



Transported Asset Protection Association

FSR 2026

TAPA Global Standard



TAPA Americas

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

www.tapaonline.org

TAPA Asia Pacific

Oxley BizHub 2
62 Ubi Road 1, #06-11
Singapore 408734

www.tapa-apac.org

TAPA EMEA

Kanaalpark 140
2321 JV Leiden
The Netherlands

www.tapaemea.org

TAPA Copyright © Do Not Copy

Spis treści

1.0 Wprowadzenie	5
1.1 Cel niniejszego dokumentu FSR.....	5
1.2 Zasoby do wdrożenia TAPA FSR.....	5
1.3 Ochrona polityk i procedur LSP	5
2.0 O TAPA	6
2.1 Cel TAPA	6
2.2 Misja TAPA	6
3.0 Standardy TAPA	7
3.1 Standardy bezpieczeństwa TAPA.....	7
3.2 Wdrożenie	7
4.0 Wytoczne prawne.....	8
4.1 Zakres.....	8
4.2 Tłumaczenie.....	8
4.3 Marka „TAPA”	8
4.4 Ograniczenie odpowiedzialności.....	8
5.0 Umowy i podwykonawstwo	9
5.1 Umowy	9
5.2 Podwykonawstwo	9
5.3 Badanie skarg i ich rozpatrywanie przez TAPA	9
6.0 Odstępstwa	10
7.0 Wymagania Bezpieczeństwa Obiektu	11
S1. Wymagania ogólne	11
S2. Ochrona terenu zewnętrznego	13
2.1 Zewnętrzny obszar obsługi ładunków magazynu, wysyłki i przyjęć.....	13
2.2 Bariery fizyczne	13
2.3 Zewnętrzne obszary doków.....	14
2.4 Dostęp pojazdów prywatnych.....	15
S3. Ściany zewnętrzne, dach i drzwi.....	16
3.1 Zewnętrzne strony obiektu: CCTV / VSS	16
3.2 Ściany zewnętrzne i dach.....	16
S4. Wejścia i wyjścia do biura oraz magazynu	19
4.1 Punkty wejścia dla odwiedzających w obszarze biurowym	19
4.2 Workforce Entry Point(s)	20
4.3 Identyfikacja kierowcy i pojazdu	20
S5. Wnętrze magazynu i biura	22
5.1 Warehouse Area: Multi-Tenant Walls.....	22

5.2	Internal Warehouse Areas.....	22
5.3	Wewnętrzne bramy dokowe i obszary doków	23
5.4	Kontrola dostępu między biurem a dokiem/magazynem	23
5.5	Obszar ładunków o wysokiej wartości (HVC).....	24
5.6	Kontrola odpadów z magazynu	25
5.7	Przedładunek i strefa przygotowania	25
5.8	Kontrola przedmiotów osobistych i przeszukania przy wyjściu	26
5.9	Kontrola sprzętu do obsługi ładunków	26
5.10	Integralność kontenera lub naczepy: kontrola 7-punktowa	26
5.11	Freight Handover Process; Security Seals	27
5.12	Integralność ładunku; proces weryfikacji załadunku/rozładunku.....	27
5.13	Oszukańcze odbiory ładunku.....	28
S6.	Systemy bezpieczeństwa: projektowanie, monitorowanie i reagowanie.....	29
6.1	Stanowisko monitoringu	29
6.2	Intruder Detection System (IDS)	29
6.3	Automatyczny system kontroli dostępu (AACs).....	30
6.4	CCTV/ VSS.....	31
6.5	Oświetlenie zewnętrzne i wewnętrzne	32
S7.	Szkolenia i procedury	33
7.1	Procedury eskalacji	33
7.2	Zaangażowanie kierownictwa	33
7.3	Szkolenie	33
7.4	Dostęp do aktywów Nabywcy.....	34
7.5	Kontrola informacji.....	34
7.6	Raportowanie incydentów bezpieczeństwa	34
7.7	Programy utrzymania (konserwacji).....	35
7.8	Szkolenie wstępne dla podwykonawców	35
7.9	Dokumentacja wysyłek i przyjęć.....	35
7.10	Proces pre-alert musi być wdrożony	36
S8.	Integralność personelu.....	37
8.1	Weryfikacja / sprawdzanie / kontrole przeszłości (w zakresie dozwolonym przez prawo lokalne) 37	
8.2	Zakończenie zatrudnienia lub ponowne zatrudnienie pracowników	37
S9.	Wymagania dotyczące funkcji centralnej (dotyczy wyłącznie certyfikacji wielooddziałowej).....	39
9.1	Postanowienia ogólne	39
9.2	Polityki i procedury	40
9.3	Raport z audytu samooceny przeprowadzany dla wszystkich lokalizacji	40
9.4	Rejestry inspekcji, dzienniki (rejestry odwiedzających/kierowców), kontrole 7-punktowe	41
9.5	Ocena ryzyka dla wszystkich lokalizacji.....	41
9.6	Układ CCTV/VSS i systemu alarmowego obiektu.....	41
9.7	Rejestry systemów alarmowych i kontroli dostępu.....	41
9.8	Rejestry szkoleń	42
9.9	Rejestry weryfikacji / sprawdzania	42
9.10	Przegląd zarządzania w celu oceny samoaudytów; zgłoszonych SCAR; strat, kradzieży; ocen ryzyka	42
8.0	Zagrożenia IT i cyberbezpieczeństwa – opcja rozszerzona	43
E8.	Wymagania obowiązkowe	43

1.0 Wprowadzenie

1.1 Cel niniejszego dokumentu FSR

Niniejszy dokument Wymagań Bezpieczeństwa Obiektu (FSR) stanowi oficjalny standard TAPA dotyczący bezpiecznego magazynowania i składowania. Jest to wspólny globalny standard, który może być wykorzystywany w umowach biznesowych/bezpieczeństwa pomiędzy Nabywcami a Dostawcami Usług Logistycznych (LSP) oraz/lub innymi Wnioskodawcami ubiegającymi się o certyfikację.

Podczas opracowywania tego standardu TAPA uwzględnia różnorodność sposobów świadczenia usług magazynowania na poziomie globalnym, regionalnym, a nawet w obrębie poszczególnych firm, oraz fakt, że FSR może mieć zastosowanie do całości lub części usług świadczonych przez LSP/Wnioskodawcę. W zależności od złożoności i wielkości łańcucha dostaw, zgodność ze standardami TAPA może być osiągnięta przez jednego LSP/Wnioskodawcę lub przez wielu LSP/Wnioskodawców oraz wykwalifikowanych podwykonawców.

Zakres

TAPA opracowała trzy opcje wspierające proces certyfikacji:

- Certyfikacja pojedynczej lokalizacji przez Niezależną Jednostkę Audytującą (IAB).
- Certyfikacja wielu lokalizacji przez IAB.
- Certyfikacja poprzez samoocenę przeprowadzoną przez Upoważnionych Audytorów (AA) LSP/Wnioskodawcy lub przez IAB (wykonując samoocenę w imieniu LSP/Wnioskodawcy).

Odbiorcy

Typowymi użytkownikami standardów TAPA są:

- Nabywcy
- LSP / Wnioskodawcy
- Organy ścigania lub inne organizacje rządowe
- Profesjonalne organizacje łańcucha dostaw
- Ubezpieczyciele

1.2 Zasoby do wdrożenia TAPA FSR

Zasoby niezbędne do spełnienia wymagań FSR są odpowiedzialnością LSP/Wnioskodawcy i pokrywane są na jego koszt, chyba że zostało to uzgodnione lub inaczej określone pomiędzy Nabywcą a LSP/Wnioskodawcą.

1.3 Ochrona polityk i procedur LSP

Kopie dokumentów dotyczących polityk i procedur bezpieczeństwa będą przekazywane Nabywcy wyłącznie zgodnie z podpisanymi umowami o zachowaniu poufności pomiędzy LSP/Wnioskodawcą a Nabywcą i będą traktowane jako informacje poufne.

2.0 O TAPA

2.1 Cel TAPA

Przestępczość związana z ładunkami jest jednym z największych wyzwań w łańcuchu dostaw dla producentów wartościowych produktów wysokiego ryzyka oraz ich dostawców usług logistycznych.

Zagrożenie nie pochodzi już wyłącznie od przestępców działających okazjonalnie. Obecnie zorganizowane grupy przestępcze działają na skalę globalną i wykorzystują coraz bardziej zaawansowane metody ataków na pojazdy, obiekty oraz personel, aby osiągnąć swoje cele.

TAPA jest unikalną platformą, która łączy globalnych producentów, dostawców usług logistycznych, przewoźników, organy ścigania oraz innych interesariuszy, mając wspólny cel – ograniczenie strat w międzynarodowych łańcuchach dostaw. Głównym celem TAPA jest zapobieganie kradzieżom poprzez wykorzystanie danych w czasie rzeczywistym oraz najnowszych środków zapobiegawczych.

2.2 Misja TAPA

Misją TAPA jest pomoc w ochronie aktywów członków poprzez minimalizowanie strat ładunków w łańcuchu dostaw. TAPA realizuje to poprzez rozwój i stosowanie globalnych standardów bezpieczeństwa, uznanych praktyk branżowych, technologii, edukacji, benchmarkingu, współpracy regulacyjnej oraz proaktywne identyfikowanie trendów przestępczych i zagrożeń dla bezpieczeństwa łańcucha dostaw.

3.0 Standardy TAPA

3.1 Standardy bezpieczeństwa TAPA

Poniższe globalne standardy bezpieczeństwa TAPA zostały opracowane w celu zapewnienia bezpiecznego transportu i przechowywania ładunków o wysokiej wartości, będących celem kradzieży:

- Wymagania Bezpieczeństwa Obiektu (FSR) stanowią minimalne standardy dla bezpiecznego magazynowania lub składowania w trakcie transportu w łańcuchu dostaw.
- Wymagania Bezpieczeństwa Transportu Drogowego (TSR) koncentrują się wyłącznie na transporcie ciężarowym i określają minimalne standardy dla przewozu produktów drogą lądową w łańcuchu dostaw.
- Standardy Cyberbezpieczeństwa (CSS) mają na celu dostarczenie narzędzia pomagającego firmom zrozumieć minimalne wymagania w zakresie zarządzania IT w operacjach łańcucha dostaw, aby chronić zasoby cyfrowe przed cyberatakami i zakłóceniami operacyjnymi.

Globalne standardy bezpieczeństwa TAPA są przeglądane i w razie potrzeby aktualizowane co trzy lata.

Niniejszy dokument dotyczy wyłącznie wymagań FSR!

- Proces certyfikacji TAPA FSR jest opisany w dokumencie TAPA FSR Certification Framework.
- Aby uzyskać certyfikat TAPA FSR, należy stosować zarówno aktualną wersję TAPA FSR, jak i dokumentu TAPA FSR Certification Framework.

