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

Indice FSR

Indice FSR

1. Introduzione

1.1 Scopo di questo Documento FSR

Questo documento sui Facility Security Requirements (FSR) rappresenta lo standard ufficiale TAPA per il deposito e il magazzinaggio in sicurezza. Si tratta di uno standard globale che può essere utilizzato negli accordi commerciali / di security tra i Clienti (Buyers) e i fornitori di servizi logistici (LSP) e/o altri soggetti che richiedono la certificazione.

Nello sviluppo di questo Standard, TAPA riconosce le molteplici differenze nel modo in cui i servizi di stoccaggio sono forniti a livello globale, regionale e anche all'interno delle aziende, e che l'FSR può essere applicato a tutti o a parte dei servizi forniti da un LSP/Richiedente. A seconda della complessità e delle dimensioni della supply chain, la conformità agli standard TAPA può essere ottenuta attraverso un singolo LSP/Richiedente o più LSP/Richiedenti e subappaltatori qualificati.

Ambito di Applicazione

TAPA ha sviluppato tre opzioni a supporto della certificazione:

- Certificazione di un singolo sito da parte di un Ente Certificatore (IAB).
- Certificazione multi-sito da parte dello IAB.
- Certificazione di self-audit da parte di Auditor Autorizzati (AA) da LSP/Richiedente o IAB.

Audience

Gli utilizzatori tipici degli standard TAPA sono:

- Clienti (Buyers)
- LSP/Richiedenti
- Forze dell'Ordine o altre organizzazioni governative
- Organizzazioni professionali della supply chain
- Assicuratori

1. Introduzione

1.2 Risorse per l'implementazione di TAPA FSR

Le risorse per soddisfare i requisiti del FSR sono sotto la responsabilità e a spese dell'LSP/Richiedente, a meno che non sia stato definito o concordato diversamente tra il Cliente (Buyer) e l'LSP/Richiedente.

1.3 Protezione delle linee di condotta e delle procedure del LSP

Le copie dei documenti relativi alle linee di condotta aziendali e alle procedure di security saranno presentate al Cliente (Buyer) solo in conformità agli accordi di divulgazione firmati tra LSP/richiedente e il Cliente (Buyer) e saranno trattate come informazioni riservate.

2. Riguardo TAPA

2.1 Obiettivo di TAPA

La criminalità a danno delle spedizioni è una delle maggiori sfide della supply chain per i fabbricanti di prodotti di valore e ad alto rischio e per i loro fornitori di servizi logistici.

La minaccia non proviene più solo da criminali occasionali. Oggi le organizzazioni criminali operano a livello globale e ~~utilizzano~~ compiono attacchi sempre più sofisticati contro veicoli, magazzini e personale per raggiungere i loro obiettivi.

TAPA è un forum che riunisce produttori globali, fornitori di servizi logistici, trasportatori di merci, Forze dell'Ordine e altre parti interessate con l'obiettivo comune di ridurre le perdite delle supply chain internazionali. L'obiettivo principale di TAPA è la prevenzione dei furti attraverso l'uso di informazioni in tempo reale e delle più recenti misure di prevenzione.

2.2 Mission di TAPA

La mission di TAPA è di aiutare a proteggere il patrimonio dei membri, riducendo al minimo le perdite di merci dalla supply chain. TAPA raggiunge questo obiettivo attraverso lo sviluppo e l'applicazione di standard di sicurezza globali, pratiche di settore riconosciute, tecnologia, formazione, benchmarking, collaborazione normativa e l'identificazione proattiva delle tendenze criminali e delle minacce alla sicurezza della supply chain.

3. Gli Standard TAPA

3.1 Gli Standard di Security TAPA

I seguenti standard globali di sicurezza di TAPA sono stati creati per garantire il trasporto e lo stoccaggio sicuro di merci ad alto valore e sono mirati alla prevenzione dei furti:

- I requisiti di sicurezza per i magazzini (FSR) rappresentano gli standard minimi specifici per il deposito sicuro, o lo stoccaggio in transito, all'interno della supply chain.
- I requisiti di sicurezza per gli automezzi (TSR) si concentrano esclusivamente sul trasporto via camion e rappresentano gli standard minimi specifici per il trasporto di prodotti su strada all'interno della supply chain.

Gli standard di sicurezza globali di TAPA vengono rivisti e aggiornati ogni tre anni in base alle necessità.

Il presente documento si riferisce esclusivamente ai requisiti FSR.

- Il processo di certificazione per TAPA FSR è descritto nel documento TAPA FSR Certification Framework
- Entrambe le versioni attuali del documento TAPA FSR e del documento TAPA FSR Certification Framework devono essere seguite per ottenere lo status di certificazione TAPA FSR.

3.2 Implementazione

Il successo nell'implementazione degli standard di security TAPA dipende dalla collaborazione tra LSP (Logistics Service Providers)/Richiedenti, Clienti (Buyers - Proprietari del carico) e Auditor autorizzati TAPA.

4. Linee guida legali

4.1 Ambito di Applicazione

L'FSR è uno Standard globale e tutte le sezioni dello Standard sono obbligatorie, a meno che non venga concessa un'eccezione attraverso la procedura di deroga ufficiale. (Si veda la Sezione 6.).

4.2 Traduzione

Nelle aree geografiche in cui l'inglese non è la prima lingua, e dove la traduzione è necessaria e applicabile, è responsabilità del LSP/Richiedente e dei suoi rappresentanti garantire che qualsiasi traduzione dell'FSR, o di qualsiasi sua parte, rifletta accuratamente le intenzioni di TAPA nello sviluppo e nella pubblicazione di questi Standard.

4.3 Il Marchio "TAPA"

"TAPA" è un marchio registrato della Transported Asset Protection Association e non può essere utilizzato senza l'espressa autorizzazione scritta di TAPA attraverso i suoi uffici regionali ufficialmente riconosciuti. Gli standard TAPA e il materiale associato sono pubblicati da e attraverso TAPA stessa e non possono essere rivisti o modificati da nessuno senza l'espressa autorizzazione scritta di TAPA. L'uso improprio del marchio TAPA può comportare la rimozione della certificazione o un'azione legale.

4.4 Limiti di Responsabilità

Con la pubblicazione di questi Standard, TAPA non fornisce alcuna garanzia o assicurazione che tutti gli eventi di furto della merce saranno evitati, indipendentemente dal fatto che gli Standard siano o meno pienamente utilizzati e correttamente implementati. Qualsiasi responsabilità che possa derivare da un furto di merce in deposito, o da qualsiasi altra perdita di merce in deposito, ai sensi degli Standard FSR, sarà a carico del LSP/Richiedente e/o del Cliente (Buyer) in conformità con i termini e le condizioni del contratto in essere tra loro e con le leggi o gli statuti che possono essere applicati nella giurisdizione in questione.

5. Contratti e Subappalti

5.1 Contratti

Il corretto e sicuro trasporto, lo stoccaggio e la movimentazione dei beni del Cliente (Buyer) sono di competenza del LSP/Richiedente, dei suoi rappresentanti e subappaltatori per tutta la durata della raccolta, del transito, dello stoccaggio e della consegna, come specificato in una liberatoria o in un contratto.

Se l'FSR è citato o incluso nel contratto tra l'LSP/Richiedente e il Cliente (Buyer), deve essere menzionato anche nel programma di security dell'LSP/Richiedente.

L'LSP/Richiedente deve fornire al Cliente (Buyer) la prova della certificazione FSR e, se del caso, la prova che i requisiti FSR siano stati soddisfatti. Inoltre, qualsiasi presunta mancata attuazione dei requisiti FSR da parte dell'LSP/Richiedente deve essere risolta secondo i termini del contratto negoziato tra il Cliente (Buyer) e l'LSP/Richiedente.

