TOOLBOX

‘WEERBAAR BEDRIJF TEGEN SMOKKEL EN LADINGDIEFSTAL’

Versie juli 2024

TOOLBOX ‘WEERBAAR BEDRIJF TEGEN SMOKKEL EN LADINGDIEFSTAL’

Met deze toolbox kunnen bedrijven in transport en logistiek maatregelen nemen om te voorkomen dat de organisatie en medewerkers (on)bewust slachtoffer worden van georganiseerde criminaliteit. De nadruk ligt op vormen van smokkel en ladingdiefstal.

Ondernemers in transport en logistiek zijn zich soms onvoldoende bewust van de risico’s op smokkel en ladingdiefstal. Ze weten ook onvoldoende welke maatregelen zij kunnen nemen. Deze toolbox helpt hen daarbij.

Deze toolbox is opgedeeld in verschillende onderdelen:

De toolbox geeft handvatten voor het nemen van maatregelen op basisniveau. Voor verdieping en ondersteuning op maat, kun je terecht bij derden. Een overzicht van dit aanbod is bijgevoegd.

Hoe gebruik je de toolbox?

Maak iemand binnen je organisatie eigenaar van het traject. Het beste is een lid van het managementteam of een veiligheidsfunctionaris. Start met het inventariseren van de risicovolle goederenstromen binnen het bedrijf. Doe dit samen met collega’s die hier inzicht in kunnen geven. Je kunt vervolgens kiezen welke maatregelen je het eerst implementeert. Betrek per onderdeel de betreffende disciplines. Die onderdelen zijn: fysieke weerbaarheid (veiligheid/beveiliging), digitale weerbaarheid (ICT), sociale weerbaarheid (HR/personeelszaken) en ‘ken-je-klant’ (commercie/customer service).

Voor een effectieve aanpak wordt sterk aanbevolen om alle stappen per onderdeel strikt te doorlopen. Je kunt vervolgens binnen de onderdelen ‘shoppen’ in de verschillende geadviseerde maatregelen om zo een plan op te stellen dat past bij jouw bedrijf.

TIP:

Kleine stappen zijn een goed begin en vaak noodzakelijk voor verandering. Maak een realistisch tijdpad en stel een prioritering op van de maatregelen. Doe dat in samenspraak met de betreffende organisatieonderdelen.

Let op!

Voor het doorvoeren van een groot aantal maatregelen is toestemming nodig van de ondernemingsraad. Betrek die er op tijd bij.

ACHTERGRONDINFORMATIE

SMOKKEL EN LADINGDIEFSTAL IN TRANSPORT EN LOGISTIEK

1. Hoe criminelen misbruik maken van de legale goederenstromen

Elke crimineel heeft transport nodig. Criminelen liften mee op legale goederenstromen om illegale goederen van A naar B te verplaatsen. Daarnaast kunnen legale goederen die worden vervoerd, doelwit zijn van ladingdiefstal.

Criminelen maken op de volgende wijzen misbruik van transport en logistiek:

- **Dekmantelbedrijven**
  Ze richten (transport)bedrijven op om smokkel en criminaliteit mogelijk te maken. Procedures omtrent 'Ken-je-klant' zijn daarom van belang, zodat je controleert of je met een bonafide partij zakendoet.
- **Particuliere zending**
  Particulieren kunnen sommige bedrijven in transport en logistiek inschakelen voor zendingen. Denk aan zendingen van stukgoed of (post-)pakketten. Dat kunnen ook illegale goederen zijn.
- **Corrumperen van personeel**
  Criminelen ronselen medewerkers van bonafide transport- of logistieke bedrijven.
- **Infiltreren in bestaande bedrijven**
  Dit wordt gedaan door te solliciteren op vacatures (ook bij derden).
- **Fysiek of digitaal inbreken**
  Denk aan inbraak in systemen, bedrijven en/of het vervoermiddel.

2. Wat criminelen nodig hebben

Er zijn drie voorwaarden voor het kunnen plegen van smokkel en ladingdiefstal in georganiseerd verband: informatie, toegang en mensen. Het betreft:

- **Informatie** over goederenstromen en logistieke processen. Het gaat bijvoorbeeld om vrachtbrieven, planningen, boekingslijsten, tijdslots en pincodes, locaties van goederen en containers, transportroutes, informatie over processen, beveiliging en werkwijzen van specifieke terminals en transportbedrijven.
- **Toegang** tot beveiligde terreinen en/of het vervoermiddel. Denk aan toegang tot terminals, loodsen, warenhuizen, schepen, vrachtwagens en treinwagons.
- **Mensen** die het werk uitvoeren: het verrichten van de handelingen om drugs of goederen in bezit te krijgen.

3. Kwetsbaarheden in een organisatie

Een organisatie kan op twee vlakken kwetsbaar zijn:

- Kwetsbaarheid in techniek en processen.
  Dit betreft kwetsbaarheden in systemen en processen binnen de organisatie die gelegenheid bieden voor smokkel. Bijvoorbeeld onvoldoende beveiligingsmaatregelen of logistieke processen die gemakkelijk beïnvloedbaar zijn.
- Kwetsbaarheid in de mens.
  Dit gaat over zowel sociale als culturele factoren die maken dat mensen (on)bewust meewerken aan smokkel en diefstal.

Maatregelen rondom processen en techniek in de organisatie

Maatregelen om processen en techniek in de organisatie te beschermen zijn opgedeeld in twee onderdelen. Met digitale weerbaarheid wordt het beschermen en afschermen van informatie- en communicatietechnologie (ICT) bedoeld. Fysieke weerbaarheid gaat over het beschermen en afschermen van locaties en vervoermiddelen.

Maatregelen rondom de factor mens

Gedrag staat niet op zichzelf en wordt door allerlei factoren beïnvloed. Er zijn veel verschillende soorten gedrag: onbewust en bewust, rationeel en irrationeel. Centraal staat de vraag: 'Wat kun je als organisatie doen om gedrag van medewerkers positief te beïnvloeden en ervoor te zorgen dat medewerkers niet corrumperen?'. Deze maatregelen vallen onder sociale weerbaarheid.

4. Integriteitsschendingen in transport en logistiek

Onder het schenden van integriteit wordt verstaan:

- Onjuiste omgang met (vertrouwelijke) informatie ('lekken').
- Contacten met criminelen (in de familiesfeer, kennissenkring enz.).
- Niet optreden tegen activiteiten met criminaliteit als doel.
- Mogelijk maken van activiteiten met criminaliteit als doel.
- Advies geven aan leden van criminele samenwerkingsverbanden.

STAPPENPLAN VOOR BEDRIJVEN MET PERSONEEL

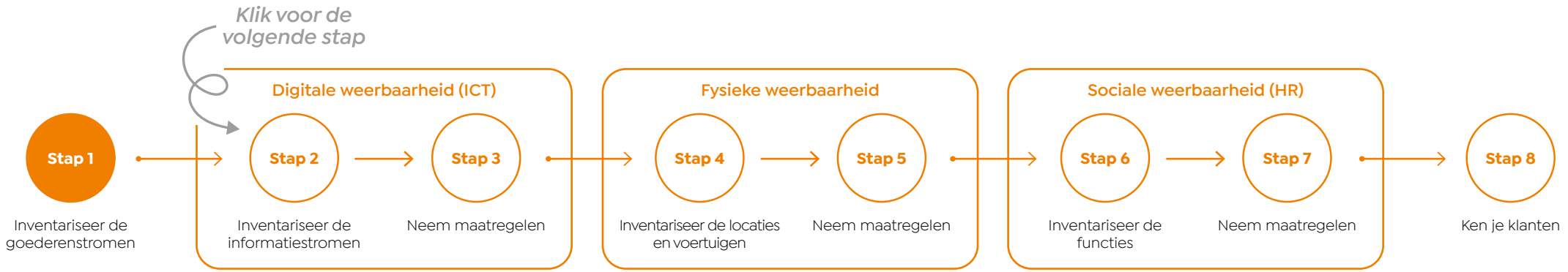
STAP 1 INVENTARISEER JE GOEDERENSTROMEN

Inventariseer de goederenstromen voor je organisatie

- Bekijk onderstaande lijst en weeg intern de risico's voor jouw bedrijf en (specifieke) transporten af. Uit onderzoek en de praktijk blijkt dat deze transporten een hoog risico vormen:

  - Transporten (in het bijzonder lijndiensten) met een goederenstroom uit Zuid-Amerika. Alle goederen uit Zuid-Amerika en aanverwante vervoersbewegingen via zee, weg, spoor, binnenvaart of lucht lopen het risico op vervoeren van cocaïne.
  - Transporten met een goederenstroom naar Engeland of Scandinavië. Zowel over zee, via de weg, het spoor en door de lucht is er een risico op mensensmokkel, verstekelingen (voornamelijk bij ferrydiensten) en smokkel van accijnsgoederen en drugs.
  - Transporten met een hoge waarde aan goederen of consumentengoederen. Denk hierbij aan auto's, alcohol, elektronica, merkkleding, sigaretten, parfum, medicijnen, maar ook aan dure (zoals edel- en ferro-) metalen. Er is een risico van ladingdiefstal en witwassen.
  - (Groupage) transporten met veel verschillende klanten en tussenstops. Dit geeft een risico op drugssmokkel en inklimmers.
  - Transporten met een (natte bulk) goederenstroom uit Azië (hoofdzakelijk China). Hierbij is er een risico op het importeren van grondstoffen voor de productie van synthetische drugs.
  - Transporten met goederen die op de lijst van drugsprecursoren of precursoren voor explosieven staan. Het risico betreft ladingdiefstal.
  - Transporten met veel particuliere zendingen (stukgoed of pakketten), met een risico op drugssmokkel en witwassen.
  - (Gekoelde) transporten met bederfelijke producten zoals groenten, fruit en bloemen. Deze transporten kennen een snelle afhandeling en doorstroom met een risico op drugssmokkel.