3.2 Wdrożenie

Skuteczne wdrożenie standardów bezpieczeństwa TAPA zależy od współpracy LSP (Dostawców Usług Logistycznych)/Wnioskodawców, Nabywców (właścicieli ładunku) oraz Upoważnionych Audytorów TAPA.

4.0 Wytyczne prawne

4.1 Zakres

FSR jest standardem globalnym, a wszystkie jego sekcje są obowiązkowe, chyba że zostanie przyznany wyjątek w ramach oficjalnego procesu odstępstw (zob. Sekcja 6 standardu FSR oraz Sekcja 7 dokumentu TAPA FSR Certification Framework).

4.2 Tłumaczenie

W regionach, w których język angielski nie jest językiem podstawowym i gdzie tłumaczenie jest konieczne, odpowiedzialnością LSP/Wnioskodawcy oraz jego przedstawicieli jest zapewnienie, że każde tłumaczenie FSR lub jego części wiernie odzwierciedla intencje TAPA przy opracowywaniu i publikowaniu tych standardów.

4.3 Marka „TAPA”

„TAPA” jest zarejestrowanym znakiem towarowym Transported Asset Protection Association i nie może być używana bez wyraźnej pisemnej zgody TAPA za pośrednictwem jej oficjalnie uznanych regionów. Standardy TAPA oraz powiązane materiały są publikowane przez TAPA i nie mogą być zmieniane, edytowane ani modyfikowane przez żadną stronę bez wyraźnej pisemnej zgody TAPA. Niewłaściwe użycie marki TAPA może skutkować cofnięciem certyfikacji lub podjęciem działań prawnych.

4.4 Ograniczenie odpowiedzialności

Publikując niniejsze standardy, TAPA nie udziela żadnej gwarancji ani zapewnienia, że wszystkie przypadki kradzieży ładunków zostaną wyeliminowane, niezależnie od tego, czy standardy zostały w pełni wdrożone i prawidłowo zastosowane. Wszelka odpowiedzialność wynikająca z kradzieży ładunku podczas magazynowania lub innej utraty ładunku w ramach standardów FSR spoczywa na LSP/Wnioskodawcy i/lub Nabywcy, zgodnie z warunkami ich umowy oraz obowiązującymi przepisami prawa w danej jurysdykcji.

5.0 Umowy i podwykonawstwo

5.1 Umowy

Bezpieczny transport, magazynowanie i obsługa aktywów Nabywcy są odpowiedzialnością LSP/Wnioskodawcy, jego przedstawicieli oraz podwykonawców na wszystkich etapach: odbioru, transportu, magazynowania i dostawy, zgodnie z warunkami określonymi w zleceniu lub umowie.

W przypadku gdy FSR jest wskazany lub włączony do umowy pomiędzy LSP/Wnioskodawcą a Nabywcą, musi on być również uwzględniony w programie bezpieczeństwa LSP/Wnioskodawcy.

LSP powinien dostarczyć Nabywcy dowód certyfikacji FSR oraz, w stosownych przypadkach, dowód spełnienia wymagań FSR. Ponadto wszelkie domniemane niewdrożenie wymagań FSR przez LSP/Wnioskodawcę powinno być rozstrzygane zgodnie z warunkami umowy uzgodnionej pomiędzy Nabywcą a LSP/Wnioskodawcą.

5.2 Podwykonawstwo

W przypadku korzystania z podwykonawców musi istnieć wymóg umowy zobowiązujący ich do spełnienia wszystkich wskazanych wymagań FSR. Wewnętrzni Upoważnieni Audytorzy LSP muszą potwierdzić, że podwykonawca spełnia wymagania FSR na tym samym poziomie.

5.3 Badanie skarg i ich rozpatrywanie przez TAPA

Jeżeli TAPA otrzyma formalną skargę dotyczącą działania certyfikowanego LSP/Wnioskodawcy, TAPA (po jej weryfikacji) może wymagać, aby LSP/Wnioskodawca zlecił ponowny audyt na własny koszt. Jeśli LSP/Wnioskodawca nie przejdzie audytu lub odmówi współpracy w tym procesie, jego certyfikat może zostać cofnięty.

6.0 Odstępstwa

Odstępstwo to pisemna zgoda przyznawana w celu zwolnienia obiektu z określonego wymagania TAPA oraz akceptacji alternatywnego rozwiązania zgodności. O odstępstwo można wnioskować, jeśli LSP/Wnioskodawca nie jest w stanie spełnić konkretnego wymagania FSR i może uzasadnić zastosowanie środków alternatywnych. Odstępstwa są ważne przez okres obowiązywania certyfikacji.

TAPA Copyright © Do Not Copy

7.0 Wymagania Bezpieczeństwa Obiektu

S1. Wymagania ogólne

Req. No.	Requirements / Controls	Applicable Level		
1.1.1	Wszystkie procedury lub polityki wymagane przez niniejszy standard muszą być udokumentowane i aktualizowane co najmniej raz na dwa lata.	(A)	(B)	(C)
1.1.2	Kierownictwo musi formalnie wyznaczyć osobę (AA) odpowiedzialną za bezpieczeństwo na terenie obiektu, która odpowiada za utrzymanie TAPA FSR, zamykanie SCARS, ocenę ryzyka, raportowanie do zarządu oraz wymagania dotyczące bezpieczeństwa łańcucha dostaw w firmie. Inna osoba (może to być ta sama osoba) będzie również odpowiedzialna za monitorowanie programu FSR. Obejmuje to planowanie kontroli zgodności, komunikację z AA, recertyfikację, zmiany w standardzie FSR itp. Osoby te mogą być pracownikami lub osobami zewnętrznymi zatrudnionymi na podstawie umowy do pełnienia tej roli.	(A)	(B)	(C)
1.1.3	Audyty wewnętrzne (przeprowadzane przez zespół międzyfunkcyjny) dotyczące systemu zarządzania bezpieczeństwem, raporty samooceny przygotowywane przez wewnętrznego AA oraz zamknięcie SCARS muszą być przeprowadzone i udokumentowane.	(A)	(B)	(C)
1.1.4	Wymagana jest procedura, rejestr i/lub plan kluczy dla zamków fizycznych, kart dostępu i/lub kluczy zarządzających i kontrolujących klucze fizyczne i elektroniczne. Procedura powinna obejmować procesy dotyczące kopiowania, przechowywania oraz reagowania na zgubione/utracone klucze.	(A)	(B)	(C)

Req. No.	Requirements / Controls	Applicable Level		
1.1.5	Udokumentowana ocena ryzyka, uwzględniająca prawdopodobieństwo i wpływ zagrożeń związanych z bezpieczeństwem, musi być przeprowadzana i aktualizowana co najmniej raz w roku. Kierownictwo musi dokonać przeglądu i potwierdzić, że zidentyfikowane ryzyka zostały ocenione oraz że wdrożono odpowiednie środki kontrolne w celu ich ograniczenia lub wyeliminowania do akceptowalnego poziomu. Co najmniej następujące typowe zdarzenia wewnętrzne/zewnętrzne muszą zostać ocenione: kradzież ładunku lub informacji, nieautoryzowany dostęp do obiektów lub ładunku, manipulacja/uszkodzenie systemów bezpieczeństwa, fikcyjne odbiory ładunku, ciągłość bezpieczeństwa w przypadku niedoborów kadrowych, klęski żywiołowe, potrzeba zastosowania barier antynajazdowych dla okien na poziomie gruntu lub bram dokowych itp. Dodatkowe zagrożenia mogą być uwzględnione w zależności od ryzyk lokalnych/krajowych.	Ⓐ	Ⓑ	Ⓒ
1.1.6	Osoba przeprowadzająca audyty wewnętrzne lub roczne dla Wnioskodawcy/LSP (określana jako LSP AA) musi być przeszkolona. Może to być ta sama osoba, o której mowa w punkcie 1.1.2, lub osoba zewnętrzna zatrudniona na podstawie umowy do pełnienia tej roli.	Ⓐ	Ⓑ	Ⓒ
1.1.7	Aby zrozumieć FSR i być zdolnym do wdrożenia wszystkich jego wymagań, wszyscy AA Wnioskodawcy/LSP muszą ukończyć i zdać odpowiedni egzamin dotyczący standardu TAPA i jego wersji, względem której będą przeprowadzać audyty.	Ⓐ	Ⓑ	Ⓒ

S2. Obwód - Ochrona ternu zewnętrznego

2.1 Zewnętrzny obszar obsługi ładunków magazynu, wysyłki i przyjęć

Req. No.	Requirements / Controls	Applicable Level		
2.1.1	CCTV (telewizja przemysłowa) / VSS (system nadzoru wizyjnego) musi umożliwiać obserwację całego ruchu w zewnętrznym obszarze obsługi ładunków, wysyłki i przyjęć (w tym punktów wejścia i wyjścia), zapewniając, że wszystkie pojazdy i osoby są możliwe do rozpoznania przez cały czas, z wyjątkiem tymczasowych przeszkód wynikających z potrzeb operacyjnych (np. załadunek i rozładunek ciężarówek w czasie rzeczywistym).	Ⓐ	Ⓑ	
2.1.2	Odpowiednie oświetlenie w obszarach załadunku i rozładunku powinno być stosowane jako podstawowy środek odstraszający przed przestępczością oraz umożliwiać obserwację operacji w tych obszarach w porze nocnej. <i>Uwaga: Oświetlenie może być stałe lub uruchamiane przez alarm, detekcję ruchu, dźwięku itp., przy czym musi zapewniać natychmiastowe oświetlenie.</i>	Ⓐ	Ⓑ	Ⓒ
2.1.3	Musi istnieć procedura opisująca sposób postępowania z nieautoryzowanymi pojazdami i osobami w zewnętrznym obszarze obsługi ładunków, wysyłki i przyjęć. Instrukcje dotyczące tej procedury muszą być przekazane odpowiednim pracownikom, w tym ochronie.	Ⓐ	Ⓑ	Ⓒ
2.1.4	Obszar obsługi ładunków, wysyłki i przyjęć musi być odpowiednio kontrolowany, aby zapobiec nieautoryzowanemu dostępowi..		Ⓑ	Ⓒ
2.1.5	W przypadku okien dostępnych z poziomu gruntu lub bram dokowych, coroczna ocena ryzyka musi uwzględniać potrzebę zastosowania barier antywłamaniowych. Ponadto powinna obejmować ocenę zastosowania osłon okiennych w celu zapobiegania nieautoryzowanemu wglądowi do wnętrza (zob. Ocena ryzyka, wymaganie 1.1.5).	Ⓐ		

2.2 Bariery fizyczne

Req. No.	Requirements / Controls	Applicable Level		
2.2.1	Bariera fizyczna (ogrodzenie) otacza obszar obsługi ładunków, wysyłki i przyjęć.	Ⓐ		