5.2 Subappalti

Il subappalto del carico include il requisito contrattuale per cui il subappaltatore dell'LSP/Richiedente soddisfi tutti gli standard FSR.

5.3 Verifica e soluzione dei reclami TAPA

Se TAPA riceve un reclamo formale relativo alle prestazioni di un LSP/Richiedente certificato, TAPA (soggetto che convalida) può richiedere che l'LSP/Richiedente sia sottoposto a un nuovo audit a spese dell'LSP/Richiedente stesso. Se l'LSP/Richiedente non supera l'audit o rifiuta di conformarsi a questo processo, il suo certificato può essere ritirato.

6. Deroghe

6. 1 Panoramica

Una deroga è un'approvazione scritta concessa per esentare una società da uno specifico requisito TAPA o per accettare una soluzione alternativa di conformità. Una deroga può essere richiesta se un LSP/Richiedente non è in grado di soddisfare un requisito specifico dell'FSR e può fornire misure alternative. Le deroghe sono valide per il periodo della certificazione.

Tutte le richieste di deroga per uno specifico requisito di sicurezza (parziale o totale) devono essere presentate tramite un modulo di richiesta di deroga TAPA (disponibile sul sito web TAPA) all'Ente di Certificazione (IAB)/Auditor Autorizzato (AA) da parte dell'LSP/Richiedente. L'LSP/Richiedente si assume la piena responsabilità dell'accuratezza delle informazioni fornite nella richiesta di deroga.

Ogni richiesta di deroga deve poi essere presentata attraverso lo IAB/AA al TAPA Regional Waiver Committee per l'approvazione. Spetta allo IAB/AA decidere se la richiesta è completa e se giustifica la presa in carico da parte di TAPA; ciò include la verifica di fattori di mitigazione e/o controlli di security alternativi.

Qualora i funzionari TAPA e/o i Clienti (Buyers) contestino che le condizioni di deroga siano cambiate, TAPA completerà un'indagine formale e l'LSP/Richiedente sarà consapevole del fatto che la deroga potrà essere revocata da TAPA.

.

6. 2 Processo Aziendale sulle Deroghe

Se un LSP non è in grado di soddisfare un requisito specifico nell'FSR, viene implementato il processo di deroga riportato di seguito.

Tabella 1: Responsabilità: Applicazione della deroga / Valutazione

Step	Responsibilità	Azione
1.	LSP/Richiedente	Stabilisce e verifica le misure di mitigazione.
2.	LSP/Richiedente	Compila il modulo di richiesta di deroga TAPA e lo invia allo IAB/AA.
3.	IAB/AA	Esamina e verifica l'integrità delle informazioni contenute nel modulo di richiesta di deroga TAPA.
4.	IAB/AA	Invia il modulo di richiesta di deroga TAPA al TAPA Regional Waiver Committee.
5.	TAPA Regional Waiver Committee	Rivede la richiesta e concede o nega la deroga.

6. Deroghe

Se la deroga è negata

Se il TAPA Regional Waiver Committee non approva la richiesta di deroga, l'LSP/Richiedente è tenuto ad implementare tutti i requisiti di security dell'FSR.

Se la deroga viene concessa

Se il TAPA Regional Waiver Committee approva la richiesta di deroga, verranno intraprese le seguenti azioni:

Tabella 2: Approvazione della Deroga

Step	Responsibilità	Azione
1.	TAPA Regional Waiver Committee	Documenta e firma le specifiche della deroga.
2.	TAPA Regional Waiver Committee	Specifica la durata di validità della deroga (fino a un massimo di tre anni) e ne invia una copia all'AA.
3.	AA	Notifica all'LSP/Richiedente l'esito della Richiesta di deroga.
4.	LSP/Richiedente	Soddisfa i requisiti per la deroga. In caso contrario, l'approvazione della deroga decade.

6.3 Deroghe per le Barriere fisiche (alla sezione 1) e per le Gabbie ad Alto Valore (HVC, alla sezione 4.5)

TAPA prenderà in considerazione una deroga a tutti o a parte dei requisiti sulla barriera perimetrale e/o sull'HVC se tutte le seguenti condizioni sono soddisfatte:

Generale:

- La richiesta di deroga viene presentata utilizzando il modulo ufficiale di richiesta deroga TAPA ed è approvata dallo IAB/AA.
- La richiesta di deroga include i dettagli di eventuali misure di mitigazione per garantire che le merci vulnerabili non siano esposte a rischi di furto o perdita non necessari.
- Una valutazione del rischio deve essere completata e presentata insieme alla richiesta di deroga. Eventuali vulnerabilità significative individuate nella valutazione del rischio devono essere elencate separatamente nella richiesta di deroga e devono essere intraprese azioni per ridurre il rischio a un livello accettabile.

Le misure di mitigazione devono essere implementate e documentate nella richiesta di deroga:

- **Barriere perimetrali:**
  - L'attrezzatura aggiuntiva, le risorse e le procedure introdotte per facilitare il rilevamento tempestivo di persone o veicoli non autorizzati possono includere, a titolo esemplificativo ma non esaustivo, illuminazione aggiuntiva, copertura delle telecamere a circuito chiuso (CCTV), procedure di controllo dell'identità di persone e veicoli, uniforme distintiva dell'LSP o uniforme distintiva solo nelle aree ad accesso limitato.
  - Devono essere installati segnali perimetrali visibili in lingua locale che indichino "Vietato l'accesso al personale non autorizzato", "Divieto di parcheggio non autorizzato".
  - Devono essere installati segnali visibili sulle porte o sulle pareti esterne delle baie di carico per istruire gli autisti, i visitatori, ecc. a procedere verso l'area appropriata per il controllo di security.
  - Confermare l'implementazione di procedure che garantiscano che le aree di movimentazione, spedizione e ricezione del carico siano ispezionate e conformi alle condizioni di deroga almeno settimanalmente.

- **HVC:**
  - Per le deroghe all'HVC, le azioni di mitigazione appropriate a minimizzare il rischio (nel caso in cui l'HVC non sia disponibile) devono essere esaminate e documentate nella valutazione del rischio annuale.
  - La richiesta di deroga comprende una dichiarazione allegata, firmata dall'LSP/richiedente, in cui si stabilisce che nessun Cliente (Buyer) richiede un HVC.

7. Requisiti di Facility Security

Sezione	Requisiti Generali	A	B	C
7.0				
7.0.1	Tutte le procedure o politicy aziendali richieste dal presente Standard devono essere documentate.	✔	✔	✔
7.0.2	Per le serrature, i badge di accesso e/o le chiavi che gestiscono e controllano le chiavi fisiche ed elettroniche è richiesta una procedura, un registro e/o un file di registrazioni delle chiavi.	✔	✔	✔

Sezione	Perimetro	A	B	C
7.1				
Piazzale Esterno del magazzino per la movimentazione, spedizione e ricezione della merce (Generale)				
7.1.1	CCTV in grado di visualizzare tutto il traffico nel piazzale esterno di movimentazione , spedizione e ricezione merci (inclusi i punti di entrata e di uscita) garantendo che tutti i veicoli e le persone siano sempre riconoscibili, a meno che non si presentino ostacoli temporanei dovuti a necessità operative (ad esempio, carico e scarico dei camion in tempo reale).	✔	✔	
7.1.2	Illuminazione adeguata nelle aree di carico e scarico. *Nota: L'illuminazione può essere costante, attivata da allarme, movimento, rilevamento del suono, ecc. con illuminazione immediata.*	✔	✔	✔
7.1.3	Procedura che descrive come i veicoli e le persone non autorizzate devono essere gestiti nel piazzale esterno di movimentazione, spedizione e ricezione della merce. Le istruzioni sulla procedura devono essere consegnate ai lavoratori interessati, comprese le guardie.	✔	✔	✔
7.1.4	Il piazzale per la movimentazione, spedizione e ricezione della merce è adeguatamente controllato per prevenire accessi non autorizzati.		✔	✔
7.1.5	Per le finestre accessibili al piano terra o le porte di carico, la valutazione annuale dei rischi deve valutare la necessità di barriere anti-ram. (Vedere Valutazione del rischio, Sezione 7.6.5.).	✔		
Barriere Fisiche				
7.1.6	La barriera fisica circonda il piazzale di movimentazione, spedizione e ricevimento merce.	✔		
7.1.7	La barriera fisica intorno al piazzale di movimentazione, spedizione e ricezione della merce ha un'altezza minima di 6 piedi / 1,8 metri. *Nota: La barriera fisica, progettata per impedire l'accesso non autorizzato, deve avere un'altezza di 6 piedi / 1,8 metri lungo tutta la sua lunghezza, comprese le aree in cui il livello del suolo cambia, cioè è inferiore.*	✔		

