

## Colofon

Eerste druk 2005

Dit is een uitgave van de regiopolitie Amsterdam-Amstelland.

Alle rechten zijn voorbehouden. Niets uit deze uitgave mag worden veeelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand of openbaar gemaakt in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of op enige andere manier, zonder voorafgaande schriftelijke toestemming van de uitgever.

Vormgeving: Reclamebureau Muller, Rosmalen

Drukwerk: Drukkerij VNV, Kapellen (B)



# TERRORISME

## TEGENHOUDEN



Gebouwen



Personeel



Informatie

Drempelverhogende maatregelen voor bedrijven



# Voorwoord

Het 'waken tegen het kwaad' is een kerntaak van de overheid. Een nieuw 'kwaad' heeft zich inmiddels ook in Nederland vertoond: terrorisme. Realisme dwingt ons onder ogen te zien dat aanslagen in de toekomst niet uitgesloten kunnen worden. En daarom is het nodig dat de overheid en samenleving rekening houden met - en zich voorbereiden op - mogelijke terroristische aanslagen.

De regiopolitie Amsterdam-Amstelland zal er alles aan doen om de kans op een aanslag te verkleinen, de gevolgen te beperken en de daders van een eventuele aanslag op te sporen. Dat kan zij echter niet alleen. Een gezamenlijke inspanning van de overheid, maatschappelijke organisaties, het bedrijfsleven en burgers is nodig. Op het gebied van criminaliteit bestaat deze samenwerking al. Ook bij het voorkomen en bestrijden van de nieuwe woeking aan het fundament van onze samenleving zullen allen hun verantwoordelijkheid moeten nemen.

Naast de algemene en bekende bedrijfsrisico's, zoals brand, bedrijfsongevallen, handelsrisico's en criminaliteit, loopt u - als ondernemer - wellicht kans getroffen te worden door terroristische activiteiten. Door uw veiligheidsrisico's in kaart te brengen en preventieve maatregelen te nemen die drempelverhogend zijn voor terroristen, zult u de veiligheidssituatie van uw bedrijf verbeteren. Dat is belangrijk voor de continuïteit en integriteit van uw onderneming.

Om u bij het opwerpen van deze drempels op weg te helpen is dit handboek samengesteld. In dit handboek zijn diverse maatregelen opgenomen die bij invoering de veiligheid van uw bedrijf zullen verhogen. U levert daarmee tevens een bijdrage aan het veiliger maken van onze regio.

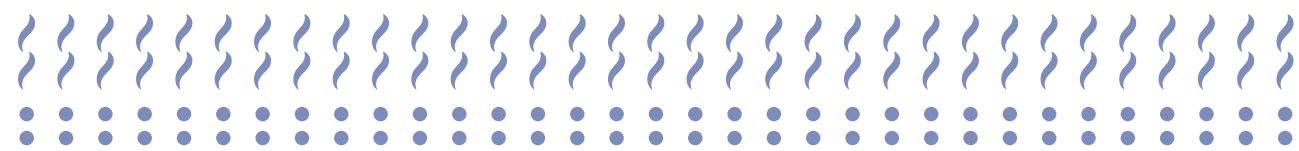
Ik dank u voor uw medewerking.

Met vriendelijke groet,  
drs. B.J.A.M. Welten,  
Korpschef regiopolitie Amsterdam-Amstelland



# Inhoudsopgave

<b>Inleiding</b>	4
Terrorisme	4
Bedrijven en terrorisme	4
Kosten	5
Samenwerking	5
Wettelijke eisen	5
Preventieve maatregelen	6
<b>Gebouwen</b>	7
Kwetsbaarheden	7
Bewustwording personeel	7
Bouwtechnische maatregelen	7
Goed schoon- en onderhouden	8
Toegang terrein	8
Openen en sluiten	9
Toegang gebouw	9
Veiligheid receptie	10
Huisregels	11
Aanhouding verdachte	11
Alarm, camera's en verlichting	12
Logistiek	13
Brandpreventie	14
<b>Personeel</b>	15
Kwetsbaarheden	15
Bewustwording personeel	15
De 'insider'	15
Aanname nieuw personeel	16



# Inhoudsopgave

Verklaring Omtrent Gedrag	17
Centraal Krediet Informatiesysteem	18
Contractanten en extern personeel	18
ID-plicht en pasjes	19
Zakenrelaties	19
Veiligheid personeel	20
Waarschuwingssysteem	20
Vervoer	21
Vrijheid van Meningsuiting	21
<b>Informatie</b>	22
Kwetsbaarheden	22
Bewustwording personeel	22
Procedures	22
Fysieke maatregelen	23
IT-beveiliging	23
Vernietigen informatie	25
Afluisterapparatuur	26
<b>Samenvatting</b>	27
<b>Trefwoordenlijst</b>	28
<b>Gebruikte en relevante bronnen</b>	32
<b>Aantekeningen</b>	34

# Inleiding

## Terrorisme

Sinds de terroristische aanslagen in de Verenigde Staten op 11 september 2001 streeft de Nederlandse regering een brede en integrale aanpak van terrorisme na. In Amsterdam en omstreken werken gemeente, justitie, politie, brandweer en gg&gd dit beleid gezamenlijk uit. Doel is het risico op een aanslag te verkleinen en de gevolgen van een eventuele aanslag te beperken. Daarnaast zal de politie er alles aan doen om de daders van een eventuele aanslag op te sporen.

De daadwerkelijk mate van dreiging is lastig te voorspellen. Nieuwe aanslagen kunnen niet worden uitgesloten en dus moet de samenleving zich voorbereiden op een terroristische dreiging en/of aanslag. Dergelijke gewelddadige incidenten zijn gelukkig zeldzaam. Voor de meeste mensen blijft terrorisme iets dat ze alleen kennen van het nieuws. Een klein aantal echter wordt helaas op één of andere manier met een terroristendaad geconfronteerd.

## Bedrijven en terrorisme

Wanneer uw bedrijf (in)direct te maken krijgt met een terroristische aanslag, kan dat allerlei gevolgen hebben. Denk aan: de veiligheid van uw personeel, een storing in uw bevoorrading of een verlies van werk aan concurrenten en faillissement. Het is daarom van belang als bedrijf maatregelen te nemen die drempelverhogend zijn voor terroristen.

Iedereen die de veiligheid van zijn bedrijf of organisatie wil verbeteren, moet beginnen met het maken van een risicoberekening om te bepalen welke maatregelen nodig zijn. Waar probeert u zich tegen te beschermen? Wat zijn uw kwetsbaarheden? Hoe waarschijnlijk is uw bedrijf een doelwit van terroristen? Hoeveel risico lopen omliggende bedrijven?

Wanneer uw bedrijf door een terroristische daad wordt getroffen, zullen de gevolgen voor uw bedrijfsvoering praktisch gezien niet veel anders zijn dan wanneer uw bedrijf in een crisis terechtkomt die niet door terrorisme is veroorzaakt. Een brand ontstaan door de explosie van een bom of door kortsluiting, blijft een brand. Een hacker kan uw computersysteem moedwillig platleggen, maar een stroomstoring kan hetzelfde



# Inleiding

effect hebben. Maatregelen ter voorkoming van terrorisme horen daarom aan te sluiten bij uw (bestaande) crisisbeheer.