- Sla de inventarisatie van de risicovolle goederenstromen op en neem deze mee naar de volgende blokken. Hoe hoger het risicoprofiel binnen je bedrijf of bij specifieke transporten, hoe meer maatregelen je moet nemen.



STAPPENPLAN VOOR BEDRIJVEN MET PERSONEEL

STAP 2 INVENTARISEER DE INFORMATIESTROMEN

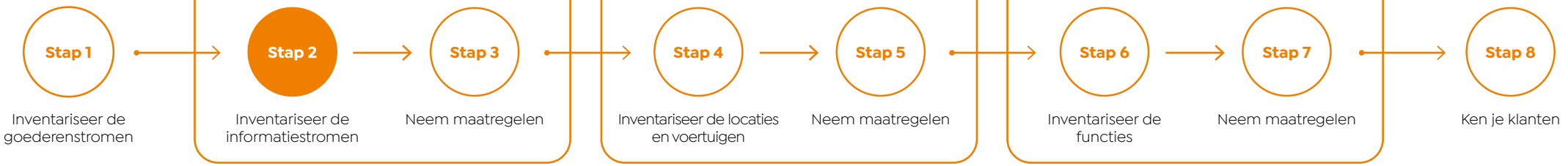
Elke organisatie heeft informatie en systemen die al dan niet risicovol zijn en waar criminelen toegang toe proberen te krijgen.

- Inventariseer de risicovolle informatie in je organisatie. Pak de lijst van risicovolle goederenstromen bij de hand. Informaties en systemen met betrekking tot deze goederenstromen vormen een hoger risico en zijn dus belangrijker om te beschermen. Denk hierbij aan:

  1. Vrachtbrieven.
  2. Logistieke systemen en software zoals Terminal Operating Systemen, boekingssystemen, planningsystemen en douanesystemen.
  3. Pincodes en tijdslots.
  4. Plattegronden.
  5. Planningen (kadeplanning, transportplanning, terminal planning, personeelsplanning).
  6. Locaties van goederen, containers en containernummers.
  7. Transportroutes.
  8. Beveiligingsmaatregelen van terreinen of vervoersmiddelen.
  9. Persoonsgegevens / HR-gegevens.
  10. Boekhouding, financiën, facturatie.

- Inventariseer wie toegang heeft tot welke risicovolle informatie en wie risicovolle handelingen kan verrichten in systemen. Doe dit aan de hand van het beantwoorden van de volgende vragen:

  - Wie heeft binnen de organisatie toegang tot risicovolle informatie en is dat nodig voor de werkzaamheden?
  - Welke risicovolle informatie gaat naar derden en is dat nodig voor de werkzaamheden?
  - Wie kan binnen de organisatie risicovolle handelingen verrichten binnen (logistieke) systemen en is dat nodig voor de werkzaamheden?



STAPPENPLAN VOOR BEDRIJVEN MET PERSONEEL

STAP 3 NEEM MAATREGELEN DIGITALE WEERBAARHEID (ICT AAN ZET)

- **Afschermen**
  Scherm risicovolle informatie af. Beperk handelingen waar mogelijk tot specifieke mappen/informatie door middel van machtigingen in systemen en autorisaties. Bepaal op welke manier hard copy-exemplaren intern zo veilig mogelijk gedeeld en bewaard kunnen worden. Kijk ook kritisch naar welke informatie naar derden gaat.

TIP:
In bepaalde gevallen moet je voor machtigingen in systemen in gesprek met je leverancier.

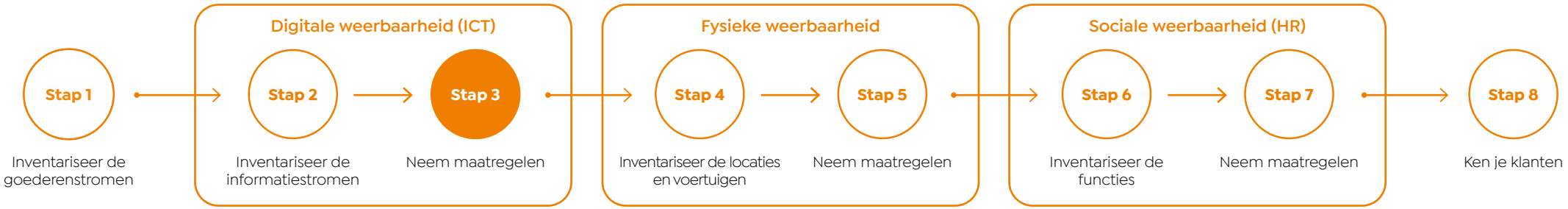
- **Beveiligen**
  Zorg voor deugdelijke beveiliging van ICT. Criminelen proberen systemen te hacken om informatie te verkrijgen of logistieke processen te beïnvloeden.
  Neem de volgende maatregelen:

  - Zorg dat medewerkers hun wachtwoord iedere drie maanden moeten veranderen.
  - Implementeer tweestapsverificatie voor het inloggen op systemen.
  - Kijk kritisch naar de beveiliging van je systemen en ICT-leveranciers, maar ook naar het kennisniveau bij je medewerkers. TLN biedt hiervoor online-hulp op het digitale platform Samen Digitaal Veilig.

TIP:
Ga eerst in gesprek met je ICT-leverancier over de beveiliging, tweestapsverificatie en het regelmatig maken van back-ups. Maak je medewerkers bewust van het gevaar van het klikken op fishing mails en onbetrouwbare linkjes.

Voor verdergaand advies kun je terecht bij derden. Een lijst met gecertificeerde bedrijven vind je hier (onder meer onder het kopje pentest): Bedrijven – Het CCV.

Tips met betrekking tot cybersecurity zijn onder het aanbod van derden aan de toolbox toegevoegd. TLN is aangesloten bij het digitale platform Samen Digitaal Veilig.



STAPPENPLAN VOOR BEDRIJVEN MET PERSONEEL

STAP 4 INVENTARISEER RISICOVOLLE LOCATIES EN VERVOERMIDDELEN

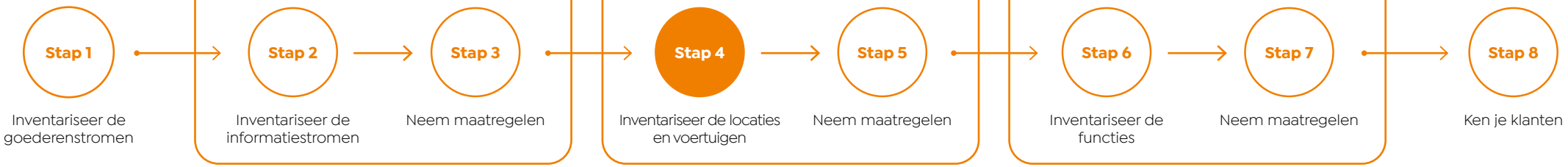
Elke organisatie kent locaties en vervoermiddelen die al dan niet risicovol zijn en waartoe criminelen toegang proberen te krijgen.

- Inventariseer de risicovolle locaties en vervoermiddelen. Pak de lijst van risicovolle goederenstromen bij de hand. Locaties en vervoermiddelen in risicovolle goederenstromen moet je beter beveiligen. Denk daarbij aan:

  1. Toegangspoorten en -wegen.
  2. Schepen.
  3. Loodsen met risicovolle en/of dure goederen.
  4. Kades.
  5. Kantoorruimtes met gevoelige informatie.
  6. (Container)terminals.
  7. Vrachtwagens.
  8. Treinwagons.

- Inventariseer wie toegang heeft tot risicovolle locaties en vervoermiddelen binnen het bedrijf en of dat nodig is. Doe dit aan de hand van de volgende vragen:

  - Welke interne en externe medewerkers hebben toegang tot risicovolle locaties en vervoermiddelen in het bedrijf en is dat nodig voor de werkzaamheden?
  - Is er een aanmeld- en toegangsprocedure, registratie en controle bij de in- en uitgangen van terreinen en risicovolle locaties?



STAPPENPLAN VOOR BEDRIJVEN MET PERSONEEL

STAP 5 NEEM MAATREGELEN FYSIEKE WEERBAARHEID (VEILIGHEID/BEVEILIGING AAN ZET)

- **Compartimenteren**
  Compartimenteer en beperk waar mogelijk de toegang tot risicovolle locaties.
  - Compartimenteer en beperk de toegang door een passensysteem (eventueel met biometrie), hekwerken en waarschuwingsborden. Autoriseer personeel en derden per functie of opdracht tot locaties.
  - Registreer wie waar aanwezig is, via het passensysteem of de beveiliging bij toegangspoorten. ISPS-plichtige bedrijven zijn verplicht een toegangsregistratie te hebben. Zorg eventueel voor visitatie bij in- en uitgangen.

