



CONSULTANCY • CARGO SMARTPOINT • CARGO SECURITY
GROUND CREW TRAINING CENTRE

Rapportage security audit luchtvracht Erkend Luchtvrachtagent

Datum security audit	13 mei 2026
Auditor PMT	Jack Varkevisser
Unieke identificatiecode	NL/RA/00543-00
Geldig tot	5-5-2029
	Nee

Bedrijfsnaam	N.J. Witkamp bv
Adres	ABC Westland 300
Postcode	2685 DD
Plaats	Poeldijk
Telefoonnummer	0174282930

PO nummer	
Adres voor facturering (e-mail)	

Verantwoordelijke voor de beveiliging en EU-gegevensbank	Ronald Spies
Telefoonnummer	0654901528
E-mailadres	ronald@witkamp.nl

Auditee	Ronald Spies
Auditee	Martin van de Merwe
Auditee	

Bedrijfsgegevens gewijzigd?	-
-----------------------------	---

Afspraken (A)	-
---------------	---

1.0 Algemeen		
	NORM: <i>Beveiligingsprogramma Algemeen.</i>	
1.1	Wie is aangewezen als Security Manager Luchtvracht binnen uw organisatie?	Ronald
1.2	Wie is de tekenbevoegde voor het beveiligingsprogramma?	P. Peters, directeur
1.3	Welke bedrijfsactiviteiten voert uw bedrijf uit? Inslag, Opslag, Overslag, Uitslag of vervoer.	Inslag, Uitslag
1.4	Besteedt uw bedrijf bedrijfsactiviteiten uit binnen de veilige luchtvrachtketen uit aan derden?	Nee
1.5	Zijn er andere bedrijven werkzaam op uw locatie?	Nee
1.6	Als er andere bedrijven werkzaam zijn op uw locatie, hoe wordt uw identificeerbare vracht beschermd tegen onbevoegden?	nvt
1.7	Hoeveel identificeerbare luchtvracht verstuurt u ongeveer? (ruwweg percentage of aantallen)	2%
1.8	Is er al iemand aangemeld voor Quickinform?	Ja, Ronald
1.9	Beveiligingsprogramma bevat nog de juiste algemene naamsgegevens.	Ja, Ronald
Bevindingen		
Afspraken :		
-		

2A Aannee van nieuw personeel		
NORM: punt 11.1 EU 2015/1998 <i>De procedure voor indienstname moet bestaan uit een aan de indienstname voorafgaande controle of een achtergrondonderzoek overeenkomstig punt 11.1 van de bijlage bij Uitvoeringsverordening (EU) 2015/1998. Wijziging Besluit van 10 maart 2022, nr. 3582131</i>		
2.1	Wie is verantwoordelijk voor het aannemen van nieuw personeel en het bewaren van de personeelsgegevens?	HR i.s.m. Ronald
2.2	Is er een procedure voor het aannemen van nieuw personeel?	Ja
2.3	Wordt hierbij gebruik gemaakt van een checklijst?	Ja, tevens de lijst besproken die geleverd wordt bij update personeelsdossier
2.4	Wat zijn de belangrijkste punten waarop gecontroleerd wordt, i.v.m. de luchtvrachtveiligheid, tijdens de aanname?	ID, CV, certificaten,
2.5	Voor wie vraagt u een VGB aan? (Groeperingen)	Alle vaste medewerkers
2.6	Hoe wordt de geldigheid van de VGB's bijgehouden?	Zitten in een map en worden half-jaarlijks gecontroleerd
2.7	Hoe voert u de identiteitscontrole uit?	Aan de hand van een origineel paspoort of ID-kaart
2.8	Hoe controleert u het werkverleden van de afgelopen 5 jaren en de eventuele onderbrekingen (28dagen of langer)? Denk aan verklaring in het PD en denk ook aan UZK.	Aan de hand van het CV, verklaringen hiervan worden in het PD bewaard door PZ
2.9	Hoe lang bewaart u de indienstname gegevens in het PD?	Gedurende het dienstverband tot 1 jaar hierna
2.10	Maakt u ook gebruik van inhuurpersoneel? (Welk UZB?).	Ja, niet voor de afhandeling van LV echter
2.11	Verzorgt u ook de VGB aanvragen voor het inhuurpersoneel en/of dienstverleners?	Nee
2.12	Hoe wordt het werkverleden gecontroleerd voor het inhuurpersoneel?	Opgave uitzendbureau
2.13	Heeft u ook cyberVOG's van de cyberfunctionarissen?	Niet bekend
2.14	Hoeveel medewerkers zijn er werkzaam op uw locatie en hoeveel hebben er onbegeleid toegang tot de identificeerbare luchtvracht?	Inclusief kantoor 18 medewerkers
Bevindingen		
Advies: Controleer of IT-personeel die (evt) veranderingen kunnen maken in een kritisch systeem wat niet automatisch gelogd wordt, in het bezit zijn van een cyber-VOG.		
Afspraken :		
-		