## Kosten

Wanneer u besluit veiligheidsmaatregelen te nemen, zult u moeten investeren. De ontwikkeling van goed beleid kost geld, mensuren en middelen. Weeg de kosten tegen de baten af. Zorgvuldige planning kan helpen de kosten laag te houden. Hoewel het belangrijk is niet onnodig te wachten met het nemen van maatregelen, blijven de kosten relatief laag als de aanpassingen samenvallen met ver- of nieuwbouw.

U kunt een erkend beveiligingsbedrijf inschakelen voor een risicoanalyse en voor een beveiligingsplan op maat. Voor de aanschaf van gespecialiseerde apparatuur adviseren wij u contact op te nemen met deskundige leveranciers. Zij kunnen beoordelen en adviseren welke producten u nodig heeft. U kunt de leveranciers met elkaar vergelijken. Zorg voor duidelijkheid over het beoogde doel van het product, de service en garanties die u kunt verwachten. De aanschaf van de apparatuur moet gebaseerd zijn op grondig en systematisch onderzoek, omdat anders uw investering ondoeltreffend, onnodig en duur is.

## Samenwerking

Bij gemeenschappelijke gebouwen, winkelcentra, hoofdstraten en bedrijfsparken is het mogelijk en raadzaam om gezamenlijk maatregelen te nemen die belangrijk zijn voor de bestrijding van misdaad, maar die ook drempelverhogend zijn voor terroristen. Denk bijvoorbeeld aan gemeenschappelijke toegangsbeheerprocedures en het situeren van camera's. Zo worden de doeltreffendheid verhoogd en de kosten gedrukt. Wij verwijzen hier naar het Keurmerk Veilig Ondernemen (KVO) van het Centrum voor Criminaliteitspreventie ([www.ccv.nu](http://www.ccv.nu)). Via KVO kan structureler worden samengewerkt tussen overheid, politie, brandweer en ondernemers. Het biedt een eenvoudig te hanteren methodiek om in nauwe samenwerking doeltreffende, haalbare maatregelen te treffen die de veiligheid vergroten.

## Wettelijke eisen

Uw bedrijf zal aan de verplichtingen uit de Arbo-wetgeving moeten voldoen. Onderdeel van deze wet is

# Inleiding

bijvoorbeeld het bedrijfshulpverleningsplan. Vergeet tevens niet dat alle noodzakelijke vergunningen in orde moeten zijn, zoals de gebruiksvergunning, de milieuvergunning en/of de horecavergunning. Een deel van de voorwaarden genoemd in de wet en in de vergunningen hebben betrekking op uw veiligheid.

## Preventieve maatregelen

Preventieve maatregelen omvatten niet alleen fysieke maatregelen die uw gebouwen beveiligen. Ook maatregelen op het gebied van personeel en informatie zijn belangrijk. Het heeft weinig zin te investeren in dure veiligheidsmaatregelen als die gemakkelijk door een ontevreden personeelslid kunnen worden ondermijnd of de afspraken en regels niet in acht worden genomen door uw medewerkers. Een integrale aanpak, waarbij alle facetten van de bedrijfsvoering onder de loep worden genomen, is daarom essentieel.

Dit handboek biedt een aantal praktische adviezen die zowel kleine als grote bedrijven zullen helpen in de ontwikkeling, herziening of uitbreiding van hun veiligheidsbeleid. De meeste aanbevelingen verbeteren ook uw criminaliteitsbestrijding. Wellicht heeft u in dat kader al een deel van de maatregelen genomen en hoeft u ze alleen vanuit het perspectief van terrorisme opnieuw te bekijken.

Ten slotte willen we opmerken dat dit handboek geen blauwdruk voor uw bedrijf is. De maatregelen die uw bedrijf kan of moet nemen zijn afhankelijk van de omstandigheden waarin uw bedrijf zich bevindt. Alleen een medewerker met inzicht in het daadwerkelijke bedrijfsproces kan overzien welke specifieke maatregelen een bedrijf nodig heeft.



# Gebouwen

Fysieke veiligheid is belangrijk bij de bescherming tegen alle bedreigingen, met inbegrip van terrorisme. Wanneer u de gebouwen beveiligt waarin uw werkzaamheden plaatsvinden, zorgt u indirect voor de veiligheid van uw personeel en informatie.

## Kwetsbaarheden

Bekijk uw gebouwen door de ogen van kwaadwillenden. Waar liggen uw kwetsbaarheden? Wat wilt u het meest beschermen? Waar ligt het grootste risico? Is uw terrein openlijk toegankelijk? Kunnen onbevoegden makkelijk uw gebouw binnenkomen? Hoe kan de meeste schade aan uw gebouw worden toegebracht?

## Bewustwording personeel

Ogen en oren van uw personeel, met inbegrip van schoonmaak- en onderhoudspersoneel, zijn zeer belangrijk. Zij kennen hun eigen kantoor of werkruimte. Moedig ze aan om alert te zijn op vreemd gedrag van personen en op spullen die niet op hun plaats staan of die niet in het bedrijf thuishoren. Informeer hen over ongebruikelijke activiteiten waarop zij moeten letten zoals pakketjes, tassen of andere spullen op vreemde plaatsen, verborgen spullen in vuilnisbakken en vreemden die belangstelling hebben voor minder toegankelijke plaatsen.

Alle niet-fysieke maatregelen ter bescherming van uw gebouwen, bijvoorbeeld een stringent toegangsbeleid, moeten door uw personeel worden uitgevoerd. Bedenk dat elk systeem zo sterk is als de zwakste schakel. Zorg dat uw personeel doordrongen is van het belang van de maatregelen. Houd toezicht op naleving van de afgesproken regels.

## Bouwtechnische maatregelen

Buitendeuren moeten sterk zijn, goed sluiten en over goede sloten beschikken; deuren die maar weinig gebruikt worden, moeten ook nog interne bouten hebben. Houd er bij glazen deuren rekening mee dat de sterkte afhankelijk is van de sterkte van het glas. Ramen op de benedenverdieping en ramen die makkelijk toegankelijk zijn (bijvoorbeeld op een plat dak) moeten beschikken over goede sloten.



# Gebouwen

Wanneer u bijvoorbeeld rampalen en rolluiken voor uw pand wilt plaatsen tegen inbraken is het in de meeste gemeenten verplicht een bouwvergunning en/of uitstallingsvergunning aan te vragen. Informeer vooraf naar de voorwaarden waaronder zulke bouwtechnische aanpassingen worden toegestaan.

Bij moderne gebouwen wordt vaak veel glas gebruikt. Bij een bomontploffing in moderne steden worden de meeste verwondingen veroorzaakt door rondvliegend glas. Veiligheidsglas is een essentiële maatregel om schade te beperken in het geval van een explosie. Efficiënte bescherming kan bijvoorbeeld door het gebruik van folie die, in combinatie met speciaal ontworpen netgordijnen, het versplinterde glas bij elkaar houdt.