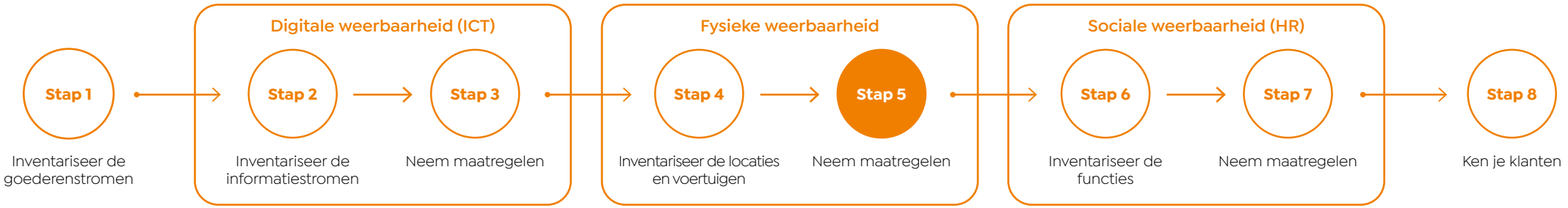
TIP:

Werk met verschillende kleuren veiligheidshesjes voor verschillende afdelingen en locaties.
Denk aan hesjes voor kantoor, warenhuizen, dienstverleners en personen die op schepen moeten komen.

- **Beveiligen**
  Zorg voor een deugdelijke beveiliging van terreinen, loodsen, voer- en vaartuigen. Criminelen proberen immers toegang te krijgen tot locaties en vervoermiddelen. Je kunt voor beveiligingsmaatregelen terecht bij derden.
  - Het CCV heeft een lijst met KIWA- en BORG-gecertificeerde bedrijven opgesteld: Bedrijven – Het CCV.
  - Voor het veilig opslaan en vervoeren van risicogoederen bestaan internationale richtlijnen met bijbehorende certificaten. Dit wordt TAPA FSR-certificering genoemd (Facility Security Requirements - A, B of C). Zie voor meer informatie: Home – TAPA EMEA.
  - Denk bij fysieke maatregelen aan hekwerken, camera's, alarmsystemen, sensoren, mechanische en elektronische sloten op trailers, GPS-tracking in containers/vrachtwagens, startonderbekers, noodknoppen en parkeren op beveiligde parkeerplaatsen. Tips met betrekking tot fysieke beveiligingsmaatregelen zijn onder het aanbod van derden aan de toolbox toegevoegd.

TIP:

Maak geen gebruik van zeilentrailers bij het vervoer van risicogoederen.

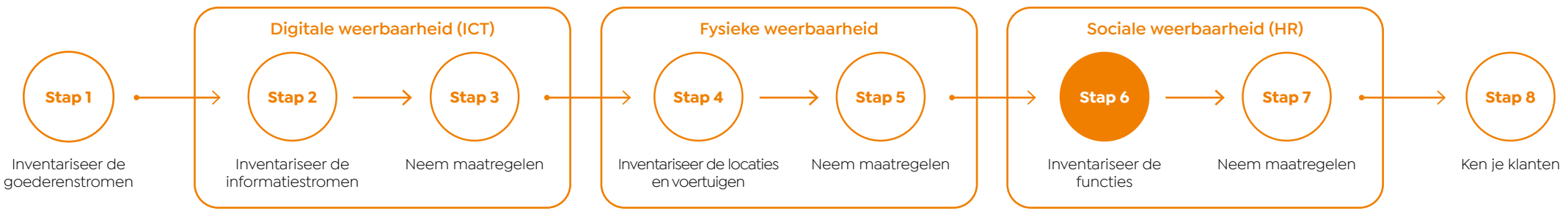


STAPPENPLAN VOOR BEDRIJVEN MET PERSONEEL

STAP 6 INVENTARISEER DE PERSONEELSFUNCTIES IN JE ORGANISATIE

Elke organisatie kent functies die (mogelijk) risicovol zijn en waartoe criminelen toegang proberen te krijgen.

- Inventariseer risicovolle functies in de organisatie. HRM/personeelszaken kan met de leidinggevende op basis van praktijkvoorbeelden functies indelen in laag, middel en hoog risico. Dit geeft een groeiend inzicht waar de risico's liggen. Gebruik hierbij ook de lijst met risicovolle goederenstromen. Functies die hierbij betrokken zijn, lopen een hoger risico. Daarnaast hebben de volgende functies een hoger risico:
  - Functies met toegang tot gevoelige informatie.
  - Functies met toegang tot gevoelige locaties.
  - Functies met een hoge mate van beslissingsbevoegdheid. Denk aan operationeel management, (transport)planners, beveiligingsbeambten, teamleiders en afdelingshoofden (ook van ICT, HR, Financiën en Commercie).
- Neem de lijst van risicovolle functies mee naar de volgende stappen. Bepaal eventueel op basis van de functie welke maatregelen wenselijk zijn.



STAPPENPLAN VOOR BEDRIJVEN MET PERSONEEL

STAP 7 NEEM MAATREGELEN 'SOCIALE WEERBAARHEID'

De mogelijke maatregelen vallen uiteen in de volgende blokken:

Werving en selectie	Tijdens het werk	Uit dienst
Vacaturetekst	Trainingen werknemers	Aandachtspunten bij vertrek
Voorbereiding sollicitatiegesprek	Verkleinen risico's	
Het sollicitatiegesprek	Blijf in gesprek	
Start nieuwe werknemer	Let op signalen	
	Als het toch misgaat	

Werving en Selectie: HRM/Personeelszaken aan zet

Vacaturetekst

Integer personeel begint aan de poort. De vacaturetekst en de website geven direct en indirect een signaal af dat integriteit belangrijk is in de organisatie en dat de sollicitant op haar of zijn integer handelen wordt beoordeeld.

Vacature

- Noem het belang van integriteit expliciet in de beschrijving van de organisatie en vacature.
- Vraag om een CV met daarin opgenomen referenties en contactgegevens.
- Vraag om kopieën van belangrijke diploma's voor de functie.
- Benoem dat een VOG (Verklaring Omtrent het Gedrag) noodzakelijk is voor de functie.
- Vermeld dat een integriteitstest onderdeel kan uitmaken van het gesprek.

Website

- Straal integriteit uit. Dan kan door op de website en sociale media stil te staan bij de normen en waarden van de organisatie en het belang van integriteit.

Voorbereiding sollicitatiegesprek

- Kom meer te weten over de sollicitant en zijn/haar netwerk via openbare bronnen. Dat je dit doet, moet je wel in de vacaturetekst vermelden.
- Neem contact op met de opgegeven referenties.
- Bekijk de opbouw van het CV, wees alert op veel wisselingen of gaten.
- Probeer de motivatie te doorgronden en let op opvallende zaken.
- Doe een check op Waarschuwingsregister Logistieke Sector (WLS). Werknemers in de logistieke sector die integriteitsschendingen hebben begaan, kunnen hier worden geregistreerd. Om het waarschuwingsregister te kunnen raadplegen, is deelname aan het WLS verplicht.

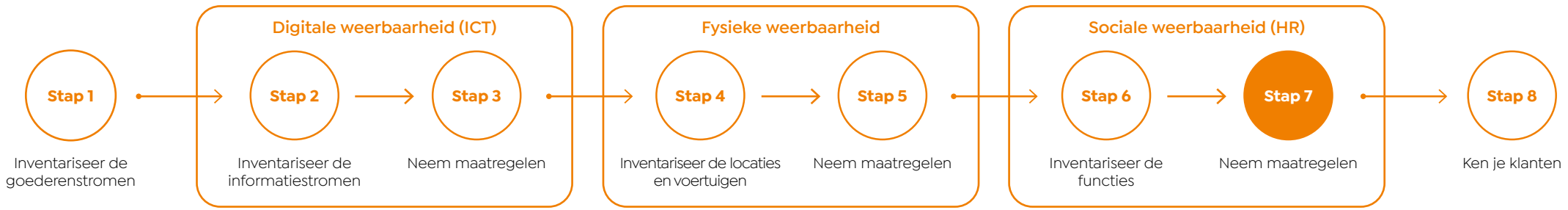
Het sollicitatiegesprek

Ben alert op verdachte achtergronden en gedrag van een sollicitant, zoals de volgende zaken.

- Het is onduidelijk waarom iemand weg is gegaan bij de vorige baan.
- Betrokkene heeft veel verschillende werkgevers binnen de logistieke sector gehad in een korte periode.
- Er is sprake van een onduidelijke motivatie voor het aangaan van deze baan.
- De sollicitatie is onlogisch gezien de woonplaats, opleiding of het carrièreverloop.

