

1. Doel van de werkinstructie

Het beveiligen van het product tegen opzettelijke besmettingen (terrorisme, sabotage, wrok).

Het beveiligen van het bedrijf tegen inbraak in de computer systemen.

Dit alles moet uiteindelijk resulteren in het op de markt brengen van een veilig product om consument, merk en branche te beschermen.

2. Betrokken functies / verantwoordelijkheden

In het overzicht hieronder worden de verantwoordelijkheden per betrokken functie / betrokkene weergegeven en in de paragrafen erna een uitgebreidere toelichting over hoe de verantwoordelijkheden beheerst worden.

Verantwoordelijke punten:

1. Wettelijke eisen
2. Identificatie van kritieke ruimtes en/of werkzaamheden en toegangsbeleid voor werknemers
3. Bezoekers en contractanten
4. Externe inspecties en bezoeken van autoriteiten beheren
5. Alle overige passende beheersingsmaatregelen

Betrokkenen	Verantwoordelijkheden + toelichting in paragraaf
Directie	Punten: 1, 2, 3, 4, 5 Paragrafen: 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.11, 4.12, 4.13, 4.14, 4.15, 4.16, 4.17, 4.18, 4.19, 5
Management team	Punten: 1, 2, 3, 4, 5 Paragrafen: 4.3, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10, 4.11, 4.12, 4.13, 4.14, 4.15, 4.16, 4.18, 4.19, 5
IT Officer / IT	Punten: 1, 5 Paragrafen: 4.3, 4.4, 4.6, 4.9, 4.12, 5
Betrokken partijen / lokale autoriteiten	Punten: 5 Paragrafen: 4.3, 4.7, 4.12, 4.19
Team van deskundigen (intern)	Punten: 1, 4, 5 Paragrafen: 4.1, 4.2, 4.3, 4.5, 4.7, 4.7.1, 4.12, 4.13, 4.14, 4.15, 4.16, 4.18, 4.19, 5
Team van deskundigen (extern)	Punten: 1 Paragrafen: 4.2, 4.3, 4.6, 4.7, 4.8, 4.9, 4.19
Leidinggevend	Punten: 3 Paragrafen: 4.5, 4.11, 4.12, 4.13, 4.14, 4.15, 4.16, 5
HACCP team (= Food defense team)	Punten: 1 Paragrafen: 4.1, 4.2, 4.13, 4.14, 4.15, 4.17, 4.18, 5

3.0 Referenties

- Servers IT
- Risicoanalyse
- Overzicht rechten in computersysteem
- Diverse telefoonlijsten (ook van de lokale autoriteiten)
- Training registratie
- I06.0 Hygiëne regels
- I06.1 Hygiëne instructies
- I06.1 Hygiene instructies
- Verladingsdocumenten
- Personeelsdossier
- Beoordelingsdocumenten kwaliteitssysteem
- Security Declaration
- I23.1 Trailer Inspectie
- I14.2 Aannemen telefoon, post(stukken)

4.0 Beschrijving instructie**4.1 Team van deskundigen**

Binnen het bedrijf is een team van deskundigen aangesteld op het gebied van security.

Dit is het HACCP team welke waar nodig uitgebreid kan worden met specifieke expertise. Het HACCP team is dus ook het Food defense team.

Een aantal personen heeft ook certificaat “veiligheidskursus” met goed gevolg afgerond. Deze training is gecertificeerd door het ministerie van Justitie volgens, EU300/2008, EU272/2009, EU185/2010. In het team is ook opgenomen een medewerker welke diploma’s beveiliging op elk niveau heeft behaald.

4.2 Risico analyse

In de product gevarenanalyse worden ook de gevaren met betrekking tot Food Defense & Security geanalyseerd en beoordeeld. Hiervoor is het HACCP team daar waar nodig uitgebreid met deskundigen op het gebied van veiligheid. (HACCP team is ook het Food defense team).

4.3 Beveiliging terrein

In Nederland worden toegangspoorten tot individuele bedrijven niet vaak toegepast.

Wel kan de parkeergarage van dit bedrijf buiten reguliere werktijden worden afgesloten door middel van een roldeur. Op het buitenterrein van dit bedrijf zijn camera’s aanwezig voor toezicht. Op bedrijventerrein zijn ook op diverse plekken camera’s aanwezig en is een beveiligingsbedrijf aanwezig.

4.4 Beveiliging gebouw / parkeerplaatsen

Het gebouw is voorzien van een beveiligingssysteem. Hierbij wordt ook gebruik gemaakt van camera’s. Verder is de omgeving van het gebouw goed verlicht. De bediening van de verlichting is alleen toegankelijk voor specifieke personen.