## Goed schoon- en onderhouden

Als u uw gebouw binnen en buiten goed schoonhoudt, wordt het moeilijker om er bommen te verbergen en makkelijker een binnengekomen (bom)melding te controleren. U kunt het aantal plaatsen waar bommen e.d. verstopt kunnen worden, verminderen door:

- alle openbare en gemeenschappelijke ruimten, zoals in- en uitgangen, ontvangstruimten, trappen, zalen, toiletten, etc. netjes en schoon te houden;
- het meubilair in dergelijke ruimten tot een minimum te beperken zodat er weinig mogelijkheden zijn om spullen te verstoppen;
- lege kantoren, ruimten en opslagkasten te sluiten;
- ervoor te zorgen dat alles een vaste plaats heeft en dat het zo blijft;
- te overwegen om vuilnisbakken te verwijderen
- eenvoudige verzegeling op onderhoudsdeuren aan te brengen; en
- externe gebieden zo schoon en opgeruimd mogelijk te houden. Snoei alle vegetatie en bomen, vooral dichtbij ingangen, om het toezicht te verbeteren en de kans om iets te verbergen, te verminderen.

## Toegang terrein

Beperk de toegang tot uw bedrijfsterrein, bijvoorbeeld door een voldoende hoog hek. Een hoogte van minstens 2,5 meter wordt voorgeschreven. Zorg voor maatregelen die het onmogelijk maken over het hek



# Gebouwen

te klimmen en/of er onderdoor te kruipen, zoals doornige struiken en betonnen bloembakken. Laat een detectiesysteem installeren.

Zorg ervoor dat uw terrein overzichtelijk is. Verwijder obstakels, zoals emballage of andere plaatsen waar personen zich achter kunnen verschuilen.

Laat beveiligings- of ander personeel onmiddellijk actie ondernemen wanneer onbevoegde individuen rondlopen tussen de auto's van uw personeel, kentekens noteren en de omgeving fotograferen of filmen.

Als u denkt een mogelijk doelwit te zijn voor een autobom, houd dan alle voertuigen op een veilige afstand. Auto's die toegelaten dienen te worden, moeten vooraf worden geïdentificeerd en gecontroleerd. Zorg voor een juiste toegangscontrole en een doordacht aangelegde, verkeersvertragende en krachtige barrière. Houd niet-essentiële voertuigen op minstens 30 meter van uw gebouw.

## Openen en sluiten

Het openen en sluiten van uw bedrijf vraagt om vastgestelde procedures om de veiligheid te vergroten. Als er andere bedrijven in de omgeving zijn, heeft het voordelen om zoveel mogelijk gelijktijdig met deze bedrijven te openen. Er is dan sprake van meer 'beweging' rondom uw bedrijf. Open en sluit indien mogelijk met twee of meer personen. Laat daarbij minstens één iemand op afstand observeren of de situatie veilig is. Controleer het pand voor sluiting op eventuele achterblijvers en op 'voorbewerkte' ramen en deuren. Check voor uw openings- of sluitingsprocedure altijd de omgeving. Indien u onregelmatigheden waarneemt (bijvoorbeeld verdachte personen of voertuigen bij uw uitgangen), stop dan onmiddellijk de procedure en breng uzelf en anderen in veiligheid. Waarschuw altijd de politie. Probeer daarbij zoveel mogelijk details van de verdachte personen en voertuigen door te geven.

## Toegang gebouw

Hang bij de publieksingang een bordje op met een telefoonnummer dat gebeld kan worden bij calamiteiten. Controleer regelmatig of het nummer nog klopt. Maak aan de buitenkant van uw gebouw zichtbaar (bijvoorbeeld d.m.v. borden, stickers, pictogrammen en camera's) dat uw pand beveiligd is.

# Gebouwen

Maak uw bedrijf van buiten naar binnen doorzichtig genoeg. Dit creëert een mogelijkheid tot extra toezicht van buitenaf. Verwijder obstakels of posters die de inkijk in uw pand belemmeren.

Maak een goed sleutelbeheerplan. Beperk het aantal in omloop zijnde sleutels. Neem sleutels van vertrekkende werknemers in en werk met sleutels die tegen kopiëren beveiligd zijn.

Een efficiënt ontvangstgebied is essentieel voor het controleren van de toegang. Zorg dat u weet wie op welk moment van de dag bij u in het pand aanwezig is. Beperk het aantal toegangspunten tot een minimum (liefst één) en zorg dat de grens tussen openbare en privé-gebieden van uw gebouw veilig, goed gesitueerd en duidelijk afgebakend is. Zorg dat eventuele extra ingangen alleen toegankelijk zijn voor geautoriseerde mensen.

Hang borden op die alle personeel, klanten, bezoekers, etc. naar de receptie verwijzen. Introduceer een passersysteem. Zorg ervoor dat personeelsleden hun passen altijd dragen en dat ze regelmatig gecontroleerd worden. Introduceer een bezoekersregistratie met speciale passen voor bezoekers. Vraag bezoekers hun passen zichtbaar boven de kleding te dragen. Zorg dat ze worden begeleid. Bezoekers horen niet zomaar door het gebouw te dwalen. Bij het weggaan dienen de passen te worden ingeleverd. Een ieder die geen pas kan tonen of verdacht handelt, moet onmiddellijk gemeld of overgedragen worden aan de beveiliging of bedrijfsleiding van het bedrijf. Laat bezoekers bij aankomst eventueel details over hun meegenomen voertuig beschrijven.

Het is raadzaam vreemde gedragingen van personen en verdachte incidenten altijd door te geven aan de verantwoordelijk manager inzake veiligheidszaken. Wanneer de informatie zo gedetailleerd mogelijk wordt bijgehouden, kan op den duur wellicht een patroon in de gedragingen worden ontdekt en kunnen potentiële terroristen sneller worden ontmanteld.

## Veiligheid receptie

Het is mogelijk een (stil) alarmsysteem aan te leggen bij de receptie, waarmee de receptionist door het



# Gebouwen

indrukken van een knop om assistentie kan verzoeken wanneer hij of zij te maken krijgt met een lastige bezoeker.

Daarnaast kan gedacht worden aan het aanbrengen van een systeem waarmee vanaf de receptie de buitendeur automatisch gesloten kan worden. De receptionist hoeft zich bij onraad dan niet naar de deur en wellicht in gevaar te begeven.

## Huisregels

Als ondernemer bent u vrij om huisregels op te stellen en deze kenbaar te maken aan uw bezoekers middels een huishoudelijk reglement. Breng het reglement aan bij de ingang en herhaal het zodanig in het bedrijf dat iedereen er kennis van kan nemen. Alleen dan zijn mensen aan de huisregels gebonden. Huisregels zijn bedoeld om aan te geven wat door u als ondernemer wel en niet toelaatbaar wordt geacht. Het is verstandig om tevens aan te geven wat u doet (sancties) als de huisregels worden overtreden. Voorbeelden van huisregels zijn: Het is verboden in dit pand foto-, film- en/of video-opnames te maken. U dient mee te werken aan een tassencontrole als daar om wordt gevraagd.