Belangrijk voor het sollicitatiegesprek:

- Voer het gesprek met twee personen. Zo kun je beter letten op non-verbaal gedrag.
- Vraag expliciet naar iemands motivatie, achtergrond en opleiding.
- Vraag welke integriteitsaspecten in het werk voor deze persoon belangrijk zijn. Geef iemand integriteitsdilemma's. Voorbeelden:
- Een onbekende benadert je met de vraag om extra geld te verdienen, wat doe je?
- Je ziet een collega bedrijfseigendommen mee naar huis nemen, wat doe je?
- Een collega vraagt om vrachtpapieren die hij/zij niet nodig heeft voor het werk, wat doe je?



STAPPENPLAN VOOR BEDRIJVEN MET PERSONEEL

STAP 7 NEEM MAATREGELEN 'SOCIALE WEERBAARHEID'

Start nieuwe werknemer
Als de nieuwe werknemer start, zijn een startgesprek en goede introductie belangrijk. Integriteit en weerbaarheid zijn belangrijke onderdelen van deze introductie. Zorg dat je de basis op orde hebt met betrekking tot een gedragscode, sanctiebeleid, interne meldprocedure, vertrouwenspersoon en voorlichtingspakket.

Bij de introductie:

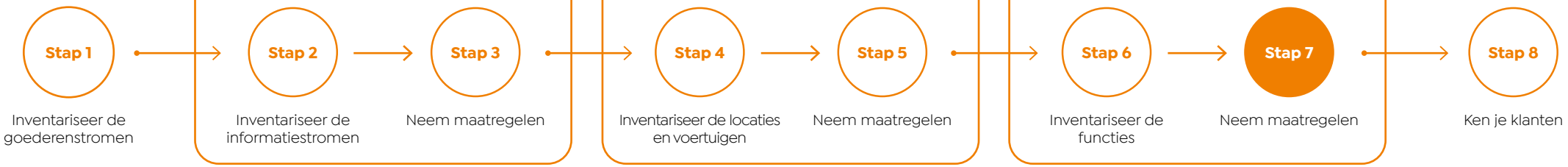
- Vraag om een VOG. Wanneer dat van toepassing is, voeg dan in de aanvraag de volgende zin toe: 'Medewerker wordt tewerkgesteld op …. De medewerker heeft toegang tot kwetsbare ladingen. Er is een hoog risico op transport van verboden middelen en heling'.
- Zorg voor een actuele gedragscode, gekoppeld aan sanctiebeleid en deel deze uit. Een gedragscode geeft duidelijkheid over de normen en waarden. Benoem in de gedragscode voorbeelden van overtredingen rondom criminaliteit en de sancties. Laat medewerkers tekenen voor ontvangst.
- Zorg voor een interne meldprocedure/klokkenluidersprocedure. Informeer de werknemer hoe er intern en extern (en anoniem) gemeld kan worden. (Voor organisaties met meer dan 50 medewerkers is een klokkenluidersprocedure verplicht.) Zie voor meer informatie en hulp bij het inrichten van een interne meldprocedure: Voor werkgevers | Wet bescherming klokkenluiders.
- Stel vertrouwenspersonen aan. Verwijs naar de vertrouwenspersoon als een medewerker ergens vertrouwelijk over in gesprek wil gaan. Denk ook aan het opleiden van vertrouwenspersonen rondom het thema criminaliteit. Mocht je aan de eisen van een klokkenluidersprocedure voldoen, is een vertrouwenspersoon verplicht, zie: Voor werkgevers | Wet bescherming klokkenluiders.
- Geef aan welke hulp en steun de werknemer kan krijgen, in welke gevallen en hoe die eruit ziet. Bijvoorbeeld bij schulden of in geval van incidenten.

Voorlichtingspakket:
Zorg voor een voorlichtingspakket met materiaal dat werknemers moeten doornemen voordat zij starten. Hierbij draait het om het bewust en weerbaar maken van je medewerkers tegenover criminaliteit. Denk als onderdelen van het pakket aan flyers, folders en (e-)learnings.

- Leer medewerkers hoe te voorkomen dat zij benaderd worden door criminelen en hoe hiermee om te gaan als het toch gebeurt.
- Leer medewerkers hoe ze signalen van criminaliteit kunnen herkennen.
- Leer medewerkers hoe te handelen als zij iets zien, iets merken of zelf benaderd worden en waar zij dit kunnen melden. Deel de meldkaart uit.
- Informeer medewerkers om niet in werkkleding over straat te lopen buiten werktijd, de auto van de zaak niet voor de voordeur te parkeren en geen informatie over het werk op sociale media te delen.
- Laat medewerkers hierover met elkaar in gesprek gaan tijdens een 'toolboxmeeting' of training.

Voorlichtingsmateriaal en (e-)learnings zijn bij het aanbod van derden aan de toolbox toegevoegd. Afhankelijk van de regio waarin je bedrijf is gevestigd en de rol in de keten kun je de volgende websites raadplegen voor materiaal: Rotterdamse haven, Veilige haven, Platform Veilig Ondernemen, www.operatiezelos.nl, SterkNoordzeekanaalgebied, SterkeLuchthaven, WeerbaareSierteeltSector, VeiligeZeehavens.

Ga terug naar overzicht



STAPPENPLAN VOOR BEDRIJVEN MET PERSONEEL

STAP 7 NEEM MAATREGELEN 'SOCIALE WEERBAARHEID'

Tijdens het werk

Trainingen werknemers

Waarom is training belangrijk?

- Fysieke trainingen hebben vaak meer effect dan informatie op papier uitdelen en bieden mogelijkheid tot interactie. Herhaal de trainingen elk jaar.

Inhoud van training

- Leer de medewerkers hoe ze kunnen voorkomen dat ze worden benaderd door criminelen en hoe ze moeten handelen als dit toch gebeurt (de 'ronselproof'-training).
- Laat medewerkers oefenen met het herkennen van signalen, hoe te handelen en waar zij dit kunnen melden (de 'security awareness'-training).

Er zijn verschillende aanbieders van ronselproof- en/of security awareness-trainingen. Kijk op:
Rotterdamse haven, Veilige haven, Platform Veilig Ondernemen, www.operatiezelos.nl, SterkNoordzeekanaalgebied, SterkeLuchthaven, WeerbaareSierteeltSector, VeiligeZeehavens.

Verkleinen van risico's

Ongeacht de functie die hij of zij heeft, kan iemand interessant zijn voor criminelen. Dit geldt ook voor uitzendkrachten en stagiairs. Specifieke functies, logistieke processen en taken binnen het bedrijf kunnen extra kwetsbaar zijn. Het is daarom van belang om preventieve maatregelen te nemen.

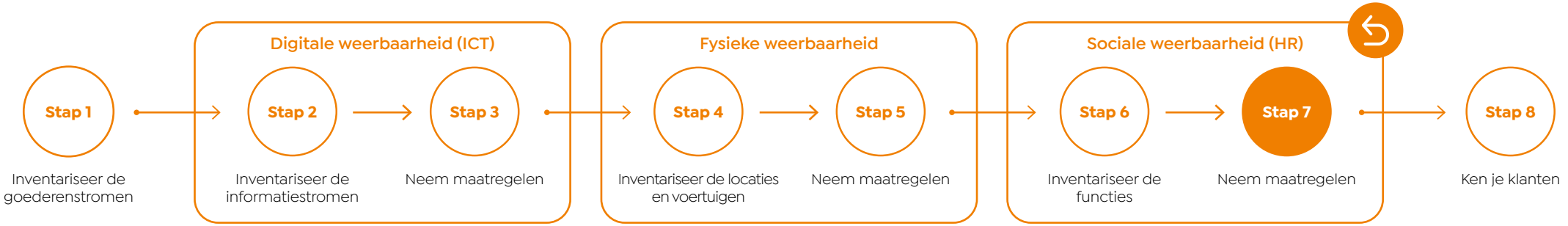
Preventieve maatregelen

- Bespreek als HRM regelmatig de 'kwetsbare' werknemers en observeer. Laat ze (eventueel tijdelijk) niet met risicovolle transporten en goederen werken.
- Zorg voor functiescheiding en vier-ogenprincipe voor kritieke functies. De verantwoordelijkheid voor risicovolle beslissingen moet niet bij één medewerker liggen. Denk aan functies waarbij medewerkers zelfstandig belangrijke beslissingen kunnen nemen in het logistieke proces of anderen kunnen machtigen (zoals forwarding, planning, commercie, veiligheid en beveiliging).
- Een functieroulatie kan helpen voorkomen dat een medewerker een integriteitsrisico loopt.
- Zorg voor roulatie in teams/ploegen/teamleiders. Vaste ploegen kunnen verkeerd gedrag in de hand werken en/of in stand houden.

Blijf in gesprek

Maak weerbaarheid en integriteit een vast onderdeel van het HRM-beleid en geef het een structurele plek in de werkoverleggen en functioneringsgesprekken.

- Ga in gesprek met je werknemers, weet hoe het met ze gaat, zowel op het werk als thuis.
- Maak in functioneringsgesprekken financiële situaties en geldzorgen bespreekbaar en biedt hulp aan. Dat kan op verschillende manieren.
- Het overnemen van de schuld door de organisatie.
- Samen werken aan een plan om de schuld terug te betalen.
- De mogelijkheid bieden om extra te werken.
- Doorverwijzen naar schuldhulpverlening.
- Promoot de vertrouwenspersoon of bedrijfsmaatschappelijk werker bij wie een medewerker (of eventueel partner) terecht kan als er problemen zijn.