7.1.8	La barriera fisica intorno al piazzale di movimentazione, spedizione e ricezione della merce deve essere mantenuta in buone condizioni.	✔		
7.1.9	I cancelli all'interno del piazzale di movimentazione, spedizione e ricezione della merce sono presidiati o controllati elettronicamente.	✔		
7.1.10	La barriera fisica intorno al piazzale di movimentazione, spedizione e ricezione della merce viene ispezionata per verificarne l'integrità e i danni almeno una volta alla settimana.	✔		
Aree esterne delle ribalte				
7.1.11	Aree esterne delle ribalte coperte tramite telecamere a colori o "giorno/notte".	✔	✔	✔
7.1.12	Telecamere montate per poter visualizzare in ogni momento tutte le operazioni e i movimenti nell'area esterna delle baie di carico/scarico, a meno che non si presenti un'ostruzione temporanea dovuta a necessità operative (ad esempi, il carico e lo scarico dei camion in tempo reale).	✔	✔	✔
7.1.13	Tutti i veicoli e gli individui intorno alle aree esterne delle baie di carico/scarico sono chiaramente riconoscibili.	✔		
7.1.14	Veicoli e individui intorno alle aree esterne delle baie di carico/scarico visibili nella maggior parte dei casi.		✔	✔
7.1.15	Tutte le aree esterne intorno alle ribalte completamente illuminate.	✔	✔	✔
Accesso dei veicoli personali				
7.1.16	Veicoli personali ammessi alle aree di movimentazione, spedizione e ricezione della merce solo se pre approvati e limitati ad aree di parcheggio assegnate/designate. Nessun parcheggio personale è autorizzato nel raggio di 25 m dalle aree esterne delle ribalte. Devono essere in vigore i processi per la pre-approvazione e le restrizioni.	✔	✔	✔

Sezione	Pareti esterne, tetti e porte	A	B	C
7.2				
Lato esterno della struttura: CCTV				
7.2.1	Sistema di telecamere esterne a colori o "giorno/notte" che coprono tutti i lati esterni della struttura.	✔		
7.2.2	Sistema di telecamere esterne a colori o "giorno/notte" che coprono i lati esterni della struttuta su cui sono presenti porte, finestre o altre aperture.		✔	
7.2.3	La visuale del sistema di telecamere esterne è sempre libera, a meno che non si presenti un ostacolo temporaneo dovuto a necessità operative (ad es. Il carico e lo scarico del camion in tempo reale).	✔		
7.2.4	Tutti i veicoli e gli individui sono chiaramente riconoscibili dal sistema di telecamere esterne.	✔		
7.2.5	Veicoli e individui visibili nella maggior parte dei casi dal sistema di telecamere esterne.		✔	
Pareti esterne e tetto				

7.2.6	Pareti esterne e tetto progettati e mantenuti per resistere alla penetrazione (Esempio: mattone, blocco, lastra di calcestruzzo inclinata, pareti in pannelli a sandwich).	✔	✔	✔
7.2.7	Qualsiasi finestra apribile, presa d'aria o altra apertura nelle pareti esterne dell'edificio, o qualsiasi finestra sigillata installata a meno di 3 metri dal piano di lavoro sulle pareti esterne della struttura, deve avere una barriera fisica **oppure** essere allarmata e collegata al sistema di allarme principale.	✔	✔	
7.2.8	Qualsiasi finestra apribile, lucernario, presa d'aria, botola di accesso o altra apertura sul tetto della struttura, deve avere una barriera fisica **oppure** essere allarmata e collegata al sistema di allarme principale.	✔		
7.2.9	L'accesso esterno al tetto (scale) deve essere: Fisicamente bloccato e coperto da CCTV (telecamere a colori o "giorno/notte"). oppure Fisicamente bloccato e allarmato.	✔		
7.2.10	Accesso esterno al tetto (scale) fisicamente bloccato.		✔	✔
7.2.11	Tutte le porte esterne del magazzino e le porte degli uffici sono allarmate per rilevare l'apertura non autorizzata e collegate al sistema di allarme principale. *Nota: Le baie di carico/scarico non sono coperte da questo requisito, vedere la sezione 7.2.17 per i requisiti di allarme delle ribalte.*	✔	✔	✔
7.2.12	Ogni porta esterna del magazzino, porta dell'ufficio o altra apertura deve essere identificata in modo univoco per porta o per zona all'interno del sistema di allarme principale.	✔		
7.2.13	Tutte le porte esterne del magazzino sono sempre chiuse e bloccate quando non in uso. Chiavi/Codici sono controllati.	✔	✔	
7.2.14	Le porte e i passaggi pedonali del magazzino non possono essere facilmente violati. Se le cerniere /cardini sono all'esterno, devono essere bloccate o saldate a punti. Le porte in vetro sono inaccettabili a meno che non siano installati dei rilevatori di rottura del vetro, o che altri dispositivi di rilevamento locali forniscano una copertura (ad es. PIR) e allertino direttamente la centrale di controllo o che il vetro sia protetto da barre/reti.	✔	✔	✔
7.2.15	Le uscite di emergenza che sono utilizzate solo per scopi di emergenza (es.: uscite antincendio), sono sempre allarmate con un rilevatore acustico singolo o a zone.	✔	✔	
7.2.16	Tutte le baie di carico/scarico sono sufficientemente robuste in modo da scoraggiare e/o ritardare l'effrazione con l'uso di piccoli utensili portatili.	✔	✔	✔
7.2.17	**Baie di carico/scarico** **Orario non operativo:** Baie di carico/scarico chiuse, messe in sicurezza (cioè elettronicamente disattivate o fisicamente bloccate). Baie di carico/scarico allarmate per rilevare intrusioni non autorizzate e generare un allarme collegato al sistema di allarme principale.	✔	✔	✔

	Orario operativo: Le baie di carico/scarico devono essere chiuse quando non sono in uso. I cancelli retrattili (a forbice), se utilizzati, devono essere messi in sicurezza con un blocco meccanico ed essere alti almeno 8 piedi / 2,4 metri.			