Bedenk dat mobiele telefoons tegenwoordig vaak ingebouwde camera's hebben. De enige effectieve manier om onbevoegde fotografie in uw gebouw te verhinderen, is door ze te verbieden.

Het willekeurig onderzoeken van (hand)bagage of de kleding is een significant afschrikmiddel. U heeft het recht toegang te weigeren aan iedereen die dat niet toestaat, indien u deze maatregel heeft opgenomen in uw huisregels. Toch mag u pas een tas bekijken of aan de kleding fouilleren indien u toestemming van de betreffende persoon heeft. Voor meer informatie kunt u contact opnemen met het VAKcentrum voor zelfstandige ondernemers in de detailhandel ([www.vakcentrum.nl](http://www.vakcentrum.nl)).

## Aanhouding verdachte

Handelt een bezoeker in strijd met de huisregels, spreek hem of haar hier op aan met zonodig het verzoek uw pand te verlaten. Heeft dit niet het gewenste resultaat dan herhaalt u de vordering. Verlaat de

# Gebouwen

bezoeker uw pand nog niet dan is er sprake van huisvredebreuk (artikel 138 Wetboek van Strafrecht). Het bedrijfspand is namelijk uw 'huis'. U bent bevoegd de man of vrouw, die nu verdachte is geworden, aan te houden.

Omdat er sprake is van een aanhouding op heterdaad (artikel 53 Wetboek van Strafvordering) mag u gestolen spullen, vernielde spullen en/of een geprepareerde tas, die de verdachte "met zich voert" in beslag nemen (artikel 95 Wetboek van Strafvordering). U mag niet in de tas(sen) kijken of er iets uitpakken. Verder mag u niet in of aan de kleding van de verdachte zitten en geen geweld gebruiken. Bel direct het nummer voor spoedeisende politiezaken 112 en draag de verdachte met de inbeslaggenomen spullen onverwijld over aan de politiemensen die ter plaatse komen. U mag de verdachte wel vasthouden tot de politiemensen zijn gearriveerd. Dit moet uiteraard fatsoenlijk en behoorlijk gebeuren.

Let altijd op uw eigen veiligheid, die van uw medewerkers en van uw bezoekers.

## Alarm, camera's en verlichting

Er zijn vele soorten alarmsystemen die waarschuwen tegen indringers. Welke u kiest is afhankelijk van de omstandigheden. Laat u goed informeren door experts. Ga na wie de code van het alarmsysteem kennen. Het is belangrijk de code regelmatig te veranderen. Zorg dat u, wanneer u een alarminstallatie heeft, ook de opvolging in geval van alarm goed heeft geregeld. Een alarm dat afgaat zonder dat er iemand op afkomt, kunt u net zo goed weglaten.

De voordelen van verlichting liggen vooral in afschrikking en herkenning. Een goed verlichtingsplan helpt het veiligheidspersoneel en is van belang bij het toezicht op de bewakingscamera's. Ga wel na of de burens geen last hebben van de verlichting.

Camera's zijn belangrijke componenten van een geïntegreerd veiligheidssysteem. Bewakingscamera's dragen niet alleen bij tot controle en onderzoek na het incident, maar kunnen ook helpen kwaadwillenden af te schrikken. Bedenk wel dat bewakingscamera's slechts efficiënt zijn bij goed onderhoud en regelmatige



# Gebouwen

controle. Vaak blijken camera's bijvoorbeeld verkeerd afgesteld te zijn, is gezichtsherkenning niet mogelijk of zijn de beelden van een dusdanig slechte kwaliteit dat ze niet voor opsporingsdoeleinden kunnen worden gebruikt.

Het gebruik van camera's voor toezicht en beveiliging is slechts toegestaan indien de aanwezigheid van de camera duidelijk is aangegeven. Het is onder voorwaarden toegestaan om camerabeveiliging op te hangen gericht op uw ingang, (nood)uitgangen, langs de gevel en op uw privé-parkeerplaats. Onder stringente voorwaarden mag u tevens gebruikmaken van camerabeveiliging buiten uw pand. Beelden opnemen van openbare parkeergelegenheden of de openbare weg is echter niet toegestaan. De Wet Bescherming Persoonsgegevens stelt zorgvuldigheidseisen voor het gebruik van beelden. De termijn voor het bewaren van videobeelden is in principe gesteld op 24 uur tot een maximum van 7 dagen. Voor videobeelden waarop incidenten zijn vastgesteld geldt een uitzondering. Het College Bescherming Persoonsgegevens (CPB) geeft op zijn website informatie over cameratoezicht. Kijk op: [www.cpbweb.nl](http://www.cpbweb.nl).

Er zijn tegenwoordig 'slimme' camera's op de markt die kunnen worden ingeprogrammeerd om bepaald gedrag te herkennen. Een goed voorbeeld is het rijgedragherkenningssysteem. Inbrekers, overvallers en terroristen zullen hun doelobject altijd bezoeken voordat zij toeslaan. Zo'n bezoek gaat gepaard met een specifiek rijgedrag, dat door het computer/camerasysteem wordt herkend. De computer slaat het kenteken op. Wanneer de auto op een incurante tijd terugkomt, slaat de computer alarm en kunnen de inzittenden op heterdaad worden betrap.

## Logistiek

Neem uw gehele logistieke proces mee in uw denken over veiligheid. Registreer en controleer wie zich op het terrein bevinden. Laat zowel de chauffeur als de mensen van een eventueel beveiligingsbedrijf toezicht houden bij het laden en lossen van goederen. Verzegel de lading met een zegel van het bedrijf. Zorg dat uw personeel direct alarm slaat als de zegel verbroken blijkt. Draag zorg voor een goed voorraadregistratiesysteem. Stel goede procedures op en maak duidelijke afspraken met uw chauffeurs. Controleer of zij zich aan de afspraken houden. Laat bijzondere ladingen door twee chauffeurs rijden. Verspreid het vervoer

## Gebouwen

van 'aantrekkelijke' goederen en zorg dat niet zichtbaar is wat er wordt vervoerd. Zorg dat niet constant dezelfde routes worden gereden en partijen of goederen op dezelfde wijze worden afgehandeld. Breng variatie aan om zodoende de risico's te verminderen. Laat chauffeurs met risicoladingen onderweg niet stoppen. Maak afspraken met ontvangers van de goederen over de duur van het laden en lossen. Vermijd lange wachttijden.

### Brandpreventie

Neem maatregelen om het risico op brand te verminderen. Zorg dat op uw terrein geen brandgevoelig materiaal geplaatst is binnen een afstand van minder dan 10 meter van een gevel van uw gebouw of van het buurbedrijf. Laat pallets en afval regelmatig afvoeren en voorzie afvalcontainers altijd van een deksel.