Req. No.	Requirements / Controls	Applicable Level		
2.2.2	Bariera fizyczna (ogrodzenie) wokół obszaru obsługi ładunków, wysyłki i przyjęć musi mieć minimalną wysokość 6 stóp / 1,8 metra. <i>Uwaga: Bariera fizyczna, zaprojektowana w celu zapobiegania nieautoryzowanemu dostępowi, musi mieć wysokość 6 stóp / 1,8 metra na całej swojej długości, w tym w miejscach, gdzie poziom gruntu się zmienia (np. jest niższy).</i>	Ⓐ		
2.2.3	Bariera fizyczna (ogrodzenie) wokół obszaru obsługi ładunków, wysyłki i przyjęć musi być utrzymywana w dobrym stanie.	Ⓐ		
2.2.4	Brama/bramy w obrębie ogrodzenia obszaru obsługi ładunków, wysyłki i przyjęć muszą być obsługiwane przez personel lub kontrolowane elektronicznie.	Ⓐ		
2.2.5	Bariera fizyczna wokół obszaru obsługi ładunków, wysyłki i przyjęć musi być sprawdzana pod kątem integralności i uszkodzeń co najmniej raz w tygodniu.	Ⓐ		

2.3 Zewnętrzne obszary doków

Req. No.	Requirements / Controls	Applicable Level		
2.3.1	Zewnętrzny obszar doków musi być objęty monitoringiem CCTV/VSS (kamery kolorowe lub „dzień/noc”).	Ⓐ	Ⓑ	Ⓒ
2.3.2	Kamery CCTV/VSS muszą być zamontowane w sposób umożliwiający obserwację wszystkich operacji i ruchu wokół doków na zewnątrz magazynu przez cały czas, z wyjątkiem tymczasowych przeszkód wynikających z potrzeb operacyjnych (np. załadunek i rozładunek ciężarówek w czasie rzeczywistym).	Ⓐ	Ⓑ	Ⓒ
2.3.3	Wszystkie pojazdy i osoby w obszarach na zewnątrz doków muszą być objęte monitoringiem CCTV/VSS, który umożliwia wyraźne odczytanie danych identyfikacyjnych pojazdu oraz rozpoznanie rysów twarzy personelu.	Ⓐ		
2.3.4	Pojazdy i osoby w obszarach na zewnątrz doków muszą być objęte monitoringiem i widoczne na nagraniach CCTV/VSS w co najmniej 75% przypadków w ciągu dnia.		Ⓑ	Ⓒ

Req. No.	Requirements / Controls	Applicable Level		
2.3.5	Wszystkie zewnętrzne obszary wokół bram dokowych muszą być w pełni oświetlone.	Ⓐ	Ⓑ	Ⓒ

2.4 Dostęp pojazdów prywatnych

Req. No.	Requirements / Controls	Applicable Level		
2.4.1	Pojazdy prywatne mogą być dopuszczone do obszarów obsługi ładunków, wysyłki i przyjęć wyłącznie po wcześniejszym zatwierdzeniu, zgodnie z udokumentowaną polityką.	Ⓐ	Ⓑ	Ⓒ
2.4.2	W promieniu 25 m / 82 stóp po zewnętrznej stronie doków nie mogą znajdować się miejsca parkingowe dla pojazdów prywatnych.	Ⓐ	Ⓑ	Ⓒ

S3. Ściany zewnętrzne, dach i drzwi

3.1 Zewnętrzne strony obiektu: CCTV / VSS

Req. No.	Requirements / Controls	Applicable Level		
3.1.1	Na wszystkich zewnętrznych ścianach/granicach obiektu musi być zainstalowany system CCTV/VSS (kamery kolorowe lub „dzień/noc”).	Ⓐ		
3.1.2	System CCTV/VSS (kamery kolorowe lub „dzień/noc”) musi obejmować zewnętrzne ściany obiektu, w tym miejsca z drzwiami, oknami lub innymi otworami.		Ⓑ	
3.1.3	Wszystkie obrazy z systemu CCTV/VSS obejmującego zewnętrzne ściany obiektu muszą być przez cały czas wyraźne i nie zasłonięte, z wyjątkiem tymczasowych przeszkód wynikających z potrzeb operacyjnych (np. załadunek i rozładunek ciężarówek w czasie rzeczywistym).	Ⓐ		
3.1.4	Wszystkie pojazdy i osoby znajdujące się wokół zewnętrznych stron obiektu muszą być objęte monitoringiem CCTV/VSS, który umożliwia wyraźne odczytanie danych identyfikacyjnych pojazdu oraz rozpoznanie rysów twarzy personelu.	Ⓐ		
3.1.5	Pojazdy i osoby muszą być widoczne na nagraniach zewnętrznych kamer CCTV/VSS w co najmniej 75% zapisów w ciągu dnia.		Ⓑ	

3.2 Ściany zewnętrzne i dach

Req. No.	Requirements / Controls	Applicable Level		
3.2.1	Ściany zewnętrzne i dach muszą być zaprojektowane oraz utrzymywane w taki sposób, aby były odporne na penetrację i zapewniały solidną ochronę fizyczną. Materiały powinny charakteryzować się odpowiednią wytrzymałością i trwałością, aby przeciwdziałać próbom siłowego wejścia. (Przykłady: cegła, bloczki betonowe, prefabrykowane panele betonowe lub wysokowytrzymałe panele warstwowe o całkowitej grubości co najmniej 50 mm oraz z wewnętrznymi i zewnętrznymi okładzinami o grubości 0,7 mm). Uwaga: W przypadku zastosowania lekkich lub niekonstrukcyjnych materiałów należy wdrożyć dodatkowe środki zabezpieczające (np. wewnętrzną siatkę stalową lub systemy wykrywania włamań), aby zapewnić równoważny poziom bezpieczeństwa.	Ⓐ	Ⓑ	Ⓒ

Req. No.	Requirements / Controls	Applicable Level		
3.2.2	Wszystkie okna, które można otworzyć, otwory wentylacyjne lub inne otwory w zewnętrznych ścianach obiektu, a także każde zamknięte okno zamontowane poniżej 3 metrów / 9 stóp 10 cali od poziomu podłogi roboczej, muszą być zabezpieczone fizyczną barierą lub wyposażone w alarm podłączony do głównego systemu alarmowego.	Ⓐ	Ⓑ	
3.2.3	Wszystkie okna możliwe do otwarcia, świetliki dachowe, otwory wentylacyjne, włazy dachowe lub inne otwory w dachu muszą być zabezpieczone poprzez: (a) solidną barierę fizyczną (np. kraty, osłony zabezpieczające lub wzmocnione pokrywy), lub (b) urządzenie wykrywania włamania zintegrowane z głównym systemem alarmowym obiektu. Uwaga: Bariery fizyczne muszą być zaprojektowane w sposób uniemożliwiający ich usunięcie lub manipulację, a zabezpieczone alarmem otwory muszą generować natychmiastowe powiadomienia w przypadku nieautoryzowanego dostępu.	Ⓐ		
3.2.4	Dostęp zewnętrzny do dachu (drabina lub schody) musi być: fizycznie zamknięty i objęty monitoringiem CCTV/VSS (kamery kolorowe lub „dzień/noc”) lub fizycznie zamknięty i zabezpieczony alarmem.	Ⓐ		
3.2.5	Dostęp zewnętrzny do dachu (drabina lub schody) musi być fizycznie zamknięty.		Ⓑ	Ⓒ
3.2.6	Wszystkie zewnętrzne drzwi osobowe magazynu oraz drzwi biurowe w obiekcie muszą być wyposażone w alarm wykrywający nieautoryzowane otwarcie i podłączone do głównego systemu alarmowego. Uwaga: Bramy dokowe nie są objęte tym wymaganiem – zob. wymaganie 3.2.12 dotyczące alarmów bram dokowych.	Ⓐ	Ⓑ	Ⓒ
3.2.7	Każde zewnętrzne drzwi magazynowe, drzwi biurowe lub inne otwarcie w obiekcie musi być jednoznacznie zidentyfikowane w głównym systemie alarmowym – indywidualnie dla każdego drzwi lub dla danej strefy.	Ⓐ		

Req. No.	Requirements / Controls	Applicable Level		
3.2.8	Wszystkie zewnętrzne drzwi magazynowe muszą być zawsze zamknięte i zabezpieczone, gdy nie są używane. W stosownych przypadkach klucze/kody muszą być kontrolowane.	Ⓐ	Ⓑ	
3.2.9	Zewnętrzne drzwi osobowe magazynu oraz ich ościeżnice nie mogą być łatwo sforsowalne. Jeśli zawiasy znajdują się na zewnątrz, muszą być zabezpieczone trzpieniami lub punktowo zespawane. Drzwi magazynowe w całości lub częściowo przeszklone są niedopuszczalne, chyba że są wyposażone w czujniki zbitcia szkła lub inne lokalne urządzenie wykrywające włamanie (np. pasywna podczerwień – PIR) i bezpośrednio podłączone do centrum monitoringu, albo szkło jest zabezpieczone kratami/siatką. TAPA zezwala obecnym posiadaczom certyfikatu, którzy nie są w stanie spełnić tego wymagania, na utrzymanie obecnych rozwiązań do czasu kolejnej rewizji. Nowi posiadacze certyfikatu lub nowe obiekty muszą spełniać to wymaganie.	Ⓐ	Ⓑ	Ⓒ
3.2.10	Wyjścia ewakuacyjne przeznaczone wyłącznie do sytuacji awaryjnych (np. wyjścia przeciwpożarowe) muszą być przez cały czas wyposażone w alarm z indywidualnym lub strefowym sygnalizatorem dźwiękowym.	Ⓐ	Ⓑ	
3.2.11	Wszystkie bramy dokowe muszą mieć wystarczającą wytrzymałość, aby odstraszać i/lub opóźniać próby sforsowania przy użyciu małych elektrycznych/akumulatorowych narzędzi ręcznych..	Ⓐ	Ⓑ	Ⓒ
3.2.12	Bramy dokowe Godziny pozaoperacyjne: Bramy dokowe muszą być zamknięte i zabezpieczone (np. elektronicznie dezaktywowane lub fizycznie zamknięte na klucz). Bramy dokowe muszą być wyposażone w alarm wykrywający nieautoryzowane wtargnięcie i generujący sygnał alarmowy podłączony do głównego systemu alarmowego.. Godziny operacyjne: Bramy dokowe muszą być zamknięte, gdy nie są aktywnie używane. Jeśli stosowane są bramy nożycowe, muszą być zabezpieczone mechaniczną zasuwą/zamkiem zatraskowym i mieć minimalną wysokość 8 stóp / 2,4 metra.	Ⓐ	Ⓑ	Ⓒ