Sezione	Varchi di accesso (ed uscita) uffici e magazzino	A	B	C
7.3				
Varco di accesso per i visitatori all'area uffici				
7.3.1	L'accesso attraverso la reception all'area uffici da parte dei visitatori è verificato da un dipendente/guardia/receptionist che è stato adeguatamente formato per il rilascio dei badge, i controlli, la registrazione, le visite, l'obbligo di accompagnamento, ecc. (processo messo in atto per le visite al di fuori dell'orario di lavoro).	✔	✔	✔
7.3.2	I varchi di accesso per i visitatori (reception) all'area uffici sono coperti da telecamere a circuito chiuso; (telecamere a colori o "giorno/notte") individui chiaramente riconoscibili in ogni momento.	✔	✔	
7.3.3	Allarme silente (panic button) presente in reception e testato settimanalmente.	✔	✔	
7.3.4	Tutti i visitatori dell'area uffici sono identificati tramite documento d'identità con foto (ad es. patente di guida, passaporto o carta d'identità nazionale, ecc.)	✔	✔	✔
7.3.5	Tutti i visitatori dell'area uffici sono registrati e il registro viene mantenuto per un minimo di 30 giorni.	✔	✔	✔
7.3.6	Tutti i badge dei visitatori devono essere riconciliati quando il visitatore lascia la sede e il registro completo deve essere controllato ogni giorno.	✔	✔	
7.3.7	Tutti i visitatori devono esporre in maniera visibile i badge o i pass e sono scortati dal personale dell'azienda.	✔	✔	
Varco di accesso della forza lavoro				
7.3.8	Il varco di accesso dipendenti è controllato 24 ore su 24, 7 giorni su 7.		✔	✔
7.3.9	Il varco di accesso dei dipendenti è controllato tramite un dispositivo elettronico di controllo accessi 24 ore su 24, 7 giorni su 7. Gli accessi sono registrati.	✔		
7.3.10	I varchi di accesso dei dipendenti sono coperti da telecamere a circuito chiuso. (Telecamere a colori o "giorno/notte").	✔	✔	
7.3.11	Dopo il controllo preliminare pre-assunzione, tutti i dipendenti devono essere muniti di un badge aziendale con foto.	✔	✔	
7.3.12	Tutti gli altri dipendenti devono essere muniti di un badge identificativo aziendale che li renda riconoscibili all'interno della struttura.	✔	✔	
7.3.13	Tutti i badge dei dipendenti devono essere chiaramente visibili.	✔	✔	

7.3.14	I badge dei dipendenti non devono essere condivisi in nessuna circostanza e deve essere in vigore una policy aziendale di rilascio dei badge.	✔	✔	
Identificazione dell'autista e del veicolo				
7.3.15	Tutti gli autisti vengono identificati tramite un documento d'identità con foto (ad es. patente di guida, passaporto o carta d'identità nazionale, ecc.) ed è mantenuto un registro degli autisti.	✔	✔	✔
7.3.16	Viene verificata la validità della patente di guida, che la foto del documento sia valida e che corrisponda all'autista.	✔	✔	✔
7.3.17	I dati identificativi del veicolo sono registrati manualmente (cioè in forma scritta) o tramite telecamere. Nella registrazione sono inclusi come minimo la targa e il tipo di veicolo.	✔		

Sezione	Interno uffici e magazzini	A	B	C
7.4				
Area Magazzino: Pareti in condivisione				
7.4.1	Le pareti interne, in condivisione dal pavimento al soffitto, e il tetto sono costruiti / progettati e mantenuti per resistere alla penetrazione (Esempio: mattoni, blocchi, lastre di calcestruzzo inclinate verso l'alto, pareti in pannelli a sandwich).	✔	✔	✔
7.4.2	Se le pareti interne, in condivisione dal pavimento al soffitto, sono costruite con reti metalliche di sicurezza o altre barriere di security riconosciute dal settore, allora è anche necessario che siano allarmate per rilevare eventuali intrusioni. *Nota: non sono accettabili reti, recinzioni di basso livello o reti non di sicurezza.*	✔	✔	✔
Aree di magazzino interne				
7.4.3	Il rilevamento intrusioni (ad es. infrarossi, movimento, suono o rilevamento vibrazioni), è necessario per monitorare le aree interne del magazzino. Gli allarmi devono essere attivati e collegati al sistema di allarme principale durante le ore non operative (cioè quando il magazzino è chiuso). *Nota: se il magazzino è operativo 24/7/366, questo requisito può essere N/A se i rischi e le relative mitigazioni sono documentati nella valutazione del rischio locale.* *Indipendentemente dagli orari di operatività, sono sempre richiesti il rilevamento delle intrusioni perimetrali o le barriere fisiche sulle porte esterne e sulle finestre al piano terra degli uffici e del magazzino. (Vedere la sezione 7.2.11).*	✔		
Ribalte interne e aree di carico/scarico				
7.4.4	Tutte le ribalte interne e le aree di carico/scarico sono coperte da telecamere a circuito chiuso. (Telecamere a colori o "giorno/notte").	✔	✔	✔
7.4.5	La visualizzazione delle merci che vengono caricate e scaricate in tutte le ribalte interne e nelle aree di carico/scarico, deve essere sempre chiara, a meno che non non si presenti un ostacolo temporaneo dovuto a necessità operative (ad es. carico e scarico del camion in tempo reale).	✔	✔	✔

7.4.6	I beni del Cliente (Buyer) sono sorvegliati al 100% da telecamere a circuito chiuso nelle aree di movimentazione del carico o nelle aree di sosta (ad esempio, aree per il disallestimento dei pallet, percorsi da e verso le scaffalature di stoccaggio, ribalta, corridoi di transito).	✔	✔	
Controllo degli accessi tra ufficio e magazzino				
7.4.7	Accesso controllato tra l'ufficio e la ribalta/magazzino.	✔	✔	
7.4.8	Gli allarmi delle porte accessibili tramite badge o intercomunicanti, tra l'ufficio e la ribalta/magazzino, sono udibili localmente **e** generano un allarme di risposta quando vengono tenute aperte per più di 60 secondi o immediatamente se forzate.	✔		
7.4.9	Gli allarmi delle porte tra l'ufficio e la ribalta/magazzino sono udibili localmente **o** inviano un allarme di risposta quando vengono tenute aperte per più di 60 secondi o aperte forzatamente.		✔	
7.4.10	I dipendenti autorizzati del LSP/Richiedente e i visitatori accompagnati possono accedere alle ribalte/aree di magazzino sulla base di necessità commerciali e limitate.	✔	✔	✔
7.4.11	L'elenco accessi alle aree di ribalta/magazzino deve essere rivisto almeno trimestralmente per limitare/verificare che il permesso di accesso sia garantito solo al personale designato/autorizzato.	✔	✔	
Gabbia ad Alto Valore (HVC) /Area				
7.4.12	Le dimensioni e l'uso della HVC possono essere dettati dall'accordo Cliente (Buyer)/LSP/Richiedente. Se non è presente un accordo, l'HVC deve essere in grado di immagazzinare un minimo di 6 metri cubi di merce.	✔	✔	
7.4.13	HVC/Area perimetrale è circondata da una gabbia o da pareti resistenti su tutti i lati, compreso il soffitto/tetto.	✔	✔	
7.4.14	Dispositivo di blocco/chiusura HVC/Area su porta/cancello.	✔	✔	
7.4.15	Copertura completa tramite telecamere a circuito chiuso (telecamere a colori o "giorno/notte") all'ingresso della HVC e nell'area interna. *Nota: Se l'HVC è troppo piccola per posizionare una telecamera all'interno, la copertura dell'ingresso è sufficiente.*	✔		
7.4.16	Copertura tramite telecamere a circuito chiuso (telecamere a colori o "giorno/notte") all'ingresso del'HVC.		✔	
7.4.17	Se è necessario l'accesso all'HVC a più di 10 persone, l'ingresso deve essere controllato elettronicamente tramite badge/chiave elettronica. Se l'accesso è richiesto a 10 o meno persone, un a serratura resistente o lucchetto è supportato da un sistema di gestione controllata delle chiavi. Le chiavi possono essere assegnate alle persone per coprire un turno, ma non devono essere cedute senza approvazione e devono essere registrate nel registro delle chiavi. Tutte le chiavi devono essere restituite e controllate quando non vengono utilizzate.	✔		