2B	Opleiden van personeel	
	<i>NORM:</i> <i>NOBB en punt 11.2 EU 2015/1998</i> <i>U moet aantonen dat alle personeelsleden (permanent personeel, tijdelijk personeel, uitzendkrachten, chauffeurs) die toegang hebben tot luchtvracht/luchtpost een passende beveiligingsbewustmakingsopleiding hebben genoten. Bovendien moet u aantonen dat alle relevante personeelsleden die beveiligingscontroles uitvoeren een opleiding of periodieke opleiding hebben genoten overeenkomstig hoofdstuk 11 van de bijlage bij Uitvoeringsverordening (EU) 2015/1998.</i>	
2.15	Wie is er verantwoordelijk voor het registreren en bijhouden van de opleidingsgegevens met betrekking tot de luchtvrachtbeveiliging?	PZ
2.16	Is er een registratieoverzicht van de trainingen?(Indexfile)	Ja
2.17	Kunnen personeelsdossiers ingezien worden tijdens een audit?	Als PZ er is wel anders m.b.v. dhr Peters
2.18	Bewaart u alle trainingscertificaten vanaf de basistraining?	Nee, kunnen worden ingezien in het PMT portal
2.19	Hoeveel personen hebben een ML-certificaat?	18
2.20	Hoeveel personen zijn er opgeleid tot Controleur?	3
2.21	Hoeveel personen zijn er opgeleid tot Supervisor?	Niemand
2.22	Hoeveel personen zijn er opgeleid tot Security Manager?	1
2.23	Heeft de security manager ook een medewerker luchtvracht opleiding?	Nee
2.24	Hoe worden de opfriscursussen gevolgd en met welke frequentie?	MLV jaarlijks online, CLV 2 x per jaar online. Security manager elke 30 maanden klassikaal
2.25	Ontvangt u, of iemand anders, de herinnering e-mails voor de opfriscursussen van uw opleidingsinstelling?	Martin
2.26	Hoe vindt de controle plaats m.b.t. de geldigheid van de diploma's van inhuurpersoneel	Word niet gedaan, niet nodig
2.27	Worden er nog andere relevante opleidingen aangeboden ter bevordering van de luchtvrachtveiligheid? Bijv. veiligheidsbewustzijns cursussen	Nee
Bevindingen		
Advies: Zorg dat er minimaal 1 supervisor per dagdeel wordt opgeleid en aanwezig is op de vloer, anders heeft een controleur weinig zin. Een supervisor training is verplicht mocht je een controleur willen gebruiken.		
Afspraken :		