Auto’s van bezoekers of medewerkers mogen niet in het verladingsgebied geparkeerd worden of bij vrachtwagens. Bezoekers parkeerplaatsen zijn aanwezig en aangegeven.

4.5 Gecontroleerde toegang tot de locatie

Niemand mag het bedrijf ongecontroleerd betreden.

Dit wordt gerealiseerd door alle deuren gesloten te houden. Toegang tot het bedrijf via:

- Receptie
- Via bemand distributiekantoor / ontvangstkantoor
- Via een bel (bv. aangesloten op een mobiele telefoon, deur op afstand te bedienen wanneer bezoeker toegelaten wordt.)
- Leidinggevend(en) (en medewerkers) zien er op toe dat niemand ongecontroleerd het bedrijf kan betreden.

(onbekende) bezoekers worden altijd begeleid door een medewerker van het bedrijf. Wanneer er twijfel bestaat over de bezoeker kan een ID kaart worden gevraagd.

Bezoekers worden geregistreerd. Op ieder moment moet bekend zijn wie er op de locatie aanwezig is. Dit voor Security doeleinden maar ook bijvoorbeeld voor ER officer / BHV (bedrijfshulpverlening) doeleinden (bv. brand).

Ook contractors moeten zich aanmelden. Verder staan contractors altijd onder toezicht van het bedrijf. Hierbij kan wel toestemming worden gegeven zelfstandig werkzaamheden uit te voeren na beoordeling van de begeleider. In luchtvrachtgebied altijd onder begeleiding. Contractors wordt gevraagd ook verdachte zaken en omstandigheden te melden.

4.6 Gecontroleerde toegang tot bedrijfsruimten

Verschillende bedrijfsruimten (bv. kantoren, IT ruimten) worden beveiligd door middel van gecontroleerde toegang. Per medewerker wordt bepaald tot welke ruimtes toegang kan worden verkregen.

Verder geldt dat medewerkers op de eigen werkplek blijven. Het is niet toegestaan voor medewerkers om zonder toestemming naar andere afdelingen te gaan.

4.7 Nieuwe medewerkers

- Via intake gesprekken moet een goed beeld gevormd worden van de medewerker.
- Identiteit van nieuwe medewerkers (vast personeel, uitzendkrachten) wordt gecheckt. (bijv. door ID checker bij Uitzend Organisaties).
- Inhoud van de CV wordt waar nodig gecheckt (bv. opleiding) en evt. onderbrekingen tijdens studie of loopbaan.
- Referenties worden gecheckt en beoordeeld naar gelang de functie dit vereist. Voor specifieke functies kan een VOG vereist zijn.
- Een kopie van de ID-kaart wordt in het personeelsdossier bewaard (met uitzondering van de uitzendkrachten).
- Nieuwe medewerkers (vast personeel & uitzendkrachten) krijgen een introductietraining bij indiensttreding. Uitzendkrachten krijgen ook een "buddy" toegewezen.

4.7.1 Uit dienst

Wanneer een werknemer uit dienst treedt zal *HR* een Formulier F18.1-Checklist in dienst /uit dienst met betreffende werknemer invullen en in dossier opslaan. Alle mogelijke vormen van toegang tot het bedrijf en informatie zal dan direct worden geblokkeerd voor deze medewerker.

4.8 Beheersing tags (elektronische sleutels)

Bij Greenpack wordt hoofdzakelijk toegang tot ruimtes verschaft d.m.v. tags. Per medewerker is bekend of er een tag is verstrekt en tot welke ruimten deze medewerker toegang heeft.

Bij uitdiensttreding of verandering van functie worden lijsten met gegevens direct aangepast, waardoor dus blokkade van toegang naar ruimtes en informatie.

Minimaal jaarlijks wordt het overzicht getoetst en gecontroleerd. *Operational Manager* is verantwoordelijk voor het tagsysteem. De verantwoording van uitgifte en autorisatie van de tags ligt bij *Operational manager*.

Voor uitgegeven badges aan bezoekers/ derden moet getekend worden voor ontvangst en inname bij de balie van de administratie. Bij afwijkingen worden direct melding van gemaakt bij *Operational Manager* en gepaste actie ondernomen.

4.9 Beheersing computersystemen

Bij IT is bekend per medewerker tot welke computersystemen er toegang is gegeven. De toegang tot de systemen is beveiligd door middel van een wachtwoord. Bij uitdiensttreding van systeembeheerder / IT Officer zullen wachtwoorden van de pc's en servers gewijzigd worden. Iedere computer gaat automatisch in de wachtstand (schermbeveiliging) wanneer er een tijdje geen gebruik van wordt gemaakt.

De systeembeheerder meldt afwijkende zaken in het systeem aan het management. Bij een aantal verkeerde pogingen tot het ingeven van een wachtwoord wordt de computer tijdelijk geblokkeerd.