STAPPENPLAN VOOR BEDRIJVEN MET PERSONEEL

STAP 7 NEEM MAATREGELEN 'SOCIALE WEERBAARHEID'

Ben alert op risicovolle factoren, zoals schulden, echtscheiding of een te hoge hypotheek. Deze zorgen voor stress en beïnvloeden het nemen van rationele beslissingen. Dergelijke factoren zijn als volgt te herkennen.

- Er is sprake van loonbeslag.
- Er wordt geld geleend van collega's.
- Een medewerker is vaker ziek.
- Een medewerker is minder alert en heeft concentratieproblemen.
- Er wordt gevraagd om een voorschot op salaris of vakantiegeld.
- De medewerker belt tijdens werktijd met schuldeisers en deurwaarders.
- Er is sprake van veelvuldig wisselen van bankrekeningnummers.
- Er is sprake van diefstal.
- De medewerker vraagt om extra shifts of werkuren.

Let op signalen

Het is belangrijk te letten op verdacht gedrag van een werknemer tijdens het werk. Niet alles is meteen reden voor argwaan. Bij meerdere signalen is alertheid wel gewenst.

Ben gewaarschuwd als een werknemer.

- Vaak buiten het rooster om op het werk komt.
- Onlogische planningen maakt of daar zonder reden in wijzigt.
- Vaak op een plek is waar hij of zij niet moet of hoeft te zijn (bijvoorbeeld op een schip).
- Verdacht aan het zoeken is in het systeem.
- Ineens veel dure spullen heeft.
- Anderen vraagt naar informatie die niet nodig is voor het werk.
- Pas, sleutels of codes (steeds) kwijt of vergeten is.
- Vaak een dienst wil ruilen.
- Zich gespannen en/of ontwijkend gedraagt, zich afzondert en/of steeds van de werkplek afgaat.
- Bij ziekte en verlof toch actief is binnen het zoeksysteem of de werkomgeving.

Als het toch misgaat

Als een medewerker in de fout is gegaan, is het belangrijk om als organisatie altijd op te treden.

Duidelijkheid en transparantie

- Leg de werknemer direct uit welke norm is overtreden.
- Leg uit wat het beleid is en wat de organisatie doet om de zaak op te lossen.
- Zorg dat de omgeving bij wie wordt ingegrepen, weet wat er is gebeurd, welke norm is overschreden en welke maatregel is getroffen.
- Geef aandacht aan de betrokken medewerker en zijn of haar partner en gezin.

Uit dienst

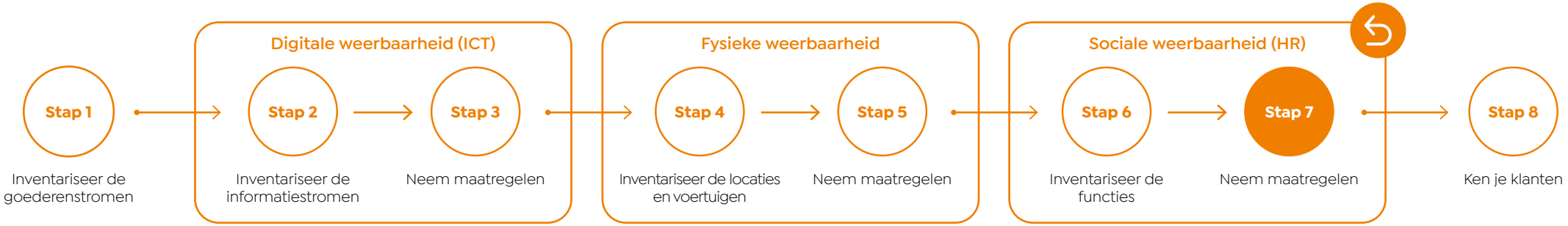
Aandachtspunten bij vertrek van een werknemer

Als een medewerker uit dienst gaat, is dit een goed moment om zicht te krijgen op verbeterpunten voor de organisatie. Dat geldt ook voor het thema criminaliteit. Het is belangrijk om zo snel mogelijk de toegang tot systemen en locaties van betrokkene in te trekken.

- Beperk informatie en toegang tijdens de uitwerkperiode.
- Hef bij uitdiensttreding accounts en toegang tot systemen op en verander wachtwoorden.
- Neem telefoons, laptops en werkkleding op de datum van uitdiensttreding in. Laat dit de medewerker vooraf duidelijk weten.
- Zorg dat je apparaten en hulpmiddelen met kritieke informatie of toegang tot systemen op afstand kunt wissen. (Dit is trouwens ook handig in geval van verlies of diefstal!)

TIP:

- Voer altijd een exitgesprek.
- Vraag naar de reden van vertrek en vraag door. Let extra op als de reden onduidelijk lijkt.
- Vraag naar kwetsbaarheden in de organisatie en verbeterpunten in relatie tot weerbaarheid van de werknemer.



STAPPENPLAN VOOR BEDRIJVEN MET PERSONEEL

STAP 8 KEN JE KLANTEN

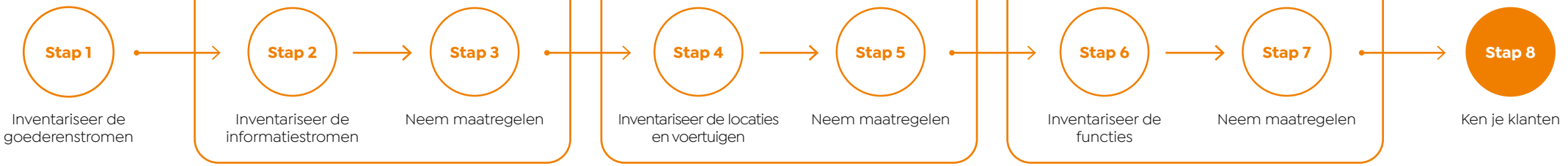
Omdat criminelen ook dekmantelbedrijven opzetten, is het van belang om eisen te stellen aan je klanten en leveranciers. Je moet weten wie ze zijn en de risico's beoordelen. Dit noemen we 'Ken-je-klant'. Je kunt bij derden hulp krijgen om het op maat inregelen van Ken-je-klant-procedures. In de basis is het belangrijk om de volgende zaken te controleren en signalen onderling te bespreken.

Ken-je-klant

- Controleer de kredietwaardigheid van de klant. Dit kan via open bronnen, opvragen van gegevens bij de klant of door inschakeling van externe bureaus.
- Controleer altijd of de klant een KvK- en btw-nummer heeft. Controleer naam, adres en vestigingslocatie. Let extra goed op als de klant alleen communiceert via Gmail, Hotmail of WhatsApp en geen eigen website heeft. Ben alert als websites 'under construction' zijn.
- Vraag om een kopie van de verzekeringspolis (met sluitende dekking en bijbehorend betalingsbewijs) en doe eventueel navraag bij de verzekeraar.
- Laat bij nieuwe klanten opdrachten altijd schriftelijk bevestigen.
- Controleer of het afleveradres bestaat en of de functie van het pand overeenkomt met wat je kunt verwachten (dat kan eenvoudig via Google Maps).
- Controleer of de transportonderneming waarmee je zakendoet beschikt over een NIWO-vergunning: Zoek vergunninghouders - NIWO.
- Raadpleeg de website van Fenex om te controleren of een expediteur is aangesloten en onder de bijbehorende voorwaarden valt: Vind een expediteur - Fenex.
- Werk zoveel mogelijk met vertrouwde en bekende logistieke partners. Wees bijvoorbeeld voorzichtig met zzp'ers.

Signalen voor alertheid

- Een klant komt weinig professioneel over en heeft weinig verstand van de sector en de zaken die worden geïmporteerd/geëxporteerd.
- De afleverlocatie is onduidelijk; er wordt ineens om een extra tussenstop verzocht of de afleverlocatie is niet ingericht op de te ontvangen goederen (bijvoorbeeld fruit bij een warenhuis zonder koelinstallaties).
- Informatieverzoeken van een klant of collega komen niet via de gebruikelijke wijze binnen (denk aan vrachtpapieren, pincodes, status van een container of goederen).
- Een (nieuwe) klant of partij is onbekend. Bijvoorbeeld niet vindbaar op het internet, zonder KvK-inschrijving en geen eigen website (of een site 'under construction'). Let extra goed op als alleen wordt gecommuniceerd via Gmail, Hotmail of WhatsApp.
- Het is onduidelijk wie de klant of opdrachtgever is en er wordt moeilijk gedaan met identificatie. Of er wordt met veel tussenpersonen gewerkt.
- De waarde van de zending staat niet in verhouding tot de kosten. Denk aan vreemde en onlogische goederen (bijvoorbeeld kroketten uit Suriname).
- Er zijn vreemde, niet-kloppende of helemaal geen goederenomschrijvingen en/of vrachtpapieren.
- De klant is nog maar een paar maanden actief.



INSTRUCTIE

‘WEERBAAR TEGEN SMOKKEL EN LADINGDIEFSTAL’

Met deze instructie kunnen ondernemers zonder personeel in transport en logistiek (‘Eigen rijders’) maatregelen nemen om te voorkomen dat zij (on) bewust slachtoffer worden van georganiseerde criminaliteit. De nadruk ligt op vormen van smokkel en ladingdiefstal.