S4. Punkty wejścia i wyjścia do biura oraz magazynu

4.1 Punkty wejścia dla odwiedzających w obszarze biurowym

Req. No.	Requirements / Controls	Applicable Level		
4.1.1	Punkty wejścia dla odwiedzających są kontrolowane przez pracownika/ochroniarza/recepcjonistę, który został przeszkolony w zakresie wydawania identyfikatorów, kontroli, prowadzenia rejestrów, obsługi odwiedzających, wymogów eskorty itp. (musi istnieć procedura dla sytuacji, gdy pracownicy rejestrują własnych gości oraz gdy wizyty odbywają się poza godzinami operacyjnymi).	Ⓐ	Ⓑ	Ⓒ
4.1.2	Punkty wejścia dla odwiedzających w obszarze biurowym muszą być objęte monitoringiem CCTV (kamery kolorowe lub „dzień/noc”), zapewniającym, że osoby są zawsze wyraźnie rozpoznawalne.	Ⓐ	Ⓑ	
4.1.3	W punktach wejścia dla odwiedzających w obszarze biurowym musi być zainstalowany alarm napadowy (panic alarm) i testowany co tydzień.	Ⓐ	Ⓑ	
4.1.4	Wszyscy odwiedzający obszar biurowy muszą być identyfikowani na podstawie dokumentu tożsamości ze zdjęciem wydanego przez organ państwowy (np. prawo jazdy, paszport lub dowód osobisty). Jeśli w obiekcie akceptowane są cyfrowe dokumenty tożsamości i jest to dozwolone przez lokalne przepisy, musi istnieć solidny proces weryfikacji (wraz z wymaganą infrastrukturą techniczną).	Ⓐ	Ⓑ	Ⓒ
4.1.5	Wszyscy odwiedzający obszar biurowy muszą być rejestrowani, a rejestr odwiedzin musi być przechowywany przez co najmniej 30 dni. Szczegóły wizyty, takie jak osoba odwiedzana oraz cel wizyty, muszą być możliwe do przesłania na podstawie informacji zapisanych w rejestrze odwiedzin.	Ⓐ	Ⓑ	Ⓒ
4.1.6	Wszystkie identyfikatory odwiedzających muszą być odbierane przy opuszczaniu obiektu przez odwiedzającego, a pełny rejestr musi być codziennie sprawdzany.	Ⓐ	Ⓑ	
4.1.7	Wszyscy odwiedzający muszą w widoczny sposób nosić identyfikatory lub przepustki oraz być eskortowani przez personel firmy.	Ⓐ	Ⓑ	

4.2 Workforce Entry Point(s)

Req. No.	Requirements / Controls	Applicable Level		
4.2.1	Dostęp do wszystkich wejść dla personelu musi być kontrolowany 24/7.		Ⓑ	Ⓒ
4.2.2	Wszystkie punkty wejścia dla personelu muszą być kontrolowane za pomocą elektronicznego systemu kontroli dostępu 24/7, a dostęp musi być rejestrowany.	Ⓐ		
4.2.3	Punkty wejścia dla personelu muszą być objęte monitoringiem CCTV/VSS (kamery kolorowe lub „dzień/noc”).	Ⓐ	Ⓑ	
4.2.4	Wszyscy pracownicy muszą otrzymać firmowe identyfikatory ze zdjęciem po zakończeniu procesu weryfikacji (vetting).	Ⓐ	Ⓑ	
4.2.5	Pozostały personel również musi otrzymać firmowe identyfikatory, aby byli rozpoznawalni na terenie obiektu.	Ⓐ	Ⓑ	
4.2.6	Wszyscy członkowie personelu muszą w widoczny sposób nosić identyfikatory.	Ⓐ	Ⓑ	
4.2.7	Identyfikatory pracownicze nie mogą być udostępniane w żadnych okolicznościach, a polityka wydawania identyfikatorów musi być wdrożona.	Ⓐ	Ⓑ	

4.3 Identyfikacja kierowcy i pojazdu

Req. No.	Requirements / Controls	Applicable Level		
4.3.1	Wszyscy kierowcy muszą być identyfikowani na podstawie dokumentu tożsamości ze zdjęciem wydanego przez organ państwowy (np. prawo jazdy, paszport lub dowód osobisty), a rejestr kierowców musi być prowadzony. Jeśli w obiekcie akceptowane są cyfrowe dokumenty tożsamości i jest to dozwolone przez lokalne przepisy, musi istnieć solidny proces weryfikacji (wraz z wymaganą infrastrukturą techniczną).	Ⓐ	Ⓑ	Ⓒ

Req. No.	Requirements / Controls	Applicable Level		
4.3.2	Należy zweryfikować, że prawo jazdy nie utraciło ważności oraz że odpowiada danej osobie kierowcy. Jeśli w obiekcie akceptowane są cyfrowe prawa jazdy i jest to dozwolone przez lokalne przepisy, musi istnieć solidny proces weryfikacji (wraz z wymaganą infrastrukturą techniczną).	Ⓐ	Ⓑ	Ⓒ
4.3.3	Identyfikatory pojazdów muszą być rejestrowane ręcznie (np. w formie pisemnej) lub za pomocą kamer. Rejestr musi zawierać co najmniej numer rejestracyjny oraz typ pojazdu.	Ⓐ		

S5. Inside Warehouse and Office

5.1 Warehouse Area: Multi-Tenant Walls

Req. No.	Requirements / Controls	Applicable Level		
5.1.1	Wewnętrzne ściany pomiędzy różnymi najemcami muszą być pełne od podłogi do sufitu i dachu oraz muszą być zaprojektowane, wykonane i utrzymywane w sposób zapewniający odporność na sforsowanie (np. cegła, bloczki, prefabrykowane płyty betonowe typu tilt-up lub ściany z paneli warstwowych o minimalnej grubości 7 mm).	Ⓐ	Ⓑ	Ⓒ
5.1.2	Jeśli wewnętrzne ściany wielonajemcze od podłogi do sufitu są wykonane z siatki o klasie bezpieczeństwa lub innej uznanej w branży bariery zabezpieczającej, muszą być również wyposażone w system alarmowy wykrywający wtargnięcie. <i>Uwaga 1: Siatki o niskiej jakości, ogrodzenia o niskim standardzie lub siatki niebędące klasy bezpieczeństwa są niedopuszczalne.</i> <i>Uwaga 2: Jeśli ściany wielonajemcze są wykonane z pełnego materiału od podłogi do sufitu, to wymaganie nie ma zastosowania.</i>	Ⓐ	Ⓑ	Ⓒ

5.2 Internal Warehouse Areas

Req. No.	Requirements / Controls	Applicable Level		
5.2.1	System wykrywania włamań (np. detekcja podczerwieni, ruchu, dźwięku lub drgań) jest wymagany do monitorowania wewnętrznych obszarów magazynowych. Alarmy muszą być aktywowane i połączone z głównym systemem alarmowym w godzinach pozaoperacyjnych (tj. gdy magazyn jest zamknięty). <i>Uwaga 1: Jeśli magazyn działa w trybie ciągłym 24/7/366, wymaganie to może nie mieć zastosowania, pod warunkiem że ryzyka i środki zaradcze są udokumentowane w lokalnej ocenie ryzyka (zob. wymaganie 1.1.5)</i> <i>Uwaga 2: Niezależnie od godzin pracy, wykrywanie włamań na obwodzie lub bariery fizyczne są zawsze wymagane dla drzwi zewnętrznych oraz okien na poziomie gruntu w biurze i magazynie (zob. wymagania 3.2.2 i 3.2.6).</i>	Ⓐ		

5.3 Wewnętrzne bramy dokowe i obszary doków

Req. No.	Requirements / Controls	Applicable Level		
5.3.1	Wszystkie bramy dokowe i obszary doków muszą być objęte monitoringiem CCTV/VSS (kamery kolorowe lub „dzień/noc” od wewnętrznej strony).	Ⓐ	Ⓑ	Ⓒ
5.3.2	Obraz ładunków podczas załadunku i rozładunku przy wszystkich wewnętrznych bramach dokowych i w obszarach doków musi być przez cały czas widoczny, z wyjątkiem tymczasowych przeszkód wynikających z potrzeb operacyjnych (np. załadunek i rozładunek ciężarówek w czasie rzeczywistym).	Ⓐ	Ⓑ	Ⓒ
5.3.3	Aktywa Nabywcy muszą być objęte w 100% monitoringiem CCTV w obszarach przemieszczania lub przygotowania ładunków (np. strefy rozformowywania/kompletacji palet, trasy do i z regałów magazynowych, doki, korytarze transportowe).	Ⓐ	Ⓑ	
5.3.4	Analiza martwych stref w celu zapewnienia 100% pokrycia CCTV ruchu ładunków musi być przeprowadzana co najmniej raz w roku, chyba że nastąpią zmiany operacyjne i/lub strukturalne w magazynie.	Ⓐ		

5.4 Kontrola dostępu między biurem a dokiem/magazynem

Req. No.	Requirements / Controls	Applicable Level		
5.4.1	Dostęp między biurem a dokiem/magazynem musi być kontrolowany.	Ⓐ	Ⓑ	
5.4.2	Dostęp kartowy lub alarmy drzwiowe z interkomem dla drzwi między biurem a dokiem/magazynem muszą być słyszalne lokalnie i generować alarm wymagający reakcji, gdy drzwi pozostają otwarte dłużej niż 60 sekund lub natychmiast w przypadku ich sforsowania.	Ⓐ		
5.4.3	Alarmy drzwiowe dla drzwi między biurem a dokiem/magazynem muszą być słyszalne lokalnie lub wysyłać sygnał alarmowy wymagający reakcji, gdy drzwi pozostają otwarte dłużej niż 60 sekund lub zostaną sforsowane.		Ⓑ	
5.4.4	Dostęp do obszarów doków/magazynu mogą mieć wyłącznie upoważnieni pracownicy LSP/Wnioskodawcy oraz eskortowani goście, na podstawie uzasadnionej potrzeby biznesowej i z odpowiednimi ograniczeniami.	Ⓐ	Ⓑ	Ⓒ
5.4.5	Lista dostępu do obszarów doków/magazynu musi być przeglądana co najmniej raz na kwartał w celu ograniczenia i weryfikacji, że uprawnienia dostępu są przyznawane wyłącznie wyznaczonemu/upoważnionemu personelowi.	Ⓐ	Ⓑ	