Wanneer uw bedrijf werkt met gevaarlijke stoffen is het van belang dat u deze opslaat, verwerkt en vernietigt in een zo veilig mogelijke omgeving. Vermijd toegang tot deze stoffen voor onbevoegden.

Branddeuren moeten functioneren en brandwerende scheidingsen moeten intact zijn. Zorg dat brandinstallaties goed werken en jaarlijks worden onderhouden. Let op dat er iemand in het bedrijf is die ze kan bedienen. Zorg tevens voor voldoende slaghaspels en brandblusapparaten in uw gebouw en zorg ervoor dat ze jaarlijks door een erkend onderhoudsbedrijf gecontroleerd worden. Weten uw medewerkers hoe ze moeten worden gebruikt?

Maak een ontruimingsplan. Zorg voor instructies aan het personeel, zodat iedereen weet wat zijn/haar taak is op het moment dat er ontruimd moet worden. Oefen deze plannen regelmatig met uw personeel. De vluchtroutes in uw pand moeten duidelijk herkenbaar zijn en mogen niet worden geblokkeerd door obstakels. De instructie, het ontruimingsplan en het oefenen zijn verplichtingen uit de Arbo-wet.

De brandweer kan u een preventie-advies op maat geven, specifiek voor uw bedrijf ([www.brandweer.nl](http://www.brandweer.nl)). Houd periodiek contact met de brandweer waarin u ook informatie geeft over eventuele gevaarlijke stoffen of brandgevaarlijke situaties. Zorg dat uw bedrijf goed bereikbaar is voor de brandweer.



## Personeel

Een deel van de maatregelen in dit hoofdstuk dient ter bescherming van uw bedrijf tegen kwaadwillende personeelsleden. Een ander deel betreft de veiligheid van uw personeel.

### Kwetsbaarheden

Concurrenten, misdadigers, spionnen, maar ook terroristen kunnen samenwerken met iemand van binnen uw organisatie. Dit kan een vaste of tijdelijke werknemer zijn of extern personeel (bijv. schoonmakers, catering, beveiligingsbeambten) dat toegang heeft tot uw gebouw. Deze 'insiders' kunnen als nieuw personeel in de organisatie geïnfiltrerd worden of binnen de organisatie worden geworven om een specifieke rol uit te voeren. Heeft u zicht op de betrouwbaarheid van uw personeel?

Behalve tegen het bedrijf kan een terroristische daad zich ook richten tegen de mensen die voor uw bedrijf werken. Terroristen zullen in enkele gevallen de identiteit en adresgegevens van werknemers van bepaalde bedrijven of organisaties willen achterhalen. Zeker het hogere management, commissarissen en/of bestuursleden behoren hierover na te denken.

### Bewustwording personeel

Moedig uw managers en personeel aan waakzaam te zijn op vreemd gedrag van collega's en dat te rapporteren. Om verdenkingen omtrent collega's te melden is vertrouwen nodig. Laat hen weten dat elke melding, ook als het later vals alarm blijkt te zijn, serieus wordt genomen en wordt beschouwd als een bijdrage aan een veilig bedrijf. Creëer een werkomgeving waarin vertrouwelijk en informeel over eigen zorgen en problemen kan worden gesproken. Stel uw personeel gerust dat alle informatie vertrouwelijk zal worden behandeld. Bescherm klokkenluiders.

Als nieuw personeel zichzelf aanbiedt behoort u extra alert te zijn. Probeer achter de beweegredenen voor de sollicitatie en het verlaten van de vorige baan te komen.

### De 'insider'

'Insiders' kunnen toegang tot uw gebouw of informatie misbruiken of benutten om de volgende redenen:

# Personeel

persoonlijke winst, verving, wraak of externe sympathieën. Soms gaat het om kwetsbare personeelsleden die onder bedreiging of door chantage tot medewerking worden gedwongen. Wat de motivatie ook is, een 'insider' kan significante schade aan uw bedrijf toebrengen.

Direct leidinggevend (leren) letten op bijzondere signalen. Klopt het bestedingspatroon van de medewerker in relatie tot zijn salaris? Onderteken bijvoorbeeld niet zomaar een werkgeversverklaring in verband met een hypotheekaanvraag. Klopt de aanvraag met het inkomen van de medewerker? Ken de persoonlijke problemen van uw medewerkers. Weet u tegen wie een loonbeslag loopt? Wie er vaak ziek is? Wat uw medewerkers doen in hun vakantie? Welke nevenfuncties uw medewerkers vervullen?

Maak beleid voor het geval u geconfronteerd wordt met niet-integer gedrag door uw personeel. Praat openlijk over afwijkend gedrag en corrigeer dit gedrag. Maak ook duidelijk welke sancties u hanteert in geval van interne criminaliteit. Zorg dat alle leidinggevend hierin het goede voorbeeld geven.

Zorg voor duidelijke taak- en functieomschrijvingen. Spreek mensen erop aan als zij hier niet aan voldoen. Leg personeelsdossiers aan waarin u alle belangrijke stukken bewaart, zoals het sollicitatieformulier, beoordelingen, gemaakte afspraken, enzovoort. Schenk in uw functionerings- en beoordelingsgesprekken aandacht aan veiligheid.

Laat medewerkers op risicoplekken regelmatig wisselen van werkplek. Organiseer bijvoorbeeld elke drie jaar jobrotation of een betrouwbaarheidscheck.

Overweeg toegangscontrole tot bijzonder 'gevoelige' ruimten. Minimaliseer de toegang tot vertrouwelijke plaatsen of informatie voor een deel van uw personeel.

### Aanname nieuw personeel

Onderzoek de betrouwbaarheid van de potentiële werknemer. Vraag de sollicitant om de volledige naam, geboortedatum en adres, en vraag hem/haar een officieel document met foto zoals een paspoort of



# Personeel

rijbewijs te tonen. Vraag om een recent rekeningafschrift om te controleren of het opgegeven adres klopt. Accepteer slechts originele documenten, want met kopieën kan makkelijker geknoeid worden. Verder kunt u om een bewijs van school- en/of beroepskwalificaties verzoeken. In hoeverre klopt het curriculum vitae? Let op schrijffouten en 'gaten' in de loopbaan. Veel bedrijven vragen om referenties, maar checken ze niet. Wij raden u aan dat toch te doen. Maak de sollicitant duidelijk wat u bij wie gaat checken en vraag om toestemming. Wat doet u als de referenties niet kloppen? Indien relevant vraagt u om een werkvergunning. Herinner sollicitanten eraan dat het verstrekken van valse inlichtingen een reden tot ontslag kan zijn.

Stel een betrouwbaarheidsprofiel op voor kwetsbare functies. Maak beleid met betrekking tot aanname van personeel op standaard-, risico- en vertrouwensfuncties. Wanneer u bijvoorbeeld topmanagers wilt aan nemen is een attitude-assesment mogelijk. Houd u ook in tijden van schaarste aan de door u vastgestelde criteria. Laat een geheimhoudingsverklaring en concurrentiebeding ondertekenen door medewerkers op gevoelige functies.