3.0	Aannameprocedure luchtvracht	
	NORM: <i>Artikel 6 EU 2015/1998</i>	
3.1	Neemt u veilige luchtvracht aan in uw proces?	Nee
3.2	Neemt u veilige vracht aan vanuit derde landen naar EU-landen?	Nee
3.3	Hoe controleert u uw ketenpartner tijdens de aanname?	Er wordt hier geen LV aangenomen, bedrijven die aanleveren hebben geen idee wat er gaat vliegen
3.4	Maakt u daarbij gebruik van de EU-database?	Nee, wel een inlog maar nauwelijks ingelogd
3.5	Wie hebben er een autorisatie voor de EU database? Is men in bezit van VGB en min MLV?	Ronald
3.6	Hoe vaak wordt de EU-database geraadpleegd? (handmatig of via systeem).	Niet
3.7	Hoe wordt er gecontroleerd dat de vrachtwagen versloten is geweest?	Niet
3.8	Hoe wordt de beveiligingscontrole uitgevoerd?	Visueel
3.9	Wordt de identiteit van de chauffeur gecontroleerd?	Nee, de chauffeurs die lossen worden niet gecontroleerd
3.10	Neemt u zendingen aan van bedrijven zonder gevestigde zakelijke relatie en wat is de procedure?	Nee, met alle aanleverende bedrijven is een zakelijke relatie.
3.11	Maakt u gebruik van de risicoinventarisatie bijlage 1 voor zendingen?	nee
3.12	Ontvangt u zendingen met een combinatie elektronische artikelen en batterijen met vloeistoffen, spuitbussen en gels (LAG's)?	Nee alleen groente en fruit
3.13	Hoe gaat u om met deze LAG's?	nvt
3.14	Hoe is de scheiding tussen veilige en onveilige luchtvracht geregeld?	Door pas op het allerlaatste moment LV te selecteren
Bevindingen		
Advies: Log regelmatig in om de logistieke partners te controleren in de EU-database en controleer ook de iD van de chauffeurs die aanleveren.		
-		
-		
Afspraken:		
3.A	-	

4.0	Beveiligingsonderzoeken	
	NORM: Artikel 6.1 en 6.3 EU 2015/1998	
4.1	Welke methode gebruikt uw bedrijf om luchtvracht veilig te verklaren? P&P, RA, KC of beveiligingsonderzoek!	P&P
4.2	Laat u beveiligingsonderzoeken uitvoeren? Besteed u dit uit?	Nee
4.3	Welke percentage luchtvracht wordt via pick & pack geselecteerd?	100%
4.4	In geval van Pick en Pack, hoe wordt de procedure uitgevoerd?	Er is tot op het laatste moment niet bekend wat LV wordt. Op een gegeven moment wordt er random vracht gepicked van de voorraad en die wordt dan pas bestempeld als luchtvracht. Als het dus klaar gezet is als LV gaat 100% vliegen.
4.5	Welke vormen van transport gebruikt uw bedrijf naast luchtvracht (weg/zee/spoor/anders)?	wegtransport
4.6	Worden er beveiligingsonderzoeken op uw eigen locatie uitgevoerd?	Nee
4.7	Zo ja, welke methodes worden er gebruikt? (eventueel apparatuur)	nvt
4.8	Hoe wordt dit uitgevoerd? (Waar/door wie/supervisor?/toegang)	nvt
4.9	Hoe wordt de vracht aangeboden aan een EDD-team, denk aan opstelling van vracht (ruimte/hoogte).	nvt
4.10	Geeft uw bedrijf zelf de status SPX/SHR af?	Ja, de SPX code die wordt vermeld op het CMR
4.11	Besteed uw bedrijf beveiligingsonderzoeken uit aan derden en beschrijf de procedure?	Nee
4.12	Is er cameratoezicht op de beveiligingsonderzoeken?	nvt
4.13	Hoe wordt de veiligheidsverklaring doorgegeven aan de volgende RA?	Via het CMR en sec dec
4.14	Maakt u gebruik van vrijstellingen voor goederen van beveiligingsonderzoeken?	Nee
4.15	Merkt u wel eens een zending aan als HRCM?	Nee
4.16	Maakt uw bedrijf gebruik van apparatuur anders als EDD voor het veilig verklaren van luchtvracht?	Nvt
Bevindingen		
Advies: Gezien onze laatste ervaringen in de sector zal de KMar niet meer akkoord gaan met de 100% P&P, men zal een vorm van screening gaan eisen om de RA status te behouden. Dat kan bijv. een PHS beveiligingsonderzoek zijn maar dan moeten er wel meer controleurs en zeker ook supervisors getraind gaan worden die de vracht visueel/handmatig onderzoeken alvorens klaar te zetten als LV. EDD is ook mogelijk.		
Afspraken:		
6.C	-	