Inleiding en gebruik instructie

Ondernemers in transport en logistiek zijn zich soms nog onvoldoende bewust van de risico’s voor smokkel en ladingdiefstal. Ze weten vaak onvoldoende welke maatregelen zij kunnen nemen. De toolbox helpt bij het nemen van preventieve maatregelen op basisniveau. Deze instructie is vooral gericht op de transportopdracht en is opgebouwd uit twee blokken:

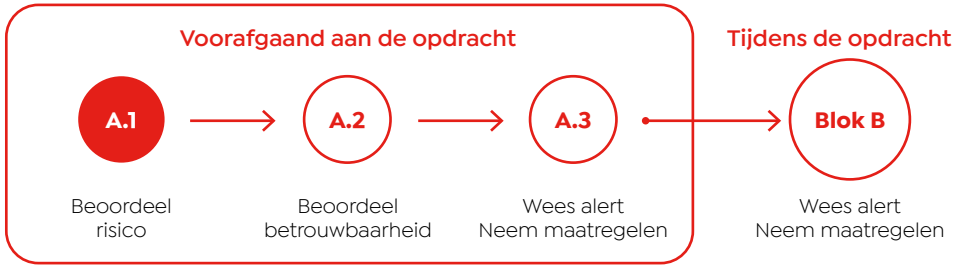
Blok A: Voorafgaand aan de opdracht.

Blok B: Tijdens de opdracht.

Blok A: Voorafgaand aan de opdracht

A.1 Beoordeel het risico van het transport

- Bepaalde transporten vormen een hoger risico voor smokkel en ladingsdiefstal. Weeg voordat je een opdracht aanneemt, het risico van de opdracht af. Dan kun je gepaste maatregelen nemen. Het gaat om de volgende transporten:
  - Transporten (en in het bijzonder lijndiensten) met een goederenstroom uit Zuid-Amerika. Alle goederen uit Zuid-Amerika en aanverwante vervoersbewegingen via zee, weg, spoor, binnenvaart of lucht lopen het risico op vervoeren van cocaïne.
  - Transporten met een goederenstroom naar Engeland of Scandinavië. Zowel over zee, via de weg, het spoor en door de lucht is er een risico op mensensmokkel, verstekelingen (voornamelijk bij ferrydiensten) en smokkel van accijnsgoederen en drugs.
  - Transporten met een hoge waarde aan goederen of consumentengoederen. Denk hierbij aan auto’s, alcohol, elektronica, merkkleding, sigaretten, parfum, medicijnen, maar ook dure (zoals edel- en ferro-)metalen. Er is een risico van ladingdiefstal en witwassen.
  - (Groupage) transporten met veel verschillende klanten en tussenstops. Dit geeft een risico op drugssmokkel en inklimmers.
  - Transporten met een (natte bulk) goederenstroom uit Azië (hoofdzakelijk China). Hierbij is er een risico op het importeren van grondstoffen voor de productie van synthetische drugs.
  - Transporten met goederen die op de lijst van drugsprecursoren of precursoren voor explosieven staan. Het risico betreft ladingdiefstal.
  - Transporten met veel particulieren zendingen (stukgoed of pakketten), met een risico op drugssmokkel en witwassen.
  - (Gekoelde) transporten met bederfbare producten zoals groenten, fruit en bloemen. Deze transporten kennen een snelle afhandeling en doorstroom met een risico op drugssmokkel.
- Hoe hoger het risicoprofiel van specifieke transporten, hoe meer maatregelen je moet nemen.



INSTRUCTIE

‘WEERBAAR TEGEN SMOKKEL EN LADINGDIEFSTAL’

A.2 Identificeer en beoordeel de betrouwbaarheid van de klant

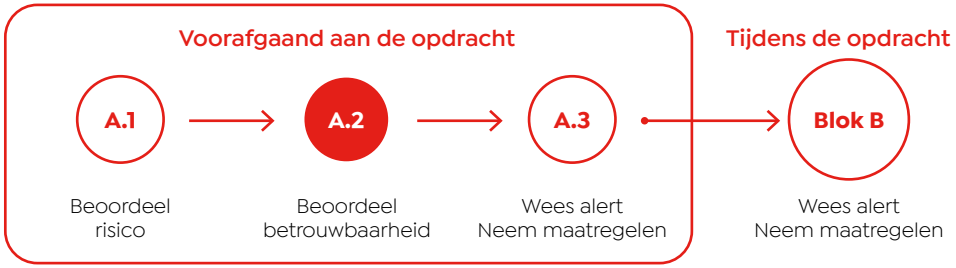
Criminelen zetten vaak ‘dekmantelbedrijven’ op. Dat zijn bedrijven die er legitiem uitzien, maar bedoeld zijn om criminele activiteiten te verhullen. Criminelen kunnen ook infiltreren bij legitieme bedrijven en personeel omkopen of onder druk zetten. Daarom is het van belang om voorafgaand aan de opdracht de klant te identificeren en de risico’s te beoordelen. Vertrouw je het niet? Neem de opdracht niet aan en/of meld je vermoeden.

Ken je klant!

- Controleer de kredietwaardigheid van de klant. Dit kan via open bronnen, opvragen van gegevens bij de klant of door inschakeling van externe bureaus. Accepteer betalingen alleen giraal.
- Controleer altijd of de klant een KvK- en btw-nummer heeft. Controleer naam, adres en vestigingslocatie. Let extra goed op als de klant alleen communiceert via Gmail, Hotmail of WhatsApp en geen eigen website heeft. Let ook als websites ‘under construction’ zijn en ben alert op nepwebsites. Die lijken van een betrouwbare partij te zijn, maar namen zijn net op een andere wijze geschreven.
- Maak altijd gebruik van vrachtbrieven. Zorg altijd dat je weet wat en waar je moet laden/lossen.
- Vraag om een kopie van de verzekeringspolis (met sluitende dekking en bijbehorend betalingsbewijs) en doe eventueel navraag bij de verzekeraar.
- Laat bij nieuwe klanten opdrachten altijd schriftelijk bevestigen.
- Controleer of het afleveradres bestaat en de functie van het pand overeenkomt met wat je kunt verwachten (dat kan eenvoudig via Google Maps).
- Controleer - indien van toepassing - of de transportonderneming waarmee je zakendoet beschikt over een NIWO-vergunning: Zoek Vergunninghouders - Ondernemersloket NIWO.
- Raadpleeg de website van Fenex om te controleren of een expediteur is aangesloten en onder de bijbehorende voorwaarden valt: Vind een expediteur - Fenex.
- Werk zoveel mogelijk met vertrouwde en bekende logistieke partners. Ben extra alert bij gebruik van een vrachtuitwisselingsplatform. Criminelen bieden vrachten ook via deze platformen aan.

Wanneer moet je extra waakzaam zijn?

- Een klant komt weinig professioneel over en heeft weinig verstand van de sector en de zaken die worden geïmporteerd/geëxporteerd.
- De afleverlocatie is onduidelijk; er wordt ineens om een extra tussenstop verzocht of de afleverlocatie is niet ingericht op de te ontvangen goederen (bijvoorbeeld fruit bij een warenhuis zonder koelinstallaties).
- Informatieverzoeken van een klant of collega komen niet via de gebruikelijke wijze binnen (denk aan vrachtpapieren, pincodes, status van een container of goederen).
- Een (nieuwe) klant of partij is onbekend. Bijvoorbeeld niet vindbaar op het internet, zonder KvK-inschrijving en geen eigen website (of een site ‘under construction’). Let extra goed op als alleen wordt gecommuniceerd via Gmail, Hotmail of WhatsApp.
- Het is onduidelijk wie de klant of opdrachtgever is en er wordt moeilijk gedaan met identificatie. Of er wordt met veel tussenpersonen gewerkt.
- De waarde van de zending staat niet in verhouding tot de kosten. Denk aan vreemde en onlogische goederen (bijvoorbeeld kroketten uit Suriname).
- Er zijn vreemde, niet-kloppende of helemaal geen goederenomschrijvingen en/of vrachtpapieren.
- De klant is nog maar een paar maanden actief.



INSTRUCTIE

‘WEERBAAR TEGEN SMOKKEL EN LADINGDIEFSTAL’

A.3 Wees alert en neem preventieve maatregelen

Criminelen hebben voor het uitvoeren van hun smokkelactiviteiten of ladingdiefstal bijna altijd hulp nodig van binnenuit. Als vrachtwagenchauffeur vervul je een belangrijk rol in het logistieke proces. Zo beschik je over toegang, informatie en voer je handelingen uit. Ook jij kunt dus benaderd worden voor hulp of onbewust slachtoffer worden.

Preventieve maatregelen

- Neem nooit extra vracht mee buiten je opdracht om.
- Deel geen informatie over je werk met onbekenden of op sociale media.
- Draag geen werkkleding buiten werktijd.
- Wees alert op een ‘klant’ of ‘collega’ die vraagt naar informatie die hij/zij niet nodig heeft.
- Lees en volg de verschillende (e-)learnings die beschikbaar zijn: Rotterdamse haven, Veilige haven, Platform Veilig Ondernemen, www.operatiezelos.nl, SterkNoordzeekanaalgebied, SterkeLuchthaven, WeerbaareSierteeltSector, VeiligeZeehavens.