7.4.18	Le porte/cancelli della HVC sono allarmate per rilevare l'ingresso forzato. Gli allarmi possono essere generati tramite contatti alle porte e/o l'uso di rilevatori di movimento CCTV per rilevare accessi non autorizzati.	✔		
7.4.19	Il perimetro del HVC è mantenuto in buone condizioni e ispezionato mensilmente per verificarne l'integrità e i danni.	✔		
7.4.20	LSP/Richiedente si assicura che l'accesso all'HVC sia concesso solo al personale designato/autorizzato. L'elenco degli accessi autorizzati all'HVC è rivisto mensilmente e aggiornato in tempo reale quando un dipendente lascia il lavoro o il suo accesso non è più richiesto. Deve essere in vigore una procedura per l'accesso all'HVC.	✔	✔	
Ispezione dei rifiuti dal magazzino				
7.4.21	Le principali aree di raccolta dei rifiuti del magazzino, all'interno e/o all'esterno, sono monitorate da telecamere a circuito chiuso.	✔		
7.4.22	i sacchi della spazzatura, laddove vengono utilizzati, all'interno del magazzino sono trasparenti.		✔	✔
Pre-carico e stazionamento				
7.4.23	Non è consentito alcun pre-carico o parcheggio di veicoli FTL/dedicati del Cliente (Buyer) all'esterno della struttura del magazzino durante gli orari non operativi, a meno che non sia stato concordato tra il Cliente (Buyer) e l'LSP/Richiedente. Devono essere implementate misure di security alternative (ad es. dispositivi di sicurezza aggiuntivi sul container). *Nota: con "*all'esterno della struttura del magazzino*" si intendono quelle aree separate, lontane dall'edificio, ma sempre all'interno del piazzale/ recinzione perimetrale dell'LSP/Richiedente.*	✔	✔	✔
Contenitori personali e ispezioni in uscita				
7.4.24	Procedure di security scritte definiscono il modo in cui i "contenitori ed effetti personali" sono controllati all'interno del magazzino. I contenitori personali includono contenitori per il pranzo, zaini, borse frigo, borsoni, ecc.	✔	✔	
7.4.25	Se consentito dalla legge locale, l'LSP/Richiedente deve sviluppare e mantenere una procedura documentata per le ispezioni/ perquisizioni in uscita. L'attivazione della procedura è a discrezione dell'LSP/Richiedente e/o in base all'accordo Cliente (Buyer)/LSP/Richiedente. Come minimo, la procedura deve indicare il diritto dell'LSP/richiedente di compiere ispezioni e la necessità di introdurle quando queste normalmente non sono richieste (ad es. nel caso in cui un dipendente fosse sospettato di furto).	✔		
Controllo delle attrezzature di movimentazione delle merci				
7.4.26	Procedura che richiede che tutti i muletti e le altre attrezzature ad alimentazione utilizzate per la movimentazione della merce siano disabilitati durante le ore non operative. *Nota: non sono compresi i dispositivi di movimentazione a mano / transpallet.*	✔	✔	

Integrità del container o del rimorchio; ispezione in 7 punti				
7.4.27	L'ispezione in 7 punti deve essere effettuata su tutti i container o rimorchi in uscita dedicati al Cliente (Buyer): Parete anteriore, Lato sinistro, Lato destro, Pavimento, Soffitto/Tetto, Porte interne/esterne e meccanismo di chiusura, Esterno/Sotto Carro. *Nota: questo si applica a tutti i tipi di rimorchi e container chiusi e/o sigillati (cioè non solo ai container per il trasporto marittimo).*	✔	✔	✔
Processo di consegna merci; sigilli di sicurezza				
7.4.28	Salvo specifica esenzione da parte del Cliente (Buyer), i sigilli di sicurezza anti-manomissione sono utilizzati su tutte le spedizioni dirette e senza soste intermedie. I sigilli devono essere certificati secondo lo standard ISO 17712 (classificazione I, S o H). *Nota: i sigilli non sono richiesti su spedizioni con soste multiple, a causa della complessità e del rischio associato ai conducenti che trasportano più sigilli.*	✔	✔	✔
7.4.29	LSP/Richiedente deve disporre di procedure documentate per la gestione e il controllo dei sigilli di sicurezza, dei dispositivi di chiusura delle porte dei rimorchi (container), delle serrature a perno e di altre attrezzature di security.	✔	✔	✔
7.4.30	I sigilli di sicurezza vengono apposti o rimossi solo da personale autorizzato, cioè dal personale del magazzino, che viene istruito a riconoscere e segnalare i sigilli compromessi. I sigilli non devono mai essere apposti o rimossi dall'autista, a meno che non si tratti di un'esenzione del Cliente (Buyer).	✔	✔	✔
7.4.31	Procedure in vigore per il riconoscimento e la segnalazione di sigilli di sicurezza compromessi.	✔	✔	✔
Integrità del carico; Processo di convalida del carico/scarico				
7.4.32	Valide procedure in vigore per garantire che tutti i beni del Cliente (Buyer) spediti e ricevuti vengano controllati al momento della consegna mediante un conteggio manuale e/o elettronico dei colli. Il processo deve garantire che le anomalie siano sempre riconosciute, documentate e segnalate all'LSP/Richiedente e/o al Cliente (Buyer). Le registrazioni manuali e/o elettroniche devono essere di tipo probatorio. Se gli autisti non sono presenti per assistere a questa attività, il Cliente (Buyer)/LSP/Richiedente deve garantire una verifica alternativa del conteggio, come scansioni e/o immagini CCTV, raccolte e conservate appositamente per questo scopo. *Nota: Oltre ai colli mancanti, le anomalie possono includere danni, cinghie o nastro mancanti, tagli o altre aperture evidenti, che indicano un possibile furto o sottrazione.*	✔	✔	✔
Pick-up fraudolenti				
7.4.33	L'identità dell'autista del camion, la documentazione per il ritiro del carico e i dettagli di pre-alert specificati dal Cliente (Buyer) sono verificati prima del carico. La procedura deve essere in vigore.	✔	✔	✔

Sezione	Sistemi di sicurezza; progettazione, monitoraggio e risposte	A	B	C
7.5				
Centrale di controllo				
7.5.1	Monitoraggio degli eventi di allarme 24x7x366 tramite una centrale di controllo interna o esterna di terze parti, protetta da accessi non autorizzati. *Nota: le centrali di controllo possono essere situate all'interno o all'esterno del sito e possono essere di proprietà dell'azienda o di terzi. In tutti i casi, l'accesso deve essere controllato attraverso l'uso di un sistema elettronico di controllo degli accessi (badge), serrature o scanner biometrici.*	✔	✔	✔
7.5.2	La centrale di controllo risponde a tutti gli allarmi dell'impianto di sicurezza in tempo reale 24x7x366.	✔	✔	✔
7.5.3	La centrale di controllo acquisisce l'attivazione dell'allarme e si attiva in meno di 3 minuti.	✔	✔	✔
7.5.4	Sono disponibili rapporti di monitoraggio degli allarmi.	✔	✔	✔
7.5.5	Procedure di monitoraggio post risposta in vigore.	✔	✔	✔
Sistema di rilevamento intrusioni (IDS)				
7.5.6	Tutti gli IDS vengono attivati durante le ore non operative e collegati al sistema di allarme principale.	✔	✔	✔
7.5.7	Mantenimento delle registrazioni degli allarmi IDS per 60 giorni.	✔	✔	
7.5.8	Le registrazioni degli allarmi IDS sono conservate in modo sicuro e ne viene fatto il backup.	✔		
7.5.9	Le registrazioni degli allarmi IDS sono conservate in modo sicuro.		✔	
7.5.10	Procedura per garantire che l'accesso agli IDS sia limitato alle persone autorizzate o agli amministratori di sistema. Ciò include server, console, controller, pannelli, reti e dati. Le autorizzazioni di accesso devono essere prontamente aggiornate quando i dipendenti lasciano l'organizzazione o cambiano ruolo, non richiedendone più l'accesso.	✔	✔	✔
7.5.11	Allarme trasmesso in caso di interruzione/mancanza di corrente dell'IDS. *Nota: Per i sistemi con UPS (Uninterrupted Power Supply), l'allarme viene trasmesso in caso di guasto della batteria dell'UPS.*	✔	✔	✔
7.5.12	Verifica funzionalità degli allarmi IDS in essere. *Nota: procedure che convalidano l'attivazione degli allarmi durante le ore non operative.*	✔	✔	✔

