müssen gesichert werden. Diese Sicherungen müssen regelmäßig getestet werden, und die Sicherungsdaten müssen verschlüsselt und an einen sekundären, externen Standort übertragen werden.

Nr. Anforderung	Anforderungen / Kontrollen
E8.1.8	Der LSP/Antragsteller muss eine Richtlinie für alle Benutzerkonten implementieren, um den Zugriff auf Informationssysteme mithilfe eindeutiger individueller Kennungen und sicherer Passwörter zu verwalten und zu kontrollieren. Folgende Verfahren sind erforderlich: 1. Ein Programm zur Überprüfung der Passwortkonformität ist implementiert. 2. Jedem neuen Konto wird bei der Erstellung ein eindeutiges Anfangspasswort zugewiesen. 3. Anfangspasswörter dürfen weder den Namen noch die Identifikationsnummer des Benutzers enthalten und keinem Standardmuster folgen, das auf Benutzerinformationen basiert. 4. Passwörter werden den Benutzern auf sichere Weise und erst nach Überprüfung ihrer Identität übermittelt. 5. Benutzer müssen verpflichtet sein, ihr Passwort bei der ersten Anmeldung zu ändern. 6. Passwörter müssen mindestens alle 90 Tage geändert werden.

Zur Information: Die Ihnen zur Verfügung gestellte Übersetzung des Standards in die Landessprache zielt darauf ab, das Verständnis der TAPA 2026-Anforderungen zu verbessern. Die Übersetzung des Standards wurde nach bestem Wissen und Gewissen und mit der Kenntnis der erforderlichen Grundlagen initiiert und validiert. Maßgeblich für die Prüfung ist und bleibt jedoch die englische Originalversion des jeweiligen Standards.

Veröffentlichungs- und Urheberrechtsinformationen

Dieses Dokument wird von der Transported Asset Protection Association (TAPA) herausgegeben.

© TAPA 2026–2029

Alle Rechte vorbehalten. Kein Teil dieser Publikation darf ohne vorherige schriftliche Genehmigung der TAPA reproduziert, in einem Datenabfragesystem gespeichert oder in irgendeiner Form oder mit irgendwelchen Mitteln – elektronisch, mechanisch, durch Fotokopieren, Aufzeichnen oder auf andere Weise – übertragen werden, außer in den gesetzlich zulässigen Fällen.

Der in diesem Dokument enthaltene Urheberrechtshinweis gibt das Jahr der letzten Ausgabe an.

Publikationsgeschichte

Erstveröffentlichung: September 2026

Aktuelle Fassung veröffentlicht im: September 2026

Diese öffentlich verfügbare Spezifikation (PAS) tritt am 15. September 2026 in Kraft.

Status dieses Dokuments

Dieses Dokument stellt die TAPA-Sicherheitsanforderungen für Einrichtungen (FSR) – Revision 2026 dar und legt die grundlegenden Anforderungen an die Anlagensicherheit im Rahmen des TAPA-Zertifizierungssystems fest.

Das Dokument bleibt gültig, bis es von TAPA ersetzt, überarbeitet oder zurückgezogen wird.

TAPA kann zukünftige Überarbeitungen, Aktualisierungen oder Ergänzungen veröffentlichen, um sich verändernden Sicherheitsbedrohungen, Branchenpraktiken und technologischen Entwicklungen Rechnung zu tragen.

Verwendung dieses Dokuments

Die Einhaltung dieser Spezifikation kann im Rahmen des TAPA-Zertifizierungsverfahrens für Einrichtungen, die hochwertige und diebstahlgefährdete Güter umschlagen, herangezogen werden.

Organisationen, die diese Spezifikation implementieren, sind dafür verantwortlich, dass neben den in diesem Dokument beschriebenen Anforderungen auch alle geltenden rechtlichen, regulatorischen und betrieblichen Vorgaben erfüllt werden.