Digitale veiligheid

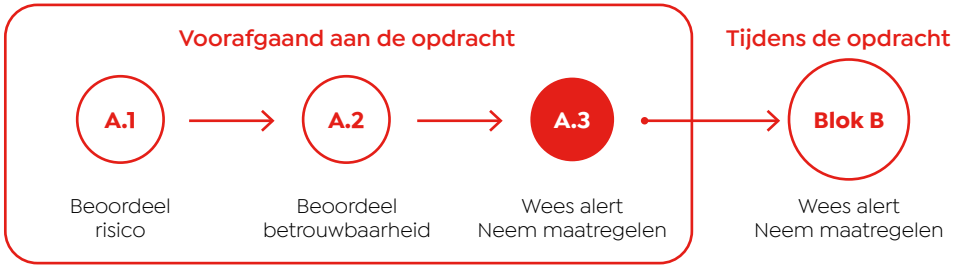
- Zorg ervoor dat je gevoelige informatie veilig opslaat en geen fysieke kopieën laat rondslingeren. Denk bij gevoelige informatie aan vrachtbrieven, transportplanningen, plattegronden, pincodes, tijdslots en transportroutes.
- Zorg voor een deugdelijk beveiliging van transportplatformen en software die je gebruikt. Verander je wachtwoord minimaal iedere drie maanden en gebruik tweestapsverificatie voor het inloggen op systemen.
- Wees alert op fishing mail en onbetrouwbare linkjes.
- Tips met betrekking tot cybersecurity zijn aan de toolbox toegevoegd onder het aanbod van derden.

Fysieke veiligheid

- Zorg voor een deugdelijke beveiliging van je vrachtwagen en eigen oplegger of trailer.
- Het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) heeft een lijst met KIWA- en BORG- gecertificeerde bedrijven opgesteld: Bedrijven – Het CCV.
- Voor het veilig opslaan en vervoeren van risicogoederen bestaan internationale richtlijnen met bijbehorende certificaten. Dit wordt TAPA FSR-certificering genoemd (Facility Security Requirements A, B of C). Zie voor meer informatie: Home – TAPA EMEA.
- Denk bij fysieke maatregelen aan alarmsystemen, mechanische en elektronische sloten, GPS-tracking in containers/vrachtwagens, startonderbekers, noodknoppen en parkeren op beveiligde parkeerplaatsen.
- Voor verdergaand advies kun je terecht bij derden. Zie aanbod van derden.

TIP:

Maak geen gebruik van zeilentrailers bij het vervoer van risicogoederen.



INSTRUCTIE

‘WEERBAAR TEGEN SMOKKEL EN LADINGDIEFSTAL’

Blok B: Tijdens de opdracht

Zorg altijd dat je weet wat voor vracht je vervoert. Hoe hoger het risicoprofiel van specifieke transporten, hoe alerter je moet zijn.

Preventieve maatregelen

- Stop bij risicovolle transporten zo min mogelijk en maak gebruik van beveiligde parkeerplaatsen.
- Zorg dat je altijd zelf bij het laden en lossen aanwezig bent. Controleer indien mogelijk of de goederen overeenkomen met de vrachtbrief.
- Controleer in het geval van containers of het container- en zegelnummer kloppen en of de container niet beschadigd is.
- Zorg dat je altijd de contactgegevens van de opdrachtgever bij de hand hebt.
- Bevestig en beveilig (met sloten) de lading volgens de voorschriften.
- Laat de klant altijd de vrachtbrief of digitaal tekenen voor ontvangst.

Signalen voor waakzaamheid

- De verzegeling op een container klopt niet of ontbreekt.
- De container is beschadigd (vloer, wand, plafond).
- De lading komt niet overeen met de vrachtbrief.
- Je wordt gevolgd door een personenauto.
- Je wordt verzocht opeens naar een andere afloslocatie te rijden.
- Je moet lossen bij een onlogische locatie (geen bedrijfsraam, geen opslagmogelijkheden voor de betreffende goederen, city-box-achtig, afgelegen, onprofessioneel personeel).
- Je mag niet bij het laden of lossen aanwezig zijn.

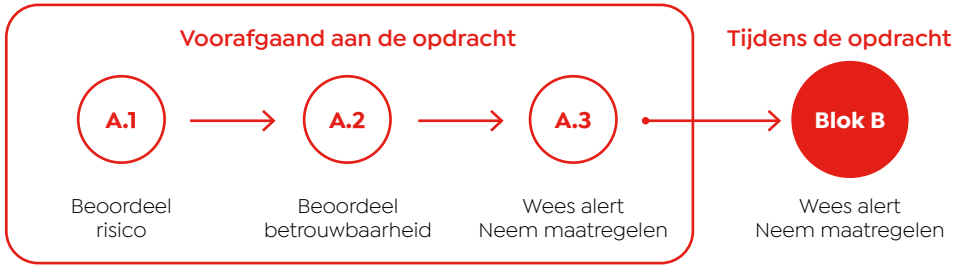
Instructies bij een verdachte situatie of arrestatie

Heb je te maken met een verdacht situatie?

- Direct hulp nodig? Bel altijd 112.
- Kies altijd voor je eigen veiligheid. Doe wat in je macht ligt en je op dat moment veilig acht. Is het voor je eigen veiligheid niet mogelijk om te melden? Doe dan alsnog achteraf een (anonieme) melding. Zie de meldkaart voor de mogelijkheden.

Heb je te maken met een arrestatie?

- Werk altijd mee.
- Vraag indien van toepassing waar je precies van wordt verdacht.
- Vraag indien nodig om juridische bijstand.



IETS VERDACHTS GEZIEN? MELD HET!

DIRECT HULP NODIG? BEL ALTIJD 112

Zo kun je melden

Als je iets vreemds ziet, hoort of meemaakt tijdens je werk, meld het dan.
Zo blijft de sector transport en logistiek een plek waar je veilig kunt werken.
Er zijn allerlei manieren om iets te melden. Ook anoniem.

Binnen je organisatie

- Bespreek het met iemand in je organisatie.
  Bijvoorbeeld een collega of leidinggevende die jij vertrouwt.
- Meld het vertrouwelijk binnen de organisatie, als dit mogelijk is.
  Bijvoorbeeld bij een vertrouwenspersoon of via een anonieme meldprocedure.

Kun of wil je dit niet? Meld dan buiten je organisatie.

- Zie je een verdachte situatie en is er direct actie nodig?
  Bel altijd 112.
- Heb jij iets verdachts gezien, gehoord of meegemaakt?
  Bel de politie via 0900-8844.
- Wil je iets melden over illegale goederen?
  Bel de Douane via 088-6223100.
- Wil je een melding doen over verstekelingen, inklimming of mensensmokkel?
  Bel de Koninklijke Marechaussee via 0800-1814.

Wil je dit niet? Meld dan anoniem.

- Dat kan via Meld Misdaad Anoniem, een onafhankelijk meldpunt waar je gegarandeerd anoniem kunt melden. Bel 0800-7000 of meld online via meldmisdaadanoniem.nl
- Anoniem melden over zware criminaliteit kan ook via Team Criminele Inlichtingen (TCI).
  Bel de politie via 0900-8844 en geef aan dat je anoniem informatie wilt delen met de TCI.

Wat is een goede en zinvolle melding?

Zeg dat het gaat om een situatie in de transport en logistiek. Beschrijf zo precies mogelijk wat je ziet of weet. Belangrijk zijn kenmerken van personen, voertuigen en/of vaartuigen.

OVERZICHT AANBOD VAN DERDEN EN ONDERSTEUNINGSMOGELIJKHEDEN LANDELIJK

Landelijk actief

L Samen Digitaal Veilig (MKB-Nederland, VNO-NCW, TLN en Fenex).

- Vanaf oktober 2024 geldt wetgeving op basis van de Europese NIS2-richtlijn voor de beveiliging van netwerk- en informatiesystemen. Hierdoor zijn bedrijven van meer dan 50 werknemers en kleinere bedrijven in sectoren als transport, verplicht om zorg te dragen voor deugdelijke beveiliging van ICT. Door middel van een audit wordt kritisch gekeken naar je systemen, ICT-leveranciers en het kennisniveau bij je medewerkers. TLN biedt hiervoor online-hulp op het digitale platform Samen Digitaal Veilig.

L Centrum voor Criminaliteitspreventie en Veiligheid (CCV)

- Risicobepaling digitale veiligheid: Informatie & advies - Digital Trust Center. Met de risicobepaling doorloop je een korte vragenlijst. Het resultaat is een overzicht van het risiconiveau van je bedrijf en een advies over te nemen maatregelen: Tools - Digital Trust Center.
- Met de Basisscan Cyberweerbaarheid - Digital Trust Center doorloop je een korte scan van de cyberweerbaarheid van je bedrijf en krijg je een overzicht van aanbevolen basisprincipes. Handige online tools vind je op: Samen Digitaal Veilig.
- Een zogeheten pentest test het niveau van je cybersecurity. Hier vind je een lijst van bedrijven die een pentest aanbieden: Pentest - Het CCV.
- Er is een tool waarmee je de risicoklasse voor inbraak van je bedrijfspand bepaalt: VRKI-tool voor bedrijven - Het CCV.
- Hier vind je een lijst van Kiwa- en BORG-gecertificeerde bedrijven voor het aanleveren van fysieke en digitale beveiligingsmaatregelen en beveiliging: Bedrijven - Het CCV.
- Bij de Hackhelpdesk kun je als ondernemer terecht voor eerste hulp bij cybercrime.