7.5.13	Allarme IDS trasmesso da linea fissa sull'apparecchio e/o guasto della linea.	✔	✔	
7.5.14	Sistema di comunicazione di backup in essere sul dispositivo IDS e/o guasto della linea.	✔	✔	
Sistema di controllo automatico degli accessi (AACS)				
7.5.15	Le registrazioni delle transazioni AACS sono disponibili per 90 giorni. Le registrazioni sono archiviate in modo sicuro; effettuato il backup.	✔	✔	
7.5.16	Procedura per garantire che l'accesso ad AACS sia limitato alle persone autorizzate o agli amministratori di sistema. Le autorizzazioni di accesso devono essere prontamente aggiornate quando gli individui lasciano l'organizzazione o cambiano ruolo, non richiedendone più l'accesso.	✔	✔	
7.5.17	I rapporti del sistema di accesso sono esaminati almeno trimestralmente per identificare irregolarità o usi impropri (ad es. tentativi multipli non riusciti, letture false (ad es. carta disattivata), prove di condivisione della carta per consentire l'accesso non autorizzato, ecc.). Processo in vigore.	✔	✔	
Telecamere a Circuito Chiuso (CCTV)				
7.5.18	Registrazione digitale delle telecamere a circuito chiuso in essere.	✔	✔	✔
7.5.19	La velocità di registrazione per le CCTV è impostata come minimo per 8 fotogrammi al secondo (fps) per telecamera. *Nota: TAPA consentirà ai detentori di certificazione ancora in corso di validità e che non hanno la possibilità di passare a 8 fps, di continuare con i 3 fps esistenti fino alla revisione del 2023. I detentori di nuova certificazione devono soddisfare il nuovo requisito.*	✔	✔	✔
7.5.20	La funzionalità relativa alla registrazione digitale viene controllata quotidianamente nei giorni operativi tramite procedura. Registrazioni disponibili.	✔	✔	✔
7.5.21	Le registrazioni delle telecamere a circuito chiuso sono conservate per un minimo di 30 giorni, ove consentito dalla legge locale. LSP/Richiedente deve fornire la prova di eventuali leggi locali che vietano l'uso di CCTV e/o limitano la conservazione dei dati video a meno di 30 giorni.	✔	✔	✔
7.5.22	Accesso strettamente controllato al sistema CCTV, inclusi hardware, software e archiviazione dati/video.	✔	✔	✔
7.5.23	Le immagini delle telecamere a circuito chiuso, per motivi di security, vengono visualizzate solo da personale autorizzato.	✔	✔	✔
7.5.24	Procedure in vigore che descrivono in dettaglio la politica aziendale di protezione dei dati delle telecamere a circuito chiuso, per quanto riguarda l'utilizzo di immagini in tempo reale e la loro conservazione in conformità con le leggi locali.	✔	✔	
Illuminazione esterna e interna				

7.5.25	I livelli di illuminazione esterna e interna sono sufficienti a supportare le immagini delle telecamere a circuito chiuso che consentono investigazioni e registrazioni di tipo probatorio.	✔	✔	
7.5.26	I livelli di illuminazione esterna e interna sono sufficienti per riconoscere chiaramente tutti i veicoli e gli individui.	✔		

Sezione	Formazione e procedure	A	B	C
7.6				
Procedure di Escalation				
7.6.1	Procedure locali in vigore per la gestione dei beni del Cliente (Buyer), compreso il processo per la segnalazione tempestiva di perdita, scomparsa o furto dei beni del Cliente (Buyer). Gli incidenti devono essere segnalati da LSP/Richiedente al Cliente (Buyer) entro 24 ore. Furti evidenti devono essere segnalati immediatamente. Il processo deve essere seguito in modo puntuale.	✔	✔	✔
7.6.2	I contatti di emergenza di Cliente (Buyer) e LSP/Richiedente per gli incidenti di security sono riportati in un elenco e disponibili. L'elenco è aggiornato ogni 6 mesi e comprende i contatti di emergenza delle Forze dell'Ordine.	✔	✔	✔
Impegno della Direzione				
7.6.3	La Direzione aziendale del fornitore deve aver nominato formalmente una persona per la security in loco che sia responsabile del mantenimento di TAPA FSR e dei requisiti di security della supply chain aziendale. Il fornitore deve anche avere una persona (può essere la stessa) responsabile del monitoraggio del programma FSR. Ciò include la programmazione dei controlli di conformità, le comunicazioni con gli AA, la ricertificazione, le modifiche allo standard FSR, ecc. *Nota: Queste persone possono essere un dipendente o una persona esterna con contratto per svolgere questo ruolo.*	✔	✔	✔
7.6.4	La Direzione deve sviluppare, comunicare e mantenere una politica di security per garantire che tutte le persone interessate (cioè dipendenti e subcontractor) siano chiaramente consapevoli delle aspettative del fornitore sulla security.	✔	✔	✔
7.6.5	Una valutazione dei rischi della struttura, che riconosca la probabilità e l'impatto degli eventi relativi alla security, deve essere condotta/aggiornata almeno una volta all'anno. Il processo di Valutazione dei Rischi deve richiedere alla Direzione di prendere decisioni basate su informazioni circa la vulnerabilità e la mitigazione del rischio stesso. Devono essere valutati almeno i seguenti eventi comuni interni/esterni: furto della merce o delle informazioni, accesso non autorizzato alle strutture o alla merce, manomissione o distruzione dei sistemi di security, prelievo fittizio del carico, continuità della sicurezza in caso di carenza di forza lavoro, disastri naturali, ecc. Altri eventi possono essere presi in considerazione in base ai rischi locali/ nazionali.	✔	✔	✔
Formazione				
7.6.6	Formazione sulla security / sensibilizzazione alle minacce da fornire a tutti i dipendenti nei primi 60 giorni di lavoro e successivamente ogni 2 anni.	✔	✔	✔