Informeel nieuwe medewerkers over de geldende normen, waarden, regels, procedures en afspraken (bijvoorbeeld door het uitreiken van het huisreglement) en geef aan welke sancties op het niet naleven van deze zaken staan.

### Verklaring Omtrent Gedrag

U kunt als werkgever een Verklaring Omtrent het Gedrag (VOG) aanvragen voor een natuurlijk persoon. In de volksmond ook wel bekend als 'bewijs van goed gedrag'. Vaak gebeurt dat als een nieuwe medewerker naar een functie solliciteert waarbij wordt gewerkt met vertrouwelijke gegevens, kwetsbare personen, geld of goederen. Voor sommige functies, zoals onderwijzer en taxichauffeur, is de verklaring zelfs verplicht.

De Verklaring Omtrent het Gedrag wordt uitgegeven door het Centraal Orgaan Verklaring Omtrent het Gedrag. Hoe u ze kunt aanvragen en andere informatie over dit onderwerp leest u op [www.justitie.nl](http://www.justitie.nl).

# Personeel

## Centraal Krediet Informatiesysteem

Schulden maken een werknemer mogelijk chantabel en u wilt weten of uw toekomstig werknemer kwetsbaar is. Het Bureau Krediet Registratie, kortweg BKR, informeert over het leen- en aflosgedrag van consumenten in Nederland. In het Centraal Krediet Informatiesysteem (CKI) van het BKR worden betalingsverplichtingen van consumenten die de afgelopen vijf jaar een krediet of kredietfaciliteit op hun naam hebben staan, vastgelegd.

De consument kan toegang krijgen tot zijn of haar eigen gegevens. Op deze basisregel gelden geen uitzonderingen, ook niet voor de werkgever. Vraag uw toekomstig werknemer daarom zijn eigen dossier op te vragen en aan u te overhandigen. Naast persoonsgegevens, treft u kredietgegevens aan en eventuele bijzonderheden gedurende de looptijd van het krediet. U ziet bovendien welke instelling het krediet ter verwerking aan BKR heeft aangeboden. Meer informatie vindt u op [www.bkr.nl](http://www.bkr.nl).

## Contractanten en extern personeel

Het gebruik van contractanten en extern personeel voor een groeiende groep diensten (bijvoorbeeld de IT-sector, schoonmaken, catering en veiligheid) kan nieuwe kwetsbaarheid tot stand brengen en ondernemingen blootstellen aan grotere 'insider'- bedreiging. Terwijl sommige uitzendorganisaties in hun selectieprocedures zorgvuldig zullen zijn, lopen uitzendorganisaties die minder streng zijn – en in het bijzonder organisaties die buitenlandse arbeiders in dienst hebben – het risico benut te worden door terroristen, hun sympathisanten en anderen die uw bedrijf willen beschadigen.

Zorg ervoor dat de uitzendorganisatie waarmee u zaken doet een contract ondertekent waarin de goede trouw van haar personeel wordt bevestigd. Maak duidelijke afspraken over de functie-, betrouwbaarheids- en vakbekwaamheidseisen die u aan uw medewerkers stelt. Bij gevoelige functies is het verstandig alsnog zelf onderzoek te doen naar de betrouwbaarheid van het geleverde personeel. Houd regelmatig toezicht op de naleving van het contract door het uitzendbureau. Benoem een vast personeelslid dat verantwoordelijk is voor het contractpersoneel (dat wil zeggen niet slechts om te letten op naleving van het contract) zodat potentiële problemen, zoals conflicten van loyaliteit, sneller wordt ontdekt.



# Personeel

## ID-plicht en pasjes

Zorg voor procedures om te controleren of de persoon die bij u verschijnt, ook daadwerkelijk degene is die door het uitzendbureau wordt gestuurd. Vraag het bureau om vooraf een recente foto plus zijn of haar volledige naam te verstrekken. Vraag iedere contractant een identiteitskaart met foto te tonen bij de ingang of receptie van uw gebouw. Dit moet geen probleem zijn, aangezien op 1 januari 2005 artikel 2 van de Wet op de Identificatieplicht in werking is getreden. Iedereen vanaf 14 jaar moet een geldig identiteitsbewijs tonen als daar door de politie, buitengewoon opsporingsambtenaar of een aangewezen toezichthouder om gevraagd wordt.

Controleer of de gegevens overeenkomen en verstrek passen met een foto aan het contractpersoneel. De pas moet altijd zichtbaar worden gedragen. Het is het beste als u de pas na het werk inneemt en de volgende dag weer overhandigt na (wederom) controle van de foto.

Controleer de contractmedewerkers wanneer zij in het gebouw zijn en vooral als zij toegang tot gevoelige ruimten hebben. Denk na over het inperken van de bevoegdheid van stagiaires, ingehuurde en vervangende krachten. Zorg voor goede begeleiding.

## Zakenrelaties

In veel van uw bedrijfsprocessen spelen externe relaties een belangrijke rol. De continuïteit van uw bedrijf is sterk afhankelijk van uw partners in business. Weet u wie uw klanten, leveranciers, adviseurs en geldverschaffers zijn? Doe gedegen onderzoek naar de kredietwaardigheid van de (potentiële) zakenrelaties die u inschakelt. Wees achterdochtig bij afwijkende zaken, zoals grote contante betalingen en vreemde combinaties van goederen. Weet u in welk netwerk uw partners zitten?

De Verklaring Omtrent het Gedrag voor rechtspersonen (VOGrp) is een nieuw instrument waarmee rechtspersonen hun integriteit kunnen tonen aan partners, andere bedrijven en overheden. U kunt deze verklaring voor uw eigen organisatie aanvragen, maar ook door een andere organisatie, waarmee u bijvoorbeeld zaken wilt doen, laten aanvragen. De VOGrp is een verklaring van de Minister van Justitie dat, voor het

# Personeel

doel waarvoor de VOGrp is aangevraagd, hem niet is gebleken van bezwaren tegen de betreffende rechts-persoon. Het Centraal Orgaan Verklaring Omtrent het Gedrag geeft de verklaring namens de Minister af. Kijk voor meer informatie op [www.justitie.nl](http://www.justitie.nl).

### Veiligheid personeel

Behalve tegen het bedrijf kan een terroristische daad zich ook richten tegen de mensen die voor uw bedrijf werken. Ook wanneer zij zich niet in het bedrijf bevinden, maar zich ophouden in openbare gelegenheden of wanneer zij thuis zijn kunnen zij (of hun familie) bedreigd, geïntimideerd en/of belaagd worden.

Terroristen zullen de identiteit en adresgegevens van werknemers van bepaalde bedrijven of organisaties willen achterhalen. Ga daarom uitermate voorzichtig om met persoonlijke gegevens van al uw medewerkers, zeker van het hogere management, commissarissen en/of bestuursleden.

Het is lastig om privé-gegevens, zoals het huisadres, te beschermen. Probeer dit toch zoveel mogelijk te doen. Vraag een geheim telefoonnummer aan. Laat privé-adressen uit bestanden, bijvoorbeeld van zakenpartners, verwijderen. Wijs uw personeel, maar ook uw familieleden (bijvoorbeeld kinderen) erop geen onnodige gegevens over u, waar u werkt en waar u woont aan derden te verstrekken.