5	HRCM	
	NORM: Artikel 6.7 EU2015/1998 en C (2015)/8005	
5.1	Hoe stelt uw bedrijf vast of een zending onder de HRCM-norm valt?	Er wordt geen LV aangenomen, en dozen met schade geselecteerd voor LV worden meteen vervangen
5.2	Neemt u wel eens (transfer)vracht aan vanuit derde landen naar de EU?	Nee
	Zo Ja:	
5.3	Hoe controleert u de documentatie?	
5.4	Weet u welke hierbij de risicolanden zijn? (Aanhangsel 6-F uitvoeringsbesluit c(2015)8005)	
5.5	Welke veiligheidscontroles en/of onderzoeken voert u hierbij uit.	
	Zo Nee:	
5.6	Weet de loods en/of kantoor wat een HRCM zending is?	Ja
5.7	Beschrijf uw procedure bij aantreffen of duiden van een HRCM zending?	Bij LV geselecteerde vracht wordt bij vermoeden van manipulatie een controleur ingezet om de vracht te controleren. Veilig maken zal via twee verschillende methodes moeten.
5.8	Wie merkt een zending aan als HRCM?	Security manager
Bevindingen		
Advies: Zorg dat een controleur een supervisor training krijgt. En 1 is eigenlijk geen dus meerdere worden geadviseerd. Zie opmerking onder H4.		
-		
-		
Afspraken:		
6.C	-	

6 Bescherming van veilige luchtvracht		
NORM: Aanhangsel 6 EU 2015/1998 U moet aantonen dat de toegang tot het opslaggedeelte wordt gecontroleerd. Als het product tijdens de opslag kan worden geïdentificeerd als luchtvracht/luchtpost, moet u aantonen dat maatregelen zijn genomen om de luchtvracht/ luchtpost in dit stadium te beschermen tegen manipulatie door onbevoegden. Ten slotte moet u aantonen dat de afgewerkte en verpakte luchtvracht/luchtpost wordt gecontroleerd alvorens te worden verzonden.		
6.1	Wordt de identiteit van bezoekers/monteurs etc. vastgesteld?	Ja
6.2	Is er altijd een begeleider aanwezig wanneer een derde partij in de loods is?	Ja
6.3	Worden onbevoegden aangesproken in de loods?	Ja
6.4	Is er een plek gecreëerd voor de opslag van veilige luchtvracht?	Ja, zodra er LV is geselecteerd is er evt een koelcel beschikbaar die op slot kan.
6.5	Is de opslag van luchtvracht voldoende beveiligd?	Ja
6.6	Vindt er een handmatige / visuele controle plaats wanneer de zending uit de opslag wordt gehaald?	Ja een visuele alvorens te laden in de truck
6.7	Wie is er in de praktijk verantwoordelijk voor deze controles?	De getrainde LV loodsmedewerker
6.8	Maakt u gebruik van beveiligingsbedrijven die zelfstandig bij luchtvracht kunnen?	Ja, mbt tot alarmopvolging
6.9	Zo ja, hoe is dit geregeld m.b.t. screening en opleiding?	Er blijft geen veilige geselecteerde vracht staan
6.10	Staan er deuren open tijdens de audit zonder toezicht?	Nee, bemand met medewerkers
Bevindingen		
Conform		
Afspraken :		
-		