5.5 Obszar ładunków o wysokiej wartości (HVC)

Req. No.	Requirements / Controls	Applicable Level		
5.5.1	Wielkość i sposób wykorzystania obszaru HVC (klatka na towary wysokiej wartości) mogą być określone w umowie pomiędzy Nabywcą a LSP/Wnioskodawcą. Jeśli taka umowa nie istnieje, obszar HVC musi umożliwiać przechowywanie co najmniej 6 metrów sześciennych produktów.	Ⓐ	Ⓑ	
5.5.2	Obszar HVC musi być ogrodzony (np. klatką) lub otoczony solidnymi ścianami ze wszystkich stron, w tym od góry/dachu.	Ⓐ	Ⓑ	
5.5.3	Obszar HVC musi być wyposażony w urządzenie blokujące drzwi/bramę.	Ⓐ	Ⓑ	
5.5.4	Wejście do HVC oraz jego wnętrze muszą być objęte pełnym monitoringiem CCTV/VSS (kamery kolorowe lub „dzień/noc”). <i>Uwaga: Jeśli obszar HVC jest zbyt mały, aby zainstalować kamerę wewnątrz, wystarczające jest objęcie monitoringiem wejścia.</i>	Ⓐ		
5.5.5	Wejście do HVC musi być objęte monitoringiem CCTV/VSS (kamery kolorowe lub „dzień/noc”).		Ⓑ	
5.5.6	Jeśli dostęp do HVC jest wymagany dla więcej niż 10 osób, dostęp musi być kontrolowany elektronicznie (np. kartą lub brelokiem). Jeśli dostęp dotyczy 10 lub mniej osób, należy zastosować system solidnych zamków lub klódek wspierany kontrolowanym systemem wydawania kluczy. Klucze mogą być wydawane pracownikom na czas zmiany, ale nie mogą być przekazywane bez zatwierdzenia i odnotowania w rejestrze kluczy. Wszystkie klucze muszą być zwracane i rozliczane po zakończeniu użytkowania.	Ⓐ		
5.5.7	Drzwi/bramy HVC muszą być wyposażone w alarm wykrywający próby sforsowania. Alarmy mogą być generowane przez czujniki drzwi i/lub system detekcji ruchu CCTV/VSS w celu wykrycia nieautoryzowanego dostępu.	Ⓐ		
5.5.8	Obwód HVC musi być utrzymywany w dobrym stanie i sprawdzany co najmniej raz w miesiącu pod kątem integralności i uszkodzeń.	Ⓐ		

Req. No.	Requirements / Controls	Applicable Level		
5.5.9	LSP/Wnioskodawca musi zapewnić, że dostęp do obszaru HVC jest przyznawany wyłącznie wyznaczonemu/upoważnionemu personelowi..	Ⓐ	Ⓑ	
	Zatwierdzona lista dostępu do HVC musi być przeglądana co najmniej raz w miesiącu i aktualizowana w czasie rzeczywistym w przypadku odejścia pracownika lub gdy przestaje on potrzebować dostępu.			
	Musi istnieć procedura dotycząca dostępu do obszaru HVC.			

5.6 Kontrola odpadów z magazynu

Req. No.	Requirements / Controls	Applicable Level		
5.6.1	Wewnętrzne i/lub zewnętrzne główne pojemniki na odpady oraz obszary ich zagęszczania w magazynie muszą być objęte monitoringiem CCTV/VSS.	Ⓐ		
5.6.2	Jeśli są stosowane, worki na odpady używane w magazynie powinny być przezroczyste.		Ⓑ	Ⓒ

5.7 Przedzaładunek i strefa przygotowania

Req. No.	Requirements / Controls	Applicable Level		
5.7.1	Podczas godzin pozaoperacyjnych nie dopuszcza się przedzaładunku ani parkowania pojazdów FTL / dedykowanych pojazdów Nabywcy poza budynkiem magazynu, chyba że zostało to uzgodnione pomiędzy Nabywcą a LSP/Wnioskodawcą.	Ⓐ	Ⓑ	Ⓒ
	Należy wdrożyć alternatywne środki bezpieczeństwa (np. dodatkowe zabezpieczenia pojazdów lub przestrzeni ładunkowych).			
	<i>Uwaga: „Poza budynkiem magazynu” oznacza obszary oddzielone od samego obiektu, znajdujące się poza nim, lecz nadal w obrębie terenu/ogrodzenia LSP/Wnioskodawcy.</i>			

5.8 Kontrola przedmiotów osobistych i przeszukania przy wyjściu

Req. No.	Requirements / Controls	Applicable Level		
5.8.1	Pisane procedury bezpieczeństwa muszą określać, w jaki sposób „przedmioty osobiste” są kontrolowane w magazynie. Przedmioty osobiste obejmują m.in. lunchboxy, plecaki, torby chłodzące, torebki itp.	Ⓐ	Ⓑ	
5.8.2	Jeśli pozwala na to prawo lokalne, LSP/Wnioskodawca musi opracować i utrzymywać udokumentowaną procedurę przeszukań przy wyjściu. Uruchomienie tej procedury zależy od decyzji LSP/Wnioskodawcy i/lub ustaleń między Nabywcą a LSP/Wnioskodawcą. Co najmniej procedura musi określać prawo LSP/Wnioskodawcy do przeprowadzania kontroli oraz kryteria ich zastosowania w sytuacjach, gdy normalnie nie są wymagane (np. w przypadku podejrzenia kradzieży przez pracowników). Pracownicy, TAS, podwykonawcy oraz odwiedzający muszą być poinformowani o tej polityce przed wejściem do magazynu.	Ⓐ		

5.9 Kontrola sprzętu do obsługi ładunków

Req. No.	Requirements / Controls	Applicable Level		
5.9.1	Musi istnieć procedura wymagająca wyłączania wszystkich wózków widłowych oraz innych zasilanych urządzeń do obsługi ładunków w godzinach pozaoperacyjnych. <i>Uwaga: Wymóg ten nie dotyczy ręcznych wózków paletowych (hand-jack/pallet-jack).</i>	Ⓐ	Ⓑ	

5.10 Integralność kontenera lub naczepy: kontrola 7-punktowa

Req. No.	Requirements / Controls	Applicable Level		
5.10.1	7-punktowa kontrola fizyczna musi być przeprowadzana dla wszystkich wyjeżdżających kontenerów i naczep dedykowanych Nabywcy, obejmująca: ścianę przednią, lewą i prawą stronę, podłogę, sufit/dach, drzwi wewnętrzne i zewnętrzne wraz z mechanizmem zamykającym oraz zewnętrzną część/podwozie. <i>Uwaga: Dotyczy to wszystkich typów naczep i kontenerów zabezpieczonych zamkiem i/lub plombą (tj. nie ogranicza się wyłącznie do kontenerów morskich).</i>	Ⓐ	Ⓑ	Ⓒ

5.11 Freight Handover Process; Security Seals

Req. No.	Requirements / Controls	Applicable Level		
5.11.1	O ile Nabywca nie zwolni z tego wymogu, plomby zabezpieczające typu „tamper evident” muszą być stosowane we wszystkich bezpośrednich, bezprzystankowych przesyłkach. Plomby muszą być certyfikowane zgodnie z normą ISO 17712 (klasyfikacja I, S lub H). <i>Uwaga: Plomby nie są wymagane w przesyłkach wieloetapowych, ze względu na złożoność i ryzyko związane z przewożeniem wielu plomb przez kierowców.</i>	Ⓐ	Ⓑ	Ⓒ
5.11.2	LSP/Wnioskodawca musi posiadać udokumentowane procedury dotyczące zarządzania i kontroli plomb zabezpieczających, zamków drzwi naczep (kontenerów), zamków typu pin oraz innego sprzętu zabezpieczającego.	Ⓐ	Ⓑ	Ⓒ
5.11.3	Plomby zabezpieczające mogą być zakładane i zdejmowane wyłącznie przez upoważniony personel (np. pracowników magazynu), przeszkolony w zakresie rozpoznawania i zgłaszania naruszonych plomb. Plomby nigdy nie mogą być zakładane ani zdejmowane przez kierowcę, chyba że istnieje wyjątek ze strony Nabywcy.	Ⓐ	Ⓑ	Ⓒ
5.11.4	Muszą istnieć procedury dotyczące rozpoznawania i zgłaszania naruszonych plomb zabezpieczających.	Ⓐ	Ⓑ	Ⓒ

5.12 Integralność ładunku; proces weryfikacji załadunku/rozładunku

Req. No.	Requirements / Controls	Applicable Level		
5.12.1	Muszą istnieć solidne procedury zapewniające, że wszystkie aktywa Nabywcy wysyłane i odbierane są weryfikowane w punkcie przekazania poprzez ręczne i/lub elektroniczne liczenie sztuk. Proces musi zapewniać, że nieprawidłowości są konsekwentnie wykrywane, dokumentowane i zgłaszane do LSP/Wnioskodawcy i/lub Nabywcy. Zapisy ręczne i/lub elektroniczne muszą mieć wartość dowodową. Jeśli kierowcy nie są obecni, aby potwierdzić te czynności, Nabywca/LSP/Wnioskodawca musi zapewnić alternatywne metody weryfikacji ilości, takie jak skany i/lub nagrania CCTV/VSS, które są gromadzone i przechowywane specjalnie w tym celu. <i>Uwaga: Oprócz brakujących sztuk, nieprawidłowości mogą obejmować uszkodzenia, brakujące pasy lub taśmy, przecięcia lub inne widoczne oznaki otwarcia, wskazujące na możliwą kradzież lub przywłaszczenie.</i>	Ⓐ	Ⓑ	Ⓒ

5.13 Oszukańcze odbiory ładunku

Req. No.	Requirements / Controls	Applicable Level		
5.13.1	Tożsamość kierowcy ciężarówki, dokumentacja odbioru ładunku oraz wymagane przez Nabywcę dane wstępnego powiadomienia (pre-alert) muszą być zweryfikowane przed załadunkiem. Musi istnieć odpowiednia procedura. Jeśli w obiekcie akceptowane są cyfrowe dokumenty tożsamości i jest to dozwolone przez lokalne przepisy, musi istnieć solidny proces weryfikacji (wraz z wymaganą infrastrukturą techniczną).	Ⓐ	Ⓑ	Ⓒ

S6. Systemy bezpieczeństwa: projektowanie, monitorowanie i reagowanie

6.1 Stanowisko monitoringu

Req. No.	Requirements / Controls	Applicable Level		
6.1.1	Monitorowanie zdarzeń alarmowych musi odbywać się 24/7/366 za pośrednictwem wewnętrznego lub zewnętrznego stanowiska monitoringu, zabezpieczonego przed nieautoryzowanym dostępem. <i>Uwaga: Stanowiska monitoringu mogą znajdować się na terenie obiektu lub poza nim i mogą być własnością firmy lub podmiotu zewnętrznego. We wszystkich przypadkach dostęp musi być kontrolowany za pomocą elektronicznego systemu kontroli dostępu (identyfikatory), zamków lub skanerów biometrycznych.</i>	Ⓐ	Ⓑ	Ⓒ
6.1.2	Stanowisko monitoringu musi reagować na wszystkie alarmy systemu bezpieczeństwa w czasie rzeczywistym 24/7/366.	Ⓐ	Ⓑ	Ⓒ
6.1.3	Stanowisko monitoringu musi potwierdzać aktywację alarmu i przekazywać zgłoszenie (eskalować) w czasie krótszym niż 3 minuty.	Ⓐ	Ⓑ	Ⓒ
6.1.4	Raporty z monitorowania alarmów muszą być dostępne.	Ⓐ	Ⓑ	Ⓒ
6.1.5	Muszą istnieć procedury reagowania dla stanowiska monitoringu.	Ⓐ	Ⓑ	Ⓒ