L PVO Nederland

- Algemene tips omtrent veilig ondernemen in de: Transport en logistiek - Platform Veilig Ondernemen.
- Tips over het voorkomen van betrokkenheid bij drugssmokkel: Hoe voorkom ik dat mijn bedrijf betrokken raakt bij drugssmokkel? Platform Veilig Ondernemen.
- Tips over het voorkomen van ladingdiefstal: Hoe voorkom ik ladingdiefstal? - Platform Veilig Ondernemen (pvo-nl.nl).
- Training Agressie & Geweld.
- Training Cybercrime.
- Security Awareness training Ondermijning.
- E-learning Transport & Logistiek (wordt binnenkort gelanceerd).
- 'Red Flags' bij criminele inmenging (in samenwerking met Avans Hogeschool). Signalen voor bedrijven om zelf criminele inmenging te kunnen herkennen: Factsheet transport en groothandels - openresearch.amsterdam.
- Bij de Hackhelpdesk kun je als ondernemer terecht voor eerste hulp bij cybercrime.

L Transport en Logistiek Nederland

- Overzicht waar vrachtwagenchauffeurs veilig kunnen parkeren: IRU - TRANSPark - Parking Area Search.
- E-learning Transport & Logistiek (nog in ontwikkeling).

L Transport Facilitated Organized Crime (TFOC)

- Security awareness-training.
- Actiedagen.
- Operatie Zelos: Operatie Zelos - YouTube / www.operatiezelos.nl.
- Uitleg over TFOC: Ondermijning in de transportbranche | politie.nl en TFOC Dutch - YouTube.
- Contact: transport-facilitated-organized-crime@politie.nl.

L Portbase

- Programma gericht op veilig werken met betrouwbare data en partijen, om (om)bewuste criminaliteit te voorkomen. Voornamelijk gericht op de goederenstromen vanuit de haven. Onder andere om pincode-fraude te voorkomen: Samen Veilig Data Delen - Portbase.

L Landelijk R Regionaal

OVERZICHT AANBOD VAN DERDEN EN ONDERSTEUNINGSMOGELIJKHEDEN REGIONAAL

Noord-Holland

R Mainport Noordzeekanaalgebied
- Op de website vind je verschillende tips over het herkennen, voorkomen en melden van (signalen) van criminaliteit in de haven.
- Verschillende awareness- en weerbaarheidstrainingen voor medewerkers. Onder andere 'ronselproof'-training. Contact: info@sterkNKG.nl.
- Bestellen van meldkaarten voor je bedrijf: info@sterkNKG.nl.
- Advies op maat voor de organisatie: info@sterkNKG.nl.

R Mainport Sierteelt
- Op de website vind je verschillende tips over herkennen, voorkomen en melden van (signalen) van criminaliteit in de sierteelt.
- 'Ronselproof'-training.
- Specifieke kennissessies.
- Weerbaarheidsscan organisatie.
- Controles met getrainde honden.
- Bewustwordingstraining voor medewerkers.
- Sessie kwetsbaarheden in de organisatie – met ex-crimineel.
- Preventief gesprek met een wijkagent.
- Impact van ondermijning op de organisatie – sessie voor MT en leidinggevenden.
- Contact: info@weerbaresierteeltsector.nl.

R Mainport Schiphol (Sterke Luchthaven)
- Website met tips, lesmateriaal voor medewerkers en managers.
- Mainport Schiphol onderhoudt een netwerk van Points of Contact Ondermijning (POCO). Een POCO is een medewerker binnen je bedrijf die wordt aangewezen als interne expert op het gebied van ondermijning. Deze medewerker vervult de rol van aanjager, verbinder en het aanspreekpunt binnen de organisatie en naar externe partners. Mocht je als bedrijf interesse hebben, dan kun je contact opnemen. Een aangewezen medewerker wordt dan opgeleid en aan het netwerk toegevoegd.
- Awareness-training ondermijning, voor het management en/of personeel.
- Advies op maat voor je bedrijf of aansluiten bij trainingen van Sterke Luchthaven kan via www.sterkeluchthaven.nl/bedrijven.

R Platform Veilig Ondernemen Noord-Holland
- Zie landelijke aanbod.
- Training Agressie en Geweld.
- Training Cybercrime.
- Awareness training Ondermijning.
- Contact: www.pvonh.nl.

R Platform Veilig Ondernemen Amsterdam-Amstelland
- Tips omtrent het voorkomen van cybercrime.
- Contact: www.pvo-amsterdamamstelland.nl.

Zuid-Holland

R Mainport Rotterdam/Deltalinqs (Rotterdamse Haven Veilige Haven)
- Website met tips, lesmateriaal voor medewerkers en managers.
- Bestellen van meldkaarten: Rotterdamse Haven Veilige Haven.
- Ronselproof training (trainingscontainer).
- Train-de-trainer toolkit. Toolkit en training waarmee bedrijven zelf aan de slag kunnen om de integriteit en weerbaarheid van de organisatie te verbeteren. Contact: info@rotterdamsehavenveiligehaven.nl.

R Platform Veilig Ondernemen Den Haag
- Zie landelijk aanbod.
- Contact: info@pvo-denhaag.nl.

R Platform Veilig Ondernemen Rotterdam
- Zie landelijke aanbod.
- Ondermijningsboot is een escaperoom gericht op het herkennen van ondermijnende criminaliteit.
- Weerbaarheidstrainingen en bijeenkomsten (ondermijning / cybercrime) voor medewerkers en bedrijven in de transport en logistiek.
- Cybersecurityscan: scan naar de organisatorische maatregelen die het bedrijf heeft genomen, gevolgd door een advies.
- Contact: info@pvo-rotterdam.nl.

OVERZICHT AANBOD VAN DERDEN EN ONDERSTEUNINGSMOGELIJKHEDEN REGIONAAL

R **FERM**
- Platform voor de cyberweerbaarheid van de Rotterdamse haven. Ferm levert actuele en relevantie dreigingsinformatie, gezamenlijke trainingen en opleidingen en een besloten community-platform voor kennisdeling. Bedrijven kunnen zich aansluiten en lid worden via info@ferm-rotterdam.nl.

Noord-Brabant

R **Mainport Zeehavens Zeeland/West-Brabant**
- Website met tips, lesmateriaal voor medewerkers en managers.
- Meldingsbereidheidscampagne 'Wat heb je aan 30.000 euro, als daarna…'? Online en offline middelen, zoals filmpjes, posters en stickers.
- Security awareness training.
- 'Ronselproof'-training.
- 'Ronselproof'-training 2.0 (focus op oefenen).
- HR/leidinggevende training en toolkit.
- Weerbaarheidslearning fysiek en digitaal voor havenmedewerkers.
- Weerbaarheidsscan en ondersteuning bij een weerbare organisatie.
- Contact: tvanvooren@borsele.nl of bmelis@borsele.nl.

R **Platform Veilig Ondernemen Zeeland/West-Brabant en Oost-Brabant**
- Zie landelijke aanbod.
- Security Awareness training transport en logistiek.
- E-learning Transport en Logistiek.
- Advies of gesprek op maat voor je bedrijf.
- Contact: secretariaat@pvo-brabant-zeeland.nl.

Zeeland

R **Mainport Zeehavens Zeeland/West-Brabant**
- Zie onder kopje Noord-Brabant.

R **Platform Veilig Ondernemen Zeeland/West-Brabant**
- Zie landelijke aanbod.
- Security Awareness training transport en logistiek.
- Advies of gesprek op maat voor je bedrijf.
- Contact: secretariaat@pvo-brabant-zeeland.nl.

Limburg

R **Platform Veilig Ondernemen Limburg**
- Zie landelijk aanbod.
- Contact: pvo-limburg.nl/contact/

Flevoland

R **Platform Veilig Ondernemen Midden-Nederland**
- Zie landelijk aanbod.
- Contact: info@pvo-middennederland.nl.

Utrecht

R **Platform Veilig Ondernemen Midden-Nederland**
- Zie landelijk aanbod.
- Contact: info@pvo-middennederland.nl.

Friesland

R **Platform Veilig Ondernemen Noord-Nederland**
- Zie landelijk aanbod.
- Contact: info@pvo-middennederland.nl.

Groningen

R **Platform Veilig Ondernemen Noord-Nederland**
- Zie landelijk aanbod.
- Contact: info@pvo-middennederland.nl.

Drenthe

R **Platform Veilig Ondernemen Noord-Nederland**
- Zie landelijk aanbod.
- Contact: info@pvo-noordnederland.nl.

Overijssel

R **Platform Veilig Ondernemen Oost-Nederland**
- Zie landelijk aanbod.
- Contact: info@pvo-oostnederland.nl.

Gelderland

R **Platform Veilig Ondernemen Oost-Nederland**
- Zie landelijk aanbod.
- Contact: info@pvo-oostnederland.nl.