7 Vervoer Veilige Luchtvracht		
NORM: Hoofdstuk 6 EU 2015/1998 Indien uw bedrijf een beroep doet op een subcontractant, moet u garanderen dat a) de luchtvracht/luchtpost door u verzegeld of verpakt is, teneinde te garanderen dat eventuele manipulatie door onbevoegden duidelijk zichtbaar is, en b) de in aanhangsel 6-E van de bijlage bij Uitvoeringsverordening (EU) 2015/1998 opgenomen vervoerdersverklaring door de vervoerder is ondertekend.		
7.1	Wie is verantwoordelijk voor het vervoer van uw veilige luchtvracht?	Expediteur
7.2	Wie vervoert uw veilige luchtvracht?	Airflo, K+N etc.
Als de opdracht tot transport door de Erkend Agent wordt gegeven:		
7.3	Maakt u gebruik van vaste vervoerder of erkend vervoerder?	Nee, momenteel alleen RA's
7.4	Indien vervoer door middel van een Erkend Agent of erkend vervoerder plaatsvindt, hoe en hoe vaak controleert u de actieve status van deze?	Niet
7.5	Hoe beschermt u uw voertuig tegen manipulatie?	Truck RA's kan op slot
7.6	Controleert u of de vrachtwagen wordt versloten voor het transport (gesloten of verzegeld)?	Ja
7.7	Maakt u gebruik van verzegeling ? Hoe worden de zegels veilig gehouden?	Zelden, liggen opgeslagen in de control tower (kantoor in loods)
7.8	Indien van toepassing, wie controleert dit en wordt dit vastgelegd?	Vanuit de control tower heeft men dit overzicht maar wordt niet geregistreerd.
Bevindingen		
Advies: Check regelmatig de logistieke partners		
Afspraken :		
-		

8 Cybersecurity		
NORM: <i>Aanhangsel 6 EU 2015/1998</i> Het is van essentieel belang dat de toegang tot de zone waar de luchtvracht/luchtpost wordt verwerkt of opgeslagen, wordt gecontroleerd.		
8.1	Wordt uw ICT omgeving beheerd door een externe partij of u zelf?	Externe partij
8.2	Indien een externe partij is deze gecertificeerd met ISO27001/27002 en/of NEN7510/16495?	Moet worden nagevraagd
8.3	Heeft u kritieke systemen benoemd in uw beveiligingsplan?	Ja
8.4	Heeft u een risico analyse uitgevoerd om uw kritieke systemen te duiden?	Nee
8.5	Hoe beveiligd u uw kritieke systemen? (ww/MFA).	ww/inlog
8.5	Hoe reageert u op cyberaanvallen?	extern
8.6	Heeft u uw ICT voorschriften beschreven in een ISMS?	Nee
8.7	Heeft uw bedrijf Cybersecurityspecialisten en hoe waarborgt u dat deze voldoen aan relevante opleidingseisen? Let op extern!	externe partij
8.8	Hebben de ICT medewerkers een cybersecurity VOG (VGB) indien hun werkzaamheden niet gelogd worden? (Kunnen logfiles veranderd of verwijderd worden?).	Niet bekend
8.9	Hebben medewerkers die in uw kritieke systemen toegang hebben maar niet bedoeld zijn om te werken met LV een cybersecurityawareness training gevolgd (+cyberVOG)?	VGB
Bevindingen		
Advies: Check of de actie van de externe serviceprovider gelogd worden, als dit niet zo is dient een cyber-VOG voor hen geregeld te worden.		
Afspraken :		