7.6.7	La formazione sulla sicurezza delle informazioni si focalizza sulla protezione dei dati di spedizione, elettronici e fisici, del Cliente (Buyer) e viene erogata ai dipendenti che hanno accesso alle informazioni del Cliente (Buyer).	✔	✔	
Accesso ai beni della Cliente (Buyer)				
7.6.8	Procedure in vigore per proteggere i beni del Cliente (Buyer) (cioè il carico) da accessi non autorizzati da parte di dipendenti, visitatori, ecc.	✔	✔	
Informazioni di Controllo				
7.6.9	Accesso ai documenti di spedizione e alle informazioni sui beni del Cliente (Buyer) controllato in base alla "necessità di sapere".	✔	✔	✔
7.6.10	Accesso ai documenti di spedizione e alle informazioni sui beni del Cliente (Buyer) monitorato e registrato.	✔	✔	✔
7.6.11	Documenti di spedizione e informazioni sui beni del Cliente (Buyer) salvaguardati fino alla distruzione.	✔	✔	✔
Segnalazione di incidenti di security				
7.6.12	Sistema di segnalazione e tracciamento degli incidenti di security in vigore, utilizzato per implementare misure proattive.	✔	✔	
Programmi di manutenzione				
7.6.13	Programmi di manutenzione in essere per tutte le installazioni/sistemi tecnici (fisici) di security, volti a garantirne la funzionalità in ogni momento (ad es. CCTV, controllo accessi, rilevamento intrusioni e illuminazione).	✔	✔	✔
7.6.14	Manutenzione preventiva effettuata una volta all'anno o secondo le specifiche del produttore.	✔	✔	✔
7.6.15	Verifiche di funzionalità di tutti i sistemi una volta alla settimana e documentate, a meno che il guasto al sistema non venga immediatamente / automaticamente segnalato, anche tramite allarme.	✔	✔	
7.6.16	Un ordine di riparazione deve essere avviato entro 48 ore dalla scoperta del guasto. Per le riparazioni che si prevede superanno le 24 ore, devono essere implementate misure di mitigazione alternative.	✔	✔	
Orientamento del Contraente				
7.6.17	L'LSP/Richiedente garantisce che tutti i subappaltatori/fornitori siano a conoscenza e si conformino ai programmi di security pertinenti dell'LSP/Richiedente.	✔	✔	✔
Registrazioni di spedizione e ricezione				
7.6.18	I documenti di spedizione e ricezione sono leggibili, completi e precisi (ad es. ora, data, firme, autista, personale addetto alla spedizione e al ricevimento, dettagli della spedizione e quantità, ecc.)	✔	✔	✔
7.6.19	LSP/richiedente deve conservare i registri di tutti i ritiri e le prove delle consegne, per un periodo non inferiore a due anni, e metterli a disposizione delle indagini sulle perdite, se necessario.	✔	✔	✔
7.6.20	La prova di consegna deve essere fornita come da accordi esistenti tra il Cliente (Buyer) e l'LSP/Richiedente. Ove richiesto dal Cliente (Buyer), a destino si deve	✔	✔	✔

	notificare l'origine entro il termine concordato dell'avvenuta ricezione della spedizione, verificando la corrispondenza dei dati.			
Processo di pre-alert				
7.6.21	Laddove il Cliente (Buyer) lo richieda, è in vigore il processo di pre-alert applicato alle spedizioni in entrata e/o in uscita. I dettagli del pre-alert devono essere concordati tra Cliente (Buyer) e LSP/Richiedente. I dettagli suggeriti includono: orario di partenza, orario di arrivo previsto, società di trasporto, nome del conducente, dettagli della targa, informazioni sulla spedizione (numero di colli, peso, lettera di vettura, ecc.) e numero del sigillo del rimorchio.	✔	✔	✔

Sezione	Integrità della forza lavoro	A	B	C
7.7				
7.1	Controllo/verifica/background check (come consentito dalla legge locale)			
7.7.1	L'LSP/Richiedente deve avere un processo di controllo / verifica / background check che includa, come minimo, controlli sul passato lavorativo e sui precedenti penali. Il controllo/verifica si applica a tutti i candidati, inclusi i dipendenti e i subcontractors. L'LSP/Richiedente richiederà anche un processo equivalente da applicare presso le aziende che forniscono lavoratori TAS (somministrati).	✔	✔	✔
7.7.2	Il lavoratore TAS è tenuto a firmare una dichiarazione in cui afferma di non avere alcuna condanna penale in corso e di rispettare le procedure di security dell'LSP/Richiedente.	✔	✔	✔
7.7.3	LSP/Richiedente avrà stipulato accordi affinchè l'agenzia e/o il subcontractor che fornisce i lavoratori TAS condivida le informazioni di base sul controllo / verifica / background check oppure l'LSP/Richiedente condurrà esso stesso tali controlli. Il controllo deve includere la verifica dei precedenti penali e dei precedenti impieghi.	✔	✔	✔
7.7.4	Procedura per la gestione della falsa dichiarazione da parte del candidato/dipendente prima e dopo l'assunzione.	✔	✔	✔
Cessazione del rapporto di lavoro o riassunzione *Nota: La cessazione del rapporto di lavoro comprende sia le separazioni volontarie che involontarie - licenziamento e dimissioni del dipendente.*				
7.7.5	Ritiro dei beni fisici aziendali dei dipendenti che terminano il rapporto di lavoro, inclusi gli ID aziendali, i badge di accesso, le chiavi, le attrezzature o le informazioni sensibili. È richiesta una procedura documentata.	✔	✔	✔
7.7.6	Protezione dei dati del Cliente (Buyer): interrompere l'accesso dei dipendenti che terminano il rapporto di lavoro ai sistemi fisici o elettronici contenenti dati del Cliente (Buyer) (inventario o programmi). Procedura richiesta.	✔	✔	✔
7.7.7	Check list in vigore per la verifica.	✔	✔	✔
7.7.8	Riassunzione: Sono in vigore procedure per evitare all'LSP/Richiedente di riassumere un dipendente se i criteri di rifiuto / licenziamento sono ancora validi.	✔	✔	✔

	Nota: le registrazioni vengono esaminate prima della ri-assunzione (es.: background del personale precedentemente licenziato o di candidati rifiutati (cui precedentemente è stato negato l'impiego).			

8. Requisiti della Funzione Centrale (applicabile solo per le certificazioni multi-sito)

Sezione	Funzione Centrale	A	B	C
8.1	**Generale**			
8.1.1	E' presente una funzione centrale per la gestione del sistema di security per tutti i siti, come definito nell'ambito della certificazione multi-sito.	✔	✔	✔
8.1.2	Tutti i siti devono avere un rapporto legale o contrattuale con la funzione centrale.	✔	✔	✔
8.1.3	E' istituito un unico sistema di gestione della security per garantire che tutti i siti soddisfino i requisiti dello standard di security TAPA applicabile.	✔	✔	✔
8.1.4	La funzione centrale e il suo sistema di gestione sono soggetti ad audit interni per garantire la conformità continuativa agli standard TAPA.	✔	✔	✔
8.1.5	La funzione centrale effettua audit dei vari siti per garantire che il sistema di gestione della security soddisfi i requisiti della normativa di riferimento e sia in grado di raggiungere i risultati previsti in tutti i siti coinvolti. Gli audit devono essere effettuati con i modelli di audit TAPA appropriati.	✔	✔	✔
8.1.6	La funzione centrale ha l'autorità e il diritto di richiedere che tutti i siti siano conformi agli standard di security TAPA e di implementare azioni correttive e preventive secondo necessità. *Nota: ove applicabile, ciò deve essere stabilito nell'accordo formale tra la funzione centrale e i siti.*	✔	✔	✔
8.2	**Politiche e procedure**			
8.2.1	La funzione centrale mantiene politiche aziendali e procedure documentate per i suoi sistemi di gestione della security, applicabili a tutti i suoi siti.	✔	✔	✔
8.2.2	La funzione centrale assicura che le politiche e le procedure siano aggiornate, comunicate, rese fruibili e applicate in modo appropriato da tutti i siti come richiesto.	✔	✔	✔
8.2.3	Le politiche e le procedure devono essere aggiornate e facilmente accessibili da tutti i siti come richiesto.	✔	✔	✔
8.3	**Rapporto di self-audit effettuato per tutti i siti**			
8.3.1	La funzione centrale incarica tutti i siti di effettuare un self-audit e tutti i report con i risultati devono essere inviati alla funzione centrale per le registrazioni e le revisioni.	✔	✔	✔
8.3.2	La funzione centrale garantisce che tutte le SCAR dei self-audit e degli audit siano adeguatamente chiuse per migliorare i propri sistemi di gestione della security.	✔	✔	✔
8.3.3	Tutti i siti devono inviare alla funzione centrale aggiornamenti sullo stato di avanzamento e report su tutte le SCAR in sospeso. La funzione centrale deve fare escalation con la Direzione dell'LSP/Richiedente se le SCAR non vengono completate prima della data di scadenza.	✔	✔	✔