Sinds 1 april 2004 is artikel 32 in het Besluit Handelsregister gewijzigd. Het geeft commissarissen, bestuurders en aandeelhouders onder bepaalde voorwaarden de mogelijkheid hun privé-gegevens uit de registers van de Kamer van Koophandel te weren. Neem voor meer informatie contact op met de Kamer van Koophandel ([www.kvk.nl](http://www.kvk.nl)).

### Waarschuwingssysteem

Stel zelf wel een lijst samen met de gegevens van uw personeel. Noteer onder andere welke familieleden moeten worden ingelicht indien het personeelslid iets overkomt. Bewaar de lijst ook op een plaats buiten het bedrijf. In geval van calamiteiten bent u in staat uw medewerkers of hun familieleden te bereiken. Ga (uiteraard) zorgvuldig om met de gegevens. Check regelmatig of de gegevens nog up-to-date zijn.



# Personeel

### Vervoer

Sluit uw auto altijd deugdelijk af. Laat in uw auto geen (persoonlijke) items liggen die verwijzen naar personen of naar uw werk.

Zorg dat er altijd iemand bij u thuis of op kantoor is die weet waar u heen gaat, wie u zult ontmoeten, hoe u reist, wanneer u verwacht aan te komen en wanneer u verwacht weer terug te zijn. Zorg dat deze persoon weet wat te doen als u onverwacht verlaat bent. Maak aantekeningen van verdachte personen of vreemde voertuigen en meld dit aan de politie. Probeer (in bijzondere gevallen) variatie aan te brengen in uw routes en vertrektijden.

### Vrijheid van meningsuiting

Wanneer u publiekelijk spreekt, realiseert u zich dan dat u met uitspraken die als onbehoorlijk kunnen worden gezien of die extreme persoonlijke meningen bevatten, de aandacht van extremisten op u kunt vestigen.



# Informatie

Informatie is gewild. Informatie over medewerkers of informatie over ontwikkelingen in uw bedrijf. Bedrijfsconcurrenten, misdadigers, buitenlandse inlichtingendiensten, spionnen of terroristen kunnen proberen toegang tot uw informatie te krijgen door in te breken in uw IT-systemen, door in het bezit te komen van gegevens die u hebt weggegooid of door te infiltreren in uw organisatie. Een inbreuk in uw systemen veroorzaakt niet alleen (flinke) ontwrichting van uw zaken. Als informatie over u of uw bedrijf in gevaar is gebracht, kan dat schadelijk zijn voor uw reputatie en geloofwaardigheid in de markt. Laat informatiebeveiliging daarom een belangrijke rol in uw geïntegreerde veiligheidsbeleid zijn.

## Kwetsbaarheden

Ga na waar uw kwetsbaarheden liggen op het gebied van informatiehuishouding. Inventariseer welke informatie aanwezig is, welke informatiedragers en hoe de informatiestromen lopen. In welke mate is uw informatie riskant? Ontwikkel duidelijk beleid over het omgaan met informatie. Benoem de waarde van de informatie en maak onderscheid in verschillende soorten gegevens naar de mate van vertrouwelijkheid. Stel richtlijnen op over hoe met vertrouwelijke stukken moet worden omgegaan. Ga na hoe belangrijke documenten worden beheerd. De maatregelen die u neemt om uw informatie te beschermen, zullen afhangen van de mate van waarschijnlijkheid dat uw organisatie een mogelijk doelwit is.

## Bewustwording personeel

Maak uw personeel bewust van de risico's en de potentiële kosten voor uw bedrijf als informatie in verkeerde handen valt. Stel samen met uw personeel regels voor het omgaan met informatie vast. Het heeft namelijk geen zin procedures te maken waar uw personeel niet achter staat. Het is niet moeilijk om systemen op te zetten. Het handhaven van een dergelijke systemen vereist echter veel discipline. Als uw medewerkers de genomen maatregelen begrijpen, zullen zij de procedures beter volgen.

## Procedures

Leg samen met uw medewerkers regels voor documentbeheer, gebruik, opslag, reproductie en vernietiging van informatiedragers vast. Bepaal hoe lang welke gegevens worden bewaard.



# Informatie

Geef uw personeelsleden alleen toegang tot de informatie die ze nodig hebben voor de uitoefening van hun functie. Maak afspraken met uw personeel over geheimhouding en zet deze afspraken op papier. Herinner uw personeel aan de afspraken als het dienstverband eindigt.

Vraag u af welke informatie uw personeel over de telefoon mag verstrekken. Sommige informatie kan tegen u of tegen individuele medewerkers van uw bedrijf worden gebruikt. Laat uw medewerkers altijd de identiteit van de beller achterhalen alvorens zij informatie doorgeven. Als ze niet zeker zijn, behoren ze de beller terug te bellen na het telefoonnummer in het telefoonboek te hebben gecheckt.

## Fysieke maatregelen

Neem basisveiligheidsmaatregelen. Schaf bijvoorbeeld beveiligde kasten aan en sluit deuren en ramen af. Probeer te vermijden dat materiaal wordt achtergelaten op bureaus, white boards, notitieborden en dergelijke, waar het gelezen of verwijderd kan worden door een toevallige voorbijganger, een bezoeker of een contractant. Beperk het meenemen van informatiedragers, zoals laptops en dossiers, naar buiten.

Bewaar vertrouwelijke en bedrijfsgevoelige documenten in een (inbraak- en brandwerende) kluis. Het is raadzaam kopieën van onmisbare systemen ook in andere gebouwen te bewaren, bij voorkeur op voldoende afstand van uw bedrijf, zodat u niet in de problemen komt indien u bij calamiteiten de toegang tot uw straat of bedrijf wordt ontzegd.

## IT-beveiliging

Een elektronische aanval kan van verschillende kanten komen. Ook terroristen kunnen in uw systemen inbreken. Hoewel zij meestal voor een fysieke aanval zullen kiezen, zijn er aanwijzingen dat terroristen steeds meer gebruikmaken van computers om bijvoorbeeld geheim te communiceren, propaganda te verspreiden en informatie te verzamelen.

Typische manieren om elektronisch aan te vallen zijn hacken (binnendringen in een beveiligd computersysteem), het toevoegen van kwaadwillige hard- of software en het uitschakelen van functionaliteiten.

# Informatie

Elektronisch aanvallen is redelijk makkelijk, omdat hulpmiddelen om dergelijke aanvallen op te zetten overal beschikbaar zijn en vaak van internet gedownload kunnen worden.

Zoals bij andere veiligheidsmaatregelen, moet u ook op IT-gebied analyseren welk risico u loopt. De omvang van het risico bepaalt de omvang van de maatregelen die u moet toepassen. Als u niet zeker bent dat u over de noodzakelijke deskundigheid beschikt om dit te doen, kunt u systeembeveiligingsdeskundigen benaderen voor advies.