9 Beveiligingscultuur en IKC		
NORM: Brief AIVD/Kmar Ter bevordering van de beveiligingscultuur wordt er verwacht dat er elk jaar een self-assessment uitgevoerd wordt en dat er eventueel acties genomen worden om de "zwakke" punten te verbeteren. Dit dient in een eigen archief bewaard worden.		
9.1	Wie is verantwoordelijk voor de interne kwaliteitscontrole?	Keurmeeste en security manager
9.2	Worden er, behalve deze audit en het self-assessment, nog andere kwaliteitscontroles uitgevoerd?	AEO en HACCP
9.3	Hoe worden de IKC-resultaten geregistreerd en afgehandeld?	Schriftelijk en met het team besproken
9.4	Is het self-assessment dit jaar al gedaan?	Nog niet
9.5	Zijn er activiteiten ontwikkeld?	Nee
9.6	Zijn er het afgelopen jaar concrete verbeterstappen uitgevoerd?	Nee
9.7	Hoe bevordert uw bedrijf de beveiligingscultuur?	Training, korte gesprekjes tijdens werk
9.8	Welke preventieve maatregelen voert uw bedrijf uit om dreigingen van binnen uit, radicalisering en incidenten die relevant zijn voor de LV beveiliging tegen te gaan?	Training, korte gesprekjes tijdens werk
9.9	Hoe kunnen personen verdenkingen van dreiging binnen uw bedrijf kenbaar maken? (vertrouwenspersoon/klokkenluider)	Vertrouwenspersoon
9.10	Zijn er regels opgesteld om vertrouwelijke informatie van uw bedrijf te beschermen of te voorkomen dat deze worden gedeeld met onbevoegden (ChatGPT, socialmedia)?	Ja in een personeelsregelement
Bevindingen		
Conform		

10	Controle van dossiers	
	NORM: Artikel 6.3 EU 2015/1998 <i>De som van alle beveiligingsmaatregelen wordt getoetst aan de hand van de export luchtvracht dossiers. Er wordt gecontroleerd of de zendingen, die als veilige vracht aangeboden worden, ook ale controlepunten hebben doorlopen. Daarnaast moet er een juiste beveiligingsstatus worden vermeld op de documenten.</i>	
Dossier 1		
AWB-nummer		
Naam afzender		
Status afzender:		BA / ELA / OA
Naam transportbedrijf		
Status transportbedrijf:		RA / KC/ AH
SPX vermelding AWB		
Bevindingen:		
Dossier 2		
AWB-nummer		
Naam afzender		
Status afzender:		BA / ELA / OA
Naam transportbedrijf		
Status transportbedrijf:		RA / KC/ AH
SPX vermelding AWB		
Bevindingen:		

11

Rapportage audit

Naar aanleiding van de interviews met de audités zijn de volgende zaken naar voren gekomen

A.

Voorblad

Bedrijfsgegevens gewijzigd?

-

1.

Algemeen

0

0

0

2.

Opleiden

Advies: Controleer of IT-personeel die (evt) veranderingen kunnen maken in een kritisch systeem wat niet automatisch gelogd wordt, in het bezit zijn van een cyber-VOG.

0

Advies: Zorg dat er minimaal 1 supervisor per dagdeel wordt opgeleid en aanwezig is op de vloer, anders heeft een controleur weinig zin. Een supervisortraining is verplicht mocht je een controleur willen gebruiken.

0

3.

Aanvraagprocedures luchtvracht

Advies: Log regelmatig in om de logistieke partners te controleren in de EU-database en controleer ook de ID van de chauffeurs die aanleveren.

-

-

4.

Beveiligingsonderzoeken

Advies: Gezien onze laatste ervaringen in de sector zal de KMar niet meer akkoord gaan met de 100% P&P, men zal een vorm van screening gaan eisen om de RA status te behouden. Dat kan bijv. een PHS beveiligingsonderzoek zijn maar dan moeten er wel meer controleurs en zeker ook supervisors getraind gaan worden die de vracht visueel/handmatig onderzoeken alvorens klaar te zetten als LV. EDD is ook mogelijk.

5.

HRCM

Advies: Zorg dat een controleur een supervisor training krijgt. En 1 is eigenlijk geen dus meerdere worden geadviseerd. Zie opmerking onder H4.

-

-

6.

Bescherming

Conform

0

0

7.

Vervoer

Advies: Check regelmatig de logistieke partners

0

0

8.

Cybersecurity

Advies: Check of de actie van de externe serviceprovider gelogd worden, als dit niet zo is dient een cyber-VOG voor hen geregeld te worden.

0

9.

Beveiligingscultuur en IKC

Conform

0

0

10.

Dossier controle

0

0

Afspraken

Onderwerp:

Actie door:

A

1

2

3

4

5

6

7

8