Voor enkele pc's met bedrijfsgevoelige informatie kan IT beheer opdracht geven het wachtwoord te wijzigen. Deze gevoelige pc's staan echter in afgesloten ruimtes welke alleen toegankelijk voor geautoriseerd personeel.

Deze personen wordt gevraagd regelmatig wachtwoord van de pc te wijzigen. Geheel afhankelijk van de toegankelijkheid is de frequentie van wijziging. Er zijn programma's zoals bv. een anti virus programma in werking en andere inbraakbeveiligingen.

Er is een procedure back-up systeem binnen het bedrijf (PRO07.2-Back up van digitale gegevens)

Gedurende de dag worden er back-ups gemaakt van alle servers. Van de servers die belangrijk zijn voor de bedrijfsprocessen wordt meerdere malen per dag een back-up gemaakt. Van de VMGP01 (Bekopak Server) wordt 3 maal daags een back-up gemaakt, om 4:30, 13:00, en 21:00 uur.

De back-up van 13:00 en 21:00 word daarnaast ook naar de vestiging in polen gekopieerd.

De dagelijkse back-up van 04:30 word minimaal een maand bewaard, deze back-up zorgt ervoor dat we snel kunnen terugvallen op de situatie van afgelopen ochtend, aangevuld met de laatste database backups.

Van de GPSQL (WorkIT Server Database) wordt er meerdere malen per dag een back-up gemaakt. De full backups draaien om 05:00, 13:00, 18:00, 23:00 en elk uur wordt er een backup gemaakt met alle wijzingen vanaf een full back-up.

De full back-ups van 05:00 en 18:00 worden elke dag gekopieerd naar Legnica, de backup van 05:00 wordt elke dag nog eens extra gekopieerd naar cloud storage.

Van de VMGP05 (Documenten) word dagelijks om 20:15 een back-up gemaakt. 6 maal per dag (8, 11, 14, 17, 20 en 23 uur) word een back-up gemaakt van de gewijzigde documenten naar een andere back-up locatie.

Daarnaast word dagelijks om 04:15 een replica gemaakt. Van de VMDC01 (Domain Controller) wordt 2 maal daags een back-up gemaakt om 02:00 en 15:00. Daarnaast wordt dagelijks om 23:15 een replica gemaakt.

Van de overige servers wordt dagelijks een back-up gemaakt, en minimaal 1 maal per week een replica.

Back-up:

De back-up van alle servers wordt gemaakt met de software van Veeam Backup and Replication.

Camerabeelden:

Greenpack heeft meer dan voldoende digitale camera's hangen, dit zijn allemaal digitale camera's met een uitstekende beeldkwaliteit. Er is een plattegrond van de werkvloer waar de nieuw geplaatste camera's op ingetekend zijn De beelden zijn alleen toegankelijk voor:

- IT Officer
- Director
- Operational manager
- Manager Bekopak
- Warehouse manager

Beelden worden automatisch binnen 4 weken verwijderd. Indien een beeld langer bewaard moet blijven voor een bepaald doeleinde zoals diefstal of een ongeval dan is dit onder beheer bij de Manager Bekopak in combinatie met IT Officer. Wanneer het incident is afgehandeld, wordt het beeld verwijderd.

De processen binnen de IT worden en zijn gedocumenteerd en zijn alleen beschikbaar voor het IT personeel.

Hierin wordt beschreven hoe:

- de back-up processen precies werken.

- een nieuwe computer moet worden geconfigureerd.
- de E-mail moet worden ingesteld.
- WorkIt en het BekoPak systeem ingesteld dienen te worden (incl. Oplossingen bij storing).
- het camerasysteem werkt, bediend kan worden en de bevoegdheden van het camera systeem.
- het inloggen van fris werkt en de inlog gegevens van Fris.
- de Hardware werkt (Handscanners, Wifi, Telefooncentrale e.a.)
- Office 365 werkt

4.10 Training leidinggevenden

Leidinggevenden moeten ervaring hebben of getraind zijn op het gebied van security. Deze ervaring / training moet bestaan uit:

- Het bewustzijn van bedreigingen
- De analyse van mogelijke bedreigingen. Met aandacht voor gevaren in iedere processtap. Denk ook aan de postkamer.
- Het herkennen van bedreigingen / verdachte situaties
- Het herkennen van aanpassingen aan trailers / containers.
- Hoe verdachte situaties te melden

Deze training moet vastgelegd worden incl. behandelde onderwerpen, datum, getekend voor training gekregen en begrepen).

Jaarlijks moet een opfriscursus Food defense & security worden gegeven. Leidinggevenden kunnen de kennis delen met hiervoor geselecteerde vaste medewerkers.