6.2 Intruder Detection System (IDS) System wykrywania włamania

Req. No.	Requirements / Controls	Applicable Level		
6.2.1	Wszystkie systemy IDS muszą być aktywowane w godzinach pozaoperacyjnych i połączone z głównym systemem alarmowym.	Ⓐ	Ⓑ	Ⓒ
6.2.2	Rejestry alarmów IDS muszą być przechowywane przez co najmniej 90 dni.	Ⓐ	Ⓑ	
6.2.3	Rejestry alarmów IDS muszą być bezpiecznie przechowywane i tworzone w ich kopie zapasowe co najmniej raz w tygodniu.	Ⓐ	Ⓑ	

Req. No.	Requirements / Controls	Applicable Level		
6.2.4	Musi istnieć procedura zapewniająca, że dostęp do IDS jest ograniczony wyłącznie do upoważnionych osób lub administratorów systemu. Obejmuje to serwery, konsole, kontrolery, panele, sieci oraz dane. Uprawnienia dostępu do IDS muszą być niezwłocznie aktualizowane w przypadku odejścia pracownika z organizacji lub zmiany jego roli, gdy dostęp nie jest już wymagany..	Ⓐ	Ⓑ	Ⓒ
6.2.5	Alarm musi być przekazywany w przypadku awarii zasilania/utruty zasilania systemu IDS. <i>Uwaga: W systemach wyposażonych w zasilanie awaryjne (UPS), alarm jest przekazywany w przypadku awarii baterii UPS.</i>	Ⓐ	Ⓑ	Ⓒ
6.2.6	Musi istnieć proces weryfikacji uzbrojenia alarmu IDS. <i>Uwaga: Muszą istnieć procedury potwierdzające, że alarmy są uzbrojone w godzinach pozaoperacyjnych.</i>	Ⓐ	Ⓑ	Ⓒ
6.2.7	Alarm IDS musi być przekazywany za pośrednictwem linii stałej lub bezprzewodowej oraz w przypadku awarii trybu komunikacji.	Ⓐ	Ⓑ	
6.2.8	W przypadku awarii urządzenia IDS i/lub linii komunikacyjnej musi być zapewniony system komunikacji zapasowej.	Ⓐ	Ⓑ	

6.3 Automatyczny system kontroli dostępu (AACS)

Req. No.	Requirements / Controls	Applicable Level		
6.3.1	Rejestry transakcji AACS muszą być dostępne przez co najmniej 90 dni. Dane muszą być bezpiecznie przechowywane oraz objęte kopiami zapasowymi.	Ⓐ	Ⓑ	
6.3.2	Musi istnieć procedura zapewniająca, że dostęp do AACS jest ograniczony wyłącznie do upoważnionych osób lub administratorów systemu. Uprawnienia dostępu muszą być niezwłocznie aktualizowane w przypadku odejścia pracownika z organizacji lub zmiany jego roli, gdy dostęp nie jest już wymagany.	Ⓐ	Ⓑ	

Req. No.	Requirements / Controls	Applicable Level		
6.3.3	Raporty systemu kontroli dostępu muszą być przeglądane co najmniej raz na kwartał w celu identyfikacji nieprawidłowości lub nadużyć (np. wielokrotne nieudane próby logowania, błędne odczyty – np. dezaktywowana karta, dowody udostępniania kart w celu umożliwienia nieautoryzowanego dostępu itp.). Musi istnieć odpowiedni proces.	Ⓐ	Ⓑ	

6.4 CCTV/ VSS System Tealwizji Przemysłowej

Req. No.	Requirements / Controls	Applicable Level		
6.4.1	Musi być wdrożony system cyfrowego zapisu CCTV/VSS.	Ⓐ	Ⓑ	Ⓒ
6.4.2	Prędkość nagrywania CCTV/VSS musi wynosić co najmniej 8 klatek na sekundę (fps) na kamerę.	Ⓐ	Ⓑ	Ⓒ
6.4.3	Funkcjonalność nagrywania cyfrowego musi być sprawdzana codziennie w dniach operacyjnych zgodnie z procedurą, a zapisy muszą być dostępne.	Ⓐ	Ⓑ	Ⓒ
6.4.4	Nagrania CCTV/VSS muszą być przechowywane przez minimum 30 dni, o ile pozwalają na to lokalne przepisy. LSP/Wnioskodawca musi przedstawić dowody na istnienie przepisów lokalnych, które zabraniają stosowania CCTV i/lub ograniczają czas przechowywania danych wideo do mniej niż 30 dni.	Ⓐ	Ⓑ	Ⓒ
6.4.5	Dostęp do systemu CCTV/VSS (w tym sprzętu, oprogramowania oraz przechowywania danych/wideo) musi być ściśle kontrolowany. Pomieszczenie musi być zamknięte na klucz, jeśli system przechowywania CCTV/VSS znajduje się na miejscu, a kontrola dostępu musi być zapewniona.	Ⓐ	Ⓑ	Ⓒ
6.4.6	Obrazy CCTV/VSS mogą być wykorzystywane do celów bezpieczeństwa wyłącznie przez upoważniony personel.	Ⓐ	Ⓑ	Ⓒ
6.4.7	Muszą istnieć procedury określające politykę ochrony danych CCTV/VSS dotyczącą wykorzystania obrazów w czasie rzeczywistym oraz archiwalnych, zgodnie z lokalnymi przepisami.	Ⓐ	Ⓑ	

6.5 Oświetlenie zewnętrzne i wewnętrzne

Req. No.	Requirements / Controls	Applicable Level		
6.5.1	Poziomy oświetlenia zewnętrznego i wewnętrznego muszą być wystarczające, aby wspierać obrazy CCTV/VSS umożliwiające prowadzenie dochodzeń oraz uzyskanie nagrań o jakości dowodowej.	Ⓐ	Ⓑ	
6.5.2	Poziomy oświetlenia zewnętrznego i wewnętrznego muszą być wystarczające, aby umożliwić wyraźne rozpoznanie wszystkich pojazdów i osób.	Ⓐ		

TAPA Copyright © Do Not Copy

S7. Szkolenia i procedury

7.1 Procedury eskalacji

Req. No.	Requirements / Controls	Applicable Level		
7.1.1	Muszą istnieć lokalne procedury dotyczące obsługi aktywów Nabywcy, w tym proces terminowego zgłaszania utraconych, brakujących lub skradzionych aktywów Nabywcy. Incydenty muszą być zgłaszane przez LSP/Wnioskodawcę do Nabywcy w ciągu 24 godzin. Oczywiście kradzieże muszą być zgłaszane natychmiast. Proces musi być stosowany konsekwentnie.	Ⓐ	Ⓑ	Ⓒ
7.1.2	Lista kontaktów awaryjnych do zarządzania obiektem po stronie Nabywcy oraz LSP/Wnioskodawcy w przypadku incydentów bezpieczeństwa musi być dostępna. Lista ta musi być aktualizowana co 6 miesięcy i obejmować kontakty do służb porządkowych.	Ⓐ	Ⓑ	Ⓒ

7.2 Zaangażowanie kierownictwa

Req. No.	Requirements / Controls	Applicable Level		
7.2.1	Kierownictwo musi opracować, komunikować oraz utrzymywać politykę bezpieczeństwa, aby zapewnić, że wszystkie odpowiednie osoby (tj. pracownicy i wykonawcy) są jasno świadome wymagań bezpieczeństwa dostawcy.	Ⓐ	Ⓑ	Ⓒ

7.3 Szkolenie

Req. No.	Requirements / Controls	Applicable Level		
7.3.1	Szkolenie z zakresu bezpieczeństwa/świadomości zagrożeń musi być zapewnione wszystkim pracownikom w ciągu pierwszych 60 dni od zatrudnienia, a następnie co najmniej co 2 lata.	Ⓐ	Ⓑ	Ⓒ
7.3.2	Szkolenie z zakresu świadomości bezpieczeństwa informacji, ukierunkowane na ochronę elektronicznych i fizycznych danych wysyłkowych Nabywcy, musi być zapewnione pracownikom mającym dostęp do informacji Nabywcy, a następnie co najmniej co 2 lata lub zgodnie z lokalnymi przepisami, jeśli określają one krótszy okres odświeżenia szkolenia.	Ⓐ	Ⓑ	Ⓒ

7.4 Dostęp do aktywów Nabywcy

Req. No.	Requirements / Controls	Applicable Level		
7.4.1	Muszą istnieć procedury mające na celu ochronę aktywów Nabywcy (tj. ładunku) przed nieautoryzowanym dostępem ze strony pracowników, odwiedzających itp.	Ⓐ	Ⓑ	Ⓒ

7.5 Kontrola informacji

Req. No.	Requirements / Controls	Applicable Level		
7.5.1	Dostęp do dokumentów wysyłkowych oraz informacji dotyczących aktywów Nabywcy musi być kontrolowany zgodnie z zasadą „need to know” (dostępu tylko dla osób, które muszą wiedzieć). Musi istnieć proces zapewniający ochronę informacji Nabywcy.	Ⓐ	Ⓑ	Ⓒ
7.5.2	Dostęp do dokumentów wysyłkowych oraz informacji o aktywach Nabywcy musi być monitorowany i rejestrowany. Muszą istnieć odpowiednie procedury i zapisy.	Ⓐ	Ⓑ	Ⓒ
7.5.3	Dokumenty wysyłkowe oraz wszelkie inne dokumenty zawierające informacje o aktywach Nabywcy muszą być zabezpieczone aż do momentu ich zniszczenia.	Ⓐ	Ⓑ	Ⓒ

7.6 Raportowanie incydentów bezpieczeństwa

Req. No.	Requirements / Controls	Applicable Level		
7.6.1	Musi istnieć system raportowania i śledzenia incydentów bezpieczeństwa, wykorzystywany do wdrażania działań proaktywnych.	Ⓐ	Ⓑ	

7.7 Programy utrzymania (konserwacji)

Req. No.	Requirements / Controls	Applicable Level		
7.7.1	Muszą istnieć programy konserwacji dla wszystkich technicznych (fizycznych) instalacji/systemów bezpieczeństwa w celu zapewnienia ich ciągłej sprawności (np. CCTV/VSS, systemy kontroli dostępu, systemy wykrywania włamań oraz oświetlenie).	(A)	(B)	(C)
7.7.2	Konserwacja zapobiegawcza musi być przeprowadzana raz w roku lub zgodnie ze specyfikacjami producenta.	(A)	(B)	(C)
7.7.3	Weryfikacja działania wszystkich systemów musi być przeprowadzana co najmniej raz w tygodniu i dokumentowana, chyba że awaria systemu jest natychmiast/automatycznie zgłaszana lub sygnalizowana alarmem.	(A)	(B)	
7.7.4	Zlecenie naprawy musi zostać zainicjowane w ciągu 48 godzin od momentu wykrycia usterki. W przypadku napraw, które mają trwać dłużej niż 24 godziny, należy wdrożyć alternatywne środki zabezpieczające.	(A)	(B)	