8.4	**Registrazioni delle ispezioni, registri (registro visitatori, registro conducenti), ispezione in 7 punti**			
8.4.1	La funzione centrale deve disporre di procedure per garantire che tutti i siti conservino i registri delle ispezioni, i registri visitatori, i registri conducenti e le ispezioni in 7 punti, ecc.	✔	✔	✔
8.5	**Valutazione del rischio di tutti i siti**			
8.5.1	La funzione centrale deve disporre di procedure per garantire che in tutti i siti siano effettuate valutazioni dei rischi, che questi ultimi vengano gestiti adeguatamente e che siano conservate le relative registrazioni.	✔	✔	✔
8.6	**Layout CCTV (videosorveglianza) ed antintrusione dei siti**			
8.6.1	La funzione centrale deve disporre di procedure che garantiscano che tutti i siti esaminino e mantengano i documenti relativi al layout di tutti i sistemi di sicurezza fisica come le telecamere a circuito chiuso e il sistema antintrusione.	✔	✔	✔
8.7	**Registrazioni di allarme e controllo accessi**			
8.7.1	La funzione centrale deve disporre di procedure che garantiscano che tutti i sistemi di allarme e di controllo degli accessi siano mantenuti e testati per assicurare la loro efficacia operativa.	✔	✔	✔
8.7.2	La funzione centrale deve disporre di procedure che consentano a tutti i siti di conservare le registrazioni di tutti i test e gli incidenti relativi a rilevamento intrusioni e controllo accessi.	✔	✔	✔
8.8	**Registrazioni della formazione**			
8.8.1	La funzione centrale deve disporre di procedure per garantire che tutti i siti mantengano adeguati registri sulla formazione dei propri dipendenti in materia di gestione della security.	✔	✔	✔
8.8.2	La funzione centrale deve disporre di procedure per garantire che tutti i siti mantengano registri di formazione sulla security per tutto il personale del sito.	✔	✔	✔
8.9	**Registrazioni dei controlli/verifiche**			
8.9.1	La funzione centrale deve disporre di procedure per garantire che tutti i siti effettuino controlli e verifiche dei registri a intervalli regolari al fine di assicurare l'integrità e l'efficacia del sistema di gestione della security.	✔	✔	✔
8.9.2	La funzione centrale deve disporre di procedure per garantire la registrazione dei dati delle revisioni, compresi i rilievi e le azioni correttive/preventive 8.1.6. che devono essere conservati.	✔	✔	✔
8.10	**Riesame della Direzione per valutare i self-audit, SCAR rilevate, eventuali perdite, furti e valutazioni del rischio.**			
8.10.1	La funzione centrale effettua un Riesame della Direzione periodico per garantire la conformità, l'efficacia e il miglioramento dei propri sistemi di gestione della security.	✔	✔	✔
8.10.2	I Riesami della Direzione riguardano, tra l'altro, l'efficacia dei self-audit, le chiusura delle SCAR, le valutazioni dei rischi, gli incidenti e le azioni di miglioramento.	✔	✔	✔
8.10.3	La funzione centrale conserva le registrazioni di tutti i Riesami della Direzione.	✔	✔	✔

9. Minaccia IT e Cyber Security – Requisito opzionale

FSR include requisiti opzionali per quanto riguarda le minacce alla sicurezza informatica che necessitano di un livello di protezione più elevato e possono essere utilizzati in aggiunta agli altri moduli. Questo requisito opzionale è destinato ad essere selezionato dall'LSP/Richiedente e/o dal suo Cliente (Buyer) come requisito aggiuntivo per le sue esigenze di sicurezza operativa. Quando questa parte viene selezionata nella valutazione pre-certificativa per far parte dell'audit di certificazione, tutti i requisiti diventano obbligatori.

Sezione	Minaccia IT e Cyber Security – Requisito opzionale
9.	***Requisiti obbligatori***
9.1	L'LSP/Richiedente deve disporre di policy di security per l'IT e le minacce informatiche. Le policy possono essere separate o in un documento unico. Le policy devono spiegare:- 1. Le azioni dell'LSP/Richiedente per identificare e rispondere alle minacce. 2. Le politiche e le procedure in vigore per proteggere, rilevare, testare e rispondere agli eventi relativi alla security. 3. I metodi per il ripristino dei sistemi informatici e/o dei dati. 4. Il protocollo di comunicazione ai Clienti (Buyers) per mitigare l'impatto sulla supply chain entro 24 ore dall'avvenuta conoscenza dell'incidente. 5. Il modo in cui le politiche aziendali vengono riviste annualmente e aggiornate in modo appropriato.
9.2	L'LSP/Richiedente deve avere un programma di formazione sulla sicurezza delle informazioni da erogare a tutti i dipendenti. Questa formazione deve: - 1. Informare circa i ruoli e le responsabilità che gli utenti di un pc hanno nel mantenere la security e i benefici ad essa associati. 2. Disporre di un sistema che garantisca che le registrazioni delle persone che ricevono la formazione siano conservate per un minimo di 2 anni.
9.3	L'LSP/Richiedente deve disporre di una policy aziendale scritta per garantire che le misure di Cyber Security siano vigore presso i subappaltatori e/o fornitori al fine di assicurare: 1. Che i requisiti di Cyber Security dell'LSP/Richiedente siano comunicati ai subappaltatori e/o ai fornitori e integrati negli accordi. 2. Che qualora i subappaltatori e/o i fornitori non riconoscano o rifiutino di adottare i requisiti di Cyber Security degli LSP/Richiedenti, vengano documentate e messe in atto misure al fine di mitigare i rischi secondo i requisiti di Cyber Security degli LSP/Richiedenti e dei loro clienti.
9.4	L'LSP/Richiedente deve disporre di un piano di mitigazione per le interruzioni di corrente (ad es. alimentazione elettrica alternativa o generatore di backup), che garantisca l'afflusso di energia elettrica verso i sistemi IT critici (identificati nella valutazione del rischio locale) per un minimo di 48 ore.
9.5	I sistemi informatici dell'LSP / Richiedente devono avere installato un software antivirus e anti-malware con licenza. Il software antivirus e anti-malware deve contenere gli ultimi aggiornamenti.
9.6	L'LSP / Richiedente deve disporre di un adeguato piano di disaster recovery IT (DRP) per il ripristino del sistema compromesso da attacchi, inclusi, a titolo esemplificativo ma non esaustivo, tutte le informazioni e i software necessari per il backup e il recupero dei dati.
9.7	È necessario eseguire il backup dei sistemi informatici dell'LSP/Richiedente. Tali backup devono essere testati regolarmente e i dati di backup devono essere crittografati e trasferiti in un luogo secondario, fuori sede.

9.8	L'LSP/Richiedente deve implementare una policy per tutti gli account degli utenti per gestire e controllare l'accesso ai Sistemi Informatici utilizzando identificatori individuali unici e password sicure. Devono essere messe in atto procedure per garantire: 1. Programma di verifica della conformità delle password. 2. Una password unica iniziale deve essere assegnata ad ogni nuovo account al momento della creazione. 3. Le password iniziali non possono contenere il nome dell'utente, il numero di identificazione o seguire uno schema standard basato sulle informazioni dell'utente. 4. Le password saranno comunicate agli utenti in modo sicuro e solo dopo la convalida dell'identità dell'utente. 5. Gli utenti devono essere tenuti a cambiare le password al momento del login iniziale. 6. Le password devono essere cambiate almeno ogni 90 giorni.

Publishing and copyright information

The TAPA copyright notice displayed in this document indicates when the document was last issued.

Publication history

First published in January 2020

First (present) edition published in January 2020

This Publicly Available Specification comes into effect on 1st July 2020