4.11 Controle op de werkvloer

Op de verschillende afdelingen zijn getrainde leidinggevenden aanwezig om toezicht te houden op de veiligheid van het proces. Ook kan aanvullend gebruik worden gemaakt van camera's. Maar die zijn met name bedoeld om vernieling, manipulatie of diefstal aan het licht te brengen (korte bewaartijd van de beelden worden wel regelmatig gecontroleerd op werking en bewaartijd) zie ook beheersing computersystemen.

4.12 Het melden van verdachte situaties

Medewerkers is gevraagd verdachte situaties (anders dan normaal begrip) direct te melden aan leidinggevenden. Binnen het bedrijf is afgesproken bij wie/ dat verdachte situaties gemeld moeten worden aan Managementteam, *Head of Security*, Directie. Medewerkers worden regelmatig geattendeerd op medewerking in deze. Op diverse plaatsen binnen het gebouw hangen pictogrammen welke aanduiden verdachte personen en situaties te melden. Deze pictogrammen verschijnen ook regelmatig in de facilitaire ruimte op daarvoor bestemde tv schermen.

4.13 Betrokkenheid personeel

Een belangrijk onderwerp om problemen te voorkomen op het gebied van de veiligheid van het product/ de veiligheid van de locatie is onderlinge betrokkenheid. Dat leidinggevenden onrust onder personeel signaleren en hierop actie ondernemen. En dat externe ontwikkelingen tijdig gesignaleerd worden. Het analyseren van ontwikkelingen is ook een onderwerp van de jaarlijkse evaluatie. Greenpack steekt veel energie in het door ontwikkelen van een voedselveiligheidscultuur in de organisatie.

4.14 Distributie / Transport

Binnenkomende en uitgaande trailers/ containers worden gecontroleerd op netheid, veiligheid en of de trailer overeenkomt met de opgegeven informatie door transporteur.

Van de chauffeurs wordt de ID gecheckt. Bij luchtvracht altijd de ID kaart controleren. Bij overige transporten de ID kaart vragen bij twijfel over de chauffeur (onbekend persoon/ bedrijf). Op de CMR moet de chauffeur zijn volledige naam noteren.

Indien er wordt gewerkt met verzegelde trailers/ containers dan moeten hiervoor aanvullende instructies worden opgesteld.

Internationale transporten en lokale verladingen worden apart van elkaar gehouden.
Producten zijn duidelijk gelabeld en aantallen zijn correct.

4.15 Distributie controle / documentcontrole

Bij binnenkomst / distributie moet de juistheid van de producten / aantallen en de juistheid van de documentatie worden gecontroleerd door een hiervoor opgeleide medewerker. Bij ladingen met seal moet er gekeken worden of seal nog in goede staat is. Afwijkingen moeten direct gemeld worden bij Head of security en directie. Bij transport voorzien welke wordt voorzien met een seal wordt eerst I23.1-Trailer inspectie uitgevoerd door medewerker Greenpack.

4.16 Persoonlijke attributen

Zoals ook staat omschreven in de Algemene veiligheidsinstructie / huisregels / personeelshandboek mogen er geen persoonlijke attributen worden meegenomen op de werkvloer. Bovendien ook aanduidingen op de werkvloer en op de tv / infoschermen in de facilitaire ruimtes.

4.17 Postkamer / administratie

Wanneer onduidelijke / verdachte pakketjes of brieven worden afgeleverd dan wordt dit gemeld aan de contactpersoon Security (Directeur Greenpack) of Food defense team lid. Deze beslist hoe het pakketje / brief afgehandeld moet worden. Dit staat ook beschreven in instructie I14.2 Aannemen telefoon en/of post(stukken).

4.18 Evaluatie / Interne Audit / Loodsrondes

De werkzaamheden op het gebied van security en de actualiteit van de risico beoordeling wordt minimaal 1x per *12 maanden of als er significante wijzigingen optreden* beoordeeld (Tijdens de jaarlijkse beoordeling van het kwaliteitssysteem).

Minimaal maandelijks wordt een loodsronde gehouden. Hierbij wordt het gebouw en de werkplek beoordeeld op veiligheid en onderhoud (dit kan gecombineerd worden met de hygiëne loodsronde).

Tijdens managementoverleg wordt food defense als agenda punt besproken.

4.19 Betrokken partijen

Er is een communicatieplan en telefoonlijst met belangrijke telefoonnummers van bijvoorbeeld lokale autoriteiten beschikbaar.

Dit kan eventueel gecombineerd worden met een algemene calamiteiten procedure.

5. Archivering

- Registraties worden minimaal een jaar bewaard. (tenzij langere bewaartijd door wetgeving aangegeven)