7.8 Szkolenie wstępne dla podwykonawców

Req. No.	Requirements / Controls	Applicable Level		
7.8.1	LSP/Wnioskodawca musi zapewnić, że wszyscy podwykonawcy/dostawcy są świadomi odpowiednich programów bezpieczeństwa LSP/Wnioskodawcy i przestrzegają ich.	(A)	(B)	(C)

7.9 Dokumentacja wysyłek i przyjęć

Req. No.	Requirements / Controls	Applicable Level		
7.9.1	Dokumenty wysyłki i przyjęcia muszą być czytelne, kompletne i dokładne (tj. czas, data, podpisy, kierowca, personel wysyłki i przyjęcia, szczegóły przesyłki oraz ilość itp.). Imiona i nazwiska kierowcy oraz nadawcy muszą być zawsze wyraźnie czytelne.	(A)	(B)	(C)
7.9.2	LSP/Wnioskodawca musi przechowywać zapisy wszystkich odbiorów oraz dowody dostaw przez okres nie krótszy niż dwa lata i udostępniać je w razie potrzeby w trakcie dochodzeń dotyczących strat.	(A)	(B)	(C)

Req. No.	Requirements / Controls	Applicable Level		
7.9.3	Dowód dostawy musi być dostarczony zgodnie z pisemną umową pomiędzy Nabywcą a LSP/Wnioskodawcą. Jeżeli Nabywca tego wymaga, miejsce docelowe musi powiadomić miejsce nadania w uzgodnionym czasie o odbiorze przesyłki, uzgadniając szczegóły z informacjami z pre-alertu.	Ⓐ	Ⓑ	Ⓒ

7.10 Proces pre-alert musi być wdrożony

Req. No.	Requirements / Controls	Applicable Level		
7.10.1	Jeżeli Nabywca tego wymaga, musi być wdrożony proces pre-alert dla przesyłek przychodzących i/lub wychodzących. Szczegóły pre-alertu muszą być uzgodnione pomiędzy Nabywcą a LSP/Wnioskodawcą. Sugerowane informacje obejmują: czas wyjazdu, przewidywany czas przyjazdu, firmę transportową, imię i nazwisko kierowcy, dane rejestracyjne pojazdu, informacje o przesyłce (liczba sztuk, waga, numer listu przewozowego itp.) oraz numery plomb naczepy.	Ⓐ	Ⓑ	Ⓒ

S8. Integralność personelu

8.1 Weryfikacja / sprawdzanie / kontrole przeszłości (w zakresie dozwolonym przez prawo lokalne)

Req. No.	Requirements / Controls	Applicable Level		
8.1.1	LSP/Wnioskodawca musi posiadać proces weryfikacji/sprawdzania/analizy przeszłości, który obejmuje co najmniej 5 lat historii zatrudnienia oraz sprawdzenie niekaralności. Weryfikacja dotyczy wszystkich kandydatów, w tym pracowników i podwykonawców. LSP/Wnioskodawca musi również zapewnić, na mocy umów, że równoważny proces jest stosowany przez firmy dostarczające pracowników TAS.	(A)	(B)	(C)
8.1.2	LSP/Wnioskodawca musi posiadać umowy zapewniające dostarczanie wymaganych informacji dotyczących weryfikacji/sprawdzania/analizy przeszłości przez agencję i/lub podwykonawcę dostarczającego pracowników TAS lub przeprowadzać taką weryfikację samodzielnie. Weryfikacja musi obejmować sprawdzenie niekaralności oraz historii zatrudnienia.	(A)	(B)	(C)
8.1.3	Musi istnieć procedura postępowania w przypadku fałszywych oświadczeń kandydatów/pracowników zarówno przed zatrudnieniem, jak i po jego rozpoczęciu.	(A)	(B)	(C)

8.2 Zakończenie zatrudnienia lub ponowne zatrudnienie pracowników

Uwaga: Zakończenie zatrudnienia obejmuje zarówno odejścia dobrowolne, jak i niedobrowolne — pracowników zwolnionych oraz tych, którzy złożyli rezygnację.

Req. No.	Requirements / Controls	Applicable Level		
8.2.1	Należy odzyskać od pracowników kończących zatrudnienie wszystkie zasoby fizyczne, w tym identyfikatory firmowe, karty dostępu, klucze, sprzęt, zasoby IT oraz informacje wrażliwe. Wymagana jest udokumentowana procedura.	(A)	(B)	(C)
8.2.2	Ochrona danych Nabywcy: należy zakończyć dostęp pracowników odchodzących do systemów fizycznych i elektronicznych, w tym tych zawierających dane Nabywcy. Wymagana jest udokumentowana procedura.	(A)	(B)	(C)
8.2.3	Musi istnieć lista kontrolna dla pracowników w procesie wdrożenia (onboarding) i zakończenia współpracy (offboarding) w celu weryfikacji.	(A)	(B)	(C)

Req. No.	Requirements / Controls	Applicable Level		
8.2.4	Ponowne zatrudnienie: Muszą istnieć procedury zapobiegające ponownemu zatrudnieniu pracowników przez LSP/Wnioskodawcę, jeśli kryteria odmowy/zakończenia zatrudnienia nadal obowiązują. <i>Uwaga: Przed ponownym zatrudnieniem należy dokonać przeglądu zapisów (np. historii wcześniej zwolnionych pracowników lub kandydatów, którym wcześniej odmówiono zatrudnienia).</i>	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

S9. Wymagania dotyczące jednostki centralnej (dotyczy wyłącznie certyfikacji wielooddziałowej)

9.1 Postanowienia ogólne

Req. No.	Requirements / Controls	Applicable Level		
9.1.1	Musi istnieć jednostka centralna zarządzająca systemem zarządzania bezpieczeństwem dla wszystkich lokalizacji objętych zakresem certyfikacji wielooddziałowej.	(A)	(B)	(C)
9.1.2	Wszystkie lokalizacje muszą mieć relację prawną lub umowną z jednostką centralną. Wymóg ten nie dotyczy lokalizacji podwykonawców włączonych do zakresu certyfikacji, zgodnie z punktem 4.2.2 dokumentu CFD.	(A)	(B)	(C)
9.1.3	Musi być ustanowiony jeden system zarządzania bezpieczeństwem, zapewniający, że wszystkie lokalizacje w jego ramach spełniają wymagania odpowiedniego standardu bezpieczeństwa TAPA.	(A)	(B)	(C)
9.1.4	Jednostka centralna oraz jej system zarządzania muszą podlegać audytom wewnętrznym w celu zapewnienia ciągłej zgodności ze standardami TAPA.	(A)	(B)	(C)
9.1.5	Jednostka centralna musi przeprowadzać audyty lokalizacji objętych zakresem, aby zapewnić, że każda lokalizacja spełnia odpowiednie wymagania TAPA FSR. Audyty muszą być przeprowadzane przy użyciu właściwych szablonów audytowych TAPA. Wszystkie indywidualne roczne audyty lokalizacji muszą zostać zakończone i być dostępne dla audytora przed rozpoczęciem procesu certyfikacji.	(A)	(B)	(C)
9.1.6	Jednostka centralna musi posiadać uprawnienia i prawo do wymagania od wszystkich lokalizacji zgodności ze standardami bezpieczeństwa TAPA oraz do wdrażania działań korygujących i zapobiegawczych w razie potrzeby. <i>Uwaga: W stosownych przypadkach powinno to być określone w formalnej umowie pomiędzy jednostką centralną a poszczególnymi lokalizacjami.</i>	(A)	(B)	(C)

9.2 Polityki i procedury

Req. No.	Requirements / Controls	Applicable Level		
9.2.1	Jednostka centralna musi utrzymywać udokumentowane polityki i procedury dotyczące systemów zarządzania bezpieczeństwem, które mają zastosowanie do wszystkich lokalizacji.	(A)	(B)	(C)
9.2.2	Jednostka centralna musi zapewnić, że polityki i procedury są odpowiednio aktualizowane, komunikowane, wdrażane i realizowane przez wszystkie lokalizacje zgodnie z wymaganiami.	(A)	(B)	(C)
9.2.3	Polityki i procedury muszą być utrzymywane i łatwo dostępne dla wszystkich lokalizacji zgodnie z potrzebami.	(A)	(B)	(C)

9.3 Raport z audytu samooceny przeprowadzany dla wszystkich lokalizacji

Req. No.	Requirements / Controls	Applicable Level		
9.3.1	Jednostka centralna musi zobowiązać wszystkie lokalizacje do przeprowadzania samooceny, a wszystkie raporty z samooceny muszą być przekazywane do funkcji centralnej w celu rejestracji i przeglądu. Zapisy muszą być przechowywane przez co najmniej dwa (2) lata.	(A)	(B)	(C)
9.3.2	Jednostka centralna musi zapewnić, że wszystkie działania SCAR wynikające z samooceny i audytów są odpowiednio zamykane w celu doskonalenia systemów zarządzania bezpieczeństwem.	(A)	(B)	(C)
9.3.3	Wszystkie lokalizacje muszą przekazywać do jednostki centralnej aktualizacje postępów oraz raporty dotyczące wszystkich otwartych SCAR. Jednostka centralna musi eskalować sprawę do kierownictwa LSP/Wnioskodawcy, jeśli SCAR nie zostaną zamknięte przed wyznaczonym terminem. Zapisy muszą być przechowywane przez co najmniej dwa (2) lata.	(A)	(B)	(C)

9.4 Rejestry inspekcji, dzienniki (rejestry odwiedzających/kierowców), kontrole 7-punktowe

Req. No.	Requirements / Controls	Applicable Level		
9.4.1	Jednostka centralna musi posiadać procedury zapewniające, że wszystkie lokalizacje prowadzą rejestry inspekcji, rejestry odwiedzających, rejestry kierowców oraz dokumentację kontroli 7-punktowej itp.	Ⓐ	Ⓑ	Ⓒ

9.5 Ocena ryzyka dla wszystkich lokalizacji

Req. No.	Requirements / Controls	Applicable Level		
9.5.1	Jednostka centralna musi posiadać procedury zapewniające, że odpowiednie oceny ryzyka oraz zarządzanie ryzykiem są przeprowadzane we wszystkich lokalizacjach, a ich zapisy są przechowywane przez co najmniej dwa (2) lata.	Ⓐ	Ⓑ	Ⓒ

9.6 Układ CCTV/VSS i systemu alarmowego obiektu

Req. No.	Requirements / Controls	Applicable Level		
9.6.1	Jednostka centralna musi posiadać procedury zapewniające, że wszystkie lokalizacje dokonują przeglądu i utrzymują dokumentację dotyczącą wszystkich fizycznych systemów bezpieczeństwa, takich jak CCTV oraz układ systemów alarmowych..	Ⓐ	Ⓑ	Ⓒ