Wanneer uw medewerkers de werkplek verlaten, behoren zij de computer en de monitor uit te schakelen. Beveilig alle computers met een wachtwoord. Medewerkers moeten zorgvuldig omgaan met hun wachtwoord. Verbied medewerkers op elkaars autorisatie te werken en blokkeer wachtwoorden van vertrekkende medewerkers. Laat medewerkers niet op een PC werken, maar op servers waarop ze moeten inloggen. Dan is beter te traceren wie welke bestanden raadpleegt. Voer verschillende autorisatieniveaus in voor verschillende gebruikers om bepaalde gegevens te beschermen.

Als er bijzondere informatie is die u wenst te beschermen, kunt u overwegen de informatie te coderen. Ook hierover kunt u om advies vragen, afhankelijk van hetgeen u wenst te coderen.

Inbraak via de telefoonlijn is te voorkomen door medewerkers alleen op internet te laten middels een stand-alone computer. Detecteer, signaleer en registreer alle inbraakpogingen in een on-line verbinding. Stel gedrags- en gebruikscodes op voor internet en zorg voor naleving. Mag iedereen internetten? Mogen alle sites worden bezocht?

Zorg ervoor dat computers die met het internet verbonden zijn met antivirus software zijn uitgerust, aangezien de meeste virussen van internet afkomstig zijn. Download regelmatig 'signature files' van de website van uw antivirus softwareleverancier. Elk van deze 'files' beschermt u tegen een bepaald type computer-virus. Maak verder regelmatig back-ups van uw informatie. Het is verstandig de back-ups (ook) elders te bewaren.



# Informatie

Koop uw systemen van betrouwbare fabrikanten en leveranciers. Zorg ervoor dat uw software zo goed mogelijk is geüpdate. Leveranciers van software maken voortdurend nieuwe beveiligingen in hun software. Deze updates zijn beschikbaar op hun websites. Controleer dit zeer geregeld.

Verzekeer u ervan dat degenen die uw systemen onderhouden, bedienen en bewaken betrouwbaar en eerlijk zijn. 'Insiders' kunnen uw systeem makkelijk saboteren. Vraag regelmatig om raad aan systeem- en service-verleners. Mocht u uiteindelijk toch een aanval ontdekken, vraag dan onmiddellijk om advies.

## Vernietigen informatie

Zorg dat gevoelige gegevens die niet meer vereist zijn, behoorlijk worden vernietigd. Vrijwel alle bedrijven ontdoen zich van grote hoeveelheden papier- en digitaal afval, waartussen zich vertrouwelijke en geheime correspondentie, plannen, cijfers of formules bevinden. Afhankelijk van de industrie, bevat dergelijk materiaal ook personeelsnamen en adressen, privé en interne telefoonnummers, productinformatie, klanten-details, technische beschrijvingen en chemische of biologische formules. Vooral in de laatste twee tonen terroristen interesse.

De belangrijkste middelen om vertrouwelijk afval te vernietigen, zijn de volgende: verscheuren, verbranding, vernietiging, verpulveren, schuring, demagnetiserende, zure en chemische technieken. Verzekeer u er voor aanschaf van, dat het beoogde vernietigingsapparaat voldoende is om de gewenste graad van vernietiging te bereiken. Welke materialen wilt u vernietigen, in welke hoeveelheden en hoe vertrouwelijk is het?

Zorg dat de vernietigingsprocedures veilig zijn. Het heeft weinig zin te investeren in kostbare apparatuur als de mensen die ermee werken zelf een risicofactor zijn. In grote organisaties zou vertrouwelijk afval eerder onder de verantwoordelijkheid van de veiligheidsmanager dan van de faciliteitenbeheerder moeten vallen.

# Informatie

Als u gebruik maakt van de diensten van een afvalverwijderingsbedrijf zorg er dan voor dat hun procedures en apparatuur voldoen aan de norm. Welke apparatuur hebben zij? Word toezicht gehouden op de inzameling en vernietiging? Zijn de auto's die gebruikt worden bij de inzameling dubbel bemand, zodat altijd iemand bij de auto achterblijft terwijl de ander verzamelt?

## Afluisterapparatuur

Als u redenen heeft om te geloven dat afluisterapparatuur in uw gebouw aanwezig is of dat u te maken heeft met een andere technische aanval, kunt u een beroep doen op veiligheidsbedrijven om uw gebouw en apparatuur 'schoon' te maken. Vraag echter niet om advies - zelfs niet in versluierde taal - in een ruimte of via een telefoon, die vermoedelijk wordt afgeluisterd. Als de aanvaller door uw verdenking wordt gealarmeerd, zal hij eenvoudig de apparatuur verwijderen of uitschakelen totdat uw veiligheidsdienst de boel veilig heeft verklaard. Gebruik een ander gebouw voor dergelijke mededelingen. Overigens hoeft het niet persé zo te zijn dat onverklaarbaar geklik of andere eigenaardigheden op uw telefoonlijn betekenen dat u wordt afgeluisterd.



# Samenvatting

- Maak een risicoberekening. Wat zijn uw kwetsbaarheden?
- Laat de maatregelen die u gaat nemen aansluiten bij uw (bestaande) crisisbeheer.
- Welke maatregelen heeft u in het kader van criminaliteitsbestrijding al genomen?
- Ga na welke maatregelen u verplicht bent te nemen. Denk aan de Arbo-wet.
- Het nemen van veiligheidsmaatregelen kost geld. Zorgvuldige planning kan helpen de kosten laag te houden. Wacht echter niet onnodig lang.
- Ga na of u kunt samenwerken met andere bedrijven. Dit is doeltreffend en kostenbesparend.
- Verbeter de bewustwording van uw personeel. Elk systeem is zo sterk als de zwakste schakel.
- Moedig uw managers en personeel aan waakzaam te zijn en verdachte personen, pakketjes, voertuigen en gedragingen te melden.
- Neem bouwtechnische maatregelen.
- Houd uw gebouw binnen en buiten goed schoon.
- Beperk de toegang tot uw terrein en gebouw.
- Zorg voor veilige openings- en sluitingsprocedures.
- Het opstellen van huisregels in een huishoudelijk reglement levert veel mogelijkheden op.
- Denk aan het aanleggen van alarmsystemen, camerabewaking en verlichting.
- Beschouw uw logistiek als onderdeel van uw bedrijf. Neem veiligheidsmaatregelen.
- Brandpreventie is een essentieel onderdeel van uw veiligheidsbeleid.
- Wees alert op 'insiders' en de schade die zij kunnen aanrichten.
- Onderzoek de betrouwbaarheid van nieuw personeel.
- Controleer de identiteit van de contractant die zich bij uw bedrijf meldt.
- Onderzoek de betrouwbaarheid van uw zakenrelaties.
- Scherm privé-gegevens van uw personeel zoveel mogelijk af.
- Maak een waarschuwingssysteem voor calamiteiten.
- Neem het woon-werkverkeer van uw medewerkers mee in uw denken over veiligheid.
- Het publiekelijk uiten van uw mening