9.7 Rejestry systemów alarmowych i kontroli dostępu

Req. No.	Requirements / Controls	Applicable Level		
9.7.1	Jednostka centralna musi posiadać procedury zapewniające, że wszystkie systemy alarmowe oraz kontroli dostępu są utrzymywane i testowane w celu zapewnienia ich skuteczności operacyjnej.	Ⓐ	Ⓑ	Ⓒ
9.7.2	Jednostka centralna musi posiadać procedury zapewniające, że wszystkie lokalizacje prowadzą rejestry wszystkich testów systemów wykrywania włamań i kontroli dostępu oraz incydentów z nimi związanych.	Ⓐ	Ⓑ	Ⓒ

9.8 Rejestry szkoleń

Req. No.	Requirements / Controls	Applicable Level		
9.8.1	Jednostka centralna powinna mieć procedury, które zapewnią, że wszystkie lokalizacje prowadzą właściwe zapisy szkoleń w zakresie zarządzania bezpieczeństwem swoich pracowników.	Ⓐ	Ⓑ	Ⓒ
9.8.2	Jednostka centralna musi posiadać procedury zapewniające, że wszystkie lokalizacje prowadzą rejestry szkoleń z zakresu bezpieczeństwa dla całego personelu. Zapisy muszą być przechowywane przez co najmniej dwa (2) lata.	Ⓐ	Ⓑ	Ⓒ

9.9 Rejestry weryfikacji / sprawdzania

Req. No.	Requirements / Controls	Applicable Level		
9.9.1	Jednostka centralna musi posiadać procedury zapewniające, że wszystkie lokalizacje dokonują przeglądu rejestrów weryfikacji i sprawdzania w regularnych odstępach czasu, aby zapewnić integralność i skuteczność systemów zarządzania bezpieczeństwem.	Ⓐ	Ⓑ	Ⓒ
9.9.2	Jednostka centralna musi posiadać procedury zapewniające, że zapisy z przeglądów, w tym ich wyniki oraz działania korygujące/zapobiegawcze (9.1.6), są utrzymywane. Zapisy muszą być przechowywane przez co najmniej dwa (2) lata.	Ⓐ	Ⓑ	Ⓒ

9.10 Przegląd zarządzania w celu oceny samoaudytów; zgłoszonych SCAR; strat, kradzieży; ocen ryzyka

Req. No.	Requirements / Controls	Applicable Level		
9.10.1	Jednostka centralna musi co najmniej przeprowadzać regularne przeglądy zarządzania w celu zapewnienia zgodności, skuteczności oraz doskonalenia systemów zarządzania bezpieczeństwem.	Ⓐ	Ⓑ	Ⓒ
9.10.2	Przeglądy zarządzania muszą obejmować m.in. skuteczność samoaudytów, zamykanie SCAR, oceny ryzyka, incydenty oraz działania doskonalące.	Ⓐ	Ⓑ	Ⓒ
9.10.3	Jednostka centralna musi przechowywać zapisy wszystkich przeglądów zarządzania przez co najmniej dwa (2) lata.	Ⓐ	Ⓑ	Ⓒ

8.0 Zagrożenia IT i cyberbezpieczeństwa – opcja rozszerzona

FSR obejmuje opcjonalne rozszerzenia dotyczące zagrożeń IT i cyberbezpieczeństwa, które są uznawane za wyższy poziom ochrony i mogą być stosowane dodatkowo do modułów. Opcja ta może zostać wybrana przez LSP/Wnioskodawcę i/lub jego Nabywcę jako dodatkowe wymagania dla potrzeb bezpieczeństwa operacyjnego. Jeśli ta opcja zostanie wybrana na etapie oceny przedcertyfikacyjnej jako część audytu certyfikacyjnego, wszystkie wymagania stają się obowiązkowe.

Opcja rozszerzona w ramach TAPA FSR zapewnia podstawowy poziom kontroli IT i cyberbezpieczeństwa na poziomie lokalizacji. Członkowie są zdecydowanie zachęceni do wdrożenia standardów Cyber Security Standards (CSS), aby osiągnąć bardziej kompleksowe i solidne ramy cyberbezpieczeństwa.

E8. Wymagania obowiązkowe

Req. No.	Requirements / Controls
E8.1.1	LSP/Wnioskodawca musi posiadać polityki bezpieczeństwa dotyczące zagrożeń IT i cyberbezpieczeństwa. Polityki mogą być odrębne lub połączone w jednym dokumencie. Muszą one określać: 1. Działania LSP/Wnioskodawcy w zakresie identyfikacji i reagowania na zagrożenia. 2. Polityki i procedury służące ochronie, wykrywaniu, testowaniu oraz reagowaniu na zdarzenia bezpieczeństwa. 3. Metody odzyskiwania systemów IT i/lub danych. 4. Protokół komunikacji z Nabywcami/Klientami w celu ograniczenia wpływu incydentu na łańcuch dostaw w ciągu 24 godzin od jego wykrycia. 5. Sposób corocznego przeglądu polityk oraz ich aktualizacji w razie potrzeby.
E8.1.2	LSP/Wnioskodawca musi zapewnić szkolenie z zakresu świadomości bezpieczeństwa informacji wszystkim pracownikom. Szkolenie to musi: 1. Obejmować role i obowiązki użytkowników komputerów w zakresie utrzymania bezpieczeństwa oraz związane z tym korzyści. 2. Posiadać system zapewniający, że rejestry osób, które odbyły szkolenie, są prowadzone i przechowywane przez co najmniej 2 lata.
E8.1.3	LSP/Wnioskodawca musi posiadać pisemną politykę zapewniającą wdrożenie środków cyberbezpieczeństwa u podwykonawców i/lub dostawców, która gwarantuje, że: 1. Wymagania LSP/Wnioskodawcy dotyczące cyberbezpieczeństwa są komunikowane podwykonawcom i/lub dostawcom oraz uwzględnione w umowach. 2. W przypadku gdy podwykonawcy i/lub dostawcy nie uznają lub odmawiają wdrożenia wymagań cyberbezpieczeństwa LSP/Wnioskodawcy, istnieją udokumentowane środki ograniczające ryzyko dla wymagań cyberbezpieczeństwa LSP/Wnioskodawcy oraz jego klientów.

E8.1.4	LSP/Wnioskodawca musi posiadać plan ograniczania skutków przerw w zasilaniu (np. alternatywne źródło zasilania lub generator zapasowy), który zapewnia zasilanie krytycznych systemów IT (określonych w lokalnej ocenie ryzyka) przez co najmniej 48 godzin.
E8.1.5	Systemy informatyczne LSP/Wnioskodawcy muszą być wyposażone w licencjonowane oprogramowanie antywirusowe i antymalware, zawierające najnowsze aktualizacje.
E8.1.6	LSP/Wnioskodawca musi posiadać odpowiedni plan odtwarzania po awarii IT (DRP – Disaster Recovery Plan) umożliwiający odzyskanie systemów po atakach naruszających ich integralność, w tym m.in. wszystkie niezbędne kopie zapasowe danych i oprogramowania oraz procedury ich odtwarzania.
E8.1.7	Systemy informatyczne LSP/Wnioskodawcy muszą być objęte kopiami zapasowymi. Kopie te muszą być regularnie testowane, a dane kopii zapasowych muszą być szyfrowane i przechowywane w drugiej, zewnętrznej lokalizacji.
E8.1.8	LSP/Wnioskodawca musi wdrożyć politykę dla wszystkich kont użytkowników w celu zarządzania i kontroli dostępu do systemów informatycznych poprzez stosowanie unikalnych identyfikatorów użytkowników oraz silnych haseł. Muszą istnieć procedury zapewniające, że: 1. Funkcjonuje program audytu zgodności haseł. 2. Każdemu nowemu kontu przypisywane jest unikalne hasło początkowe w momencie jego utworzenia. 3. Hasła początkowe nie mogą zawierać imienia/nazwiska użytkownika, numeru identyfikacyjnego ani opierać się na standardowych wzorcach wynikających z danych użytkownika. 4. Hasła są przekazywane użytkownikom w sposób bezpieczny i wyłącznie po zweryfikowaniu ich tożsamości. 5. Użytkownicy są zobowiązani do zmiany hasła przy pierwszym logowaniu. 6. Hasła muszą być zmieniane co najmniej co 90 dni.

Informacja: udostępnione Państwu tłumaczenie Standardu na język krajowy ma na celu ułatwienie zrozumienia wymagań TAPA 2026. Tłumaczenie Standardu zostało przygotowane i zweryfikowane zgodnie z najlepszą wiedzą oraz z uwzględnieniem niezbędnych podstaw merytorycznych. Jednakże na potrzeby audytu wersją wiążącą jest i pozostaje angielska wersja oryginalna danego Standardu.

Informacje o publikacji i prawach autorskich

Niniejszy dokument został opublikowany przez Transported Asset Protection Association (TAPA).

© TAPA 2026–2029

Wszelkie prawa zastrzeżone. Żadna część niniejszej publikacji nie może być powielana, przechowywana w systemie odzyskiwania danych ani przekazywana w jakiegokolwiek formie lub w jakiegokolwiek sposób — elektroniczny, mechaniczny, poprzez kopiowanie, nagrywanie lub inny — bez uprzedniej pisemnej zgody TAPA, z wyjątkiem przypadków dozwolonych przez obowiązujące przepisy prawa autorskiego.

Informacja o prawach autorskich zawarta w niniejszym dokumencie wskazuje rok, w którym dokument został ostatnio wydany.

Historia publikacji

Pierwsza publikacja: wrzesień 2026

Obecne wydanie opublikowane w: wrzesień 2026

Niniejsza Publicznie Dostępna Specyfikacja (PAS) wchodzi w życie 15 września 2026 r.

Status dokumentu

Niniejszy dokument stanowi TAPA Facility Security Requirements (FSR) – rewizja 2026 i określa podstawowe wymagania dotyczące bezpieczeństwa obiektów w ramach systemu certyfikacji TAPA.

Dokument pozostaje ważny do momentu jego zastąpienia, zmiany lub wycofania przez TAPA.

TAPA może w przyszłości publikować rewizje, aktualizacje lub poprawki w celu odzwierciedlenia zmieniających się zagrożeń bezpieczeństwa, praktyk branżowych oraz rozwoju technologicznego.

Wykorzystanie dokumentu

Zgodność z niniejszą specyfikacją może być wykorzystywana jako część procesu certyfikacji TAPA dla obiektów obsługujących ładunki o wysokiej wartości i podatne na kradzież.

Organizacje wdrażające tę specyfikację są odpowiedzialne za zapewnienie spełnienia wszystkich obowiązujących wymagań prawnych, regulacyjnych i operacyjnych, oprócz wymagań opisanych w niniejszym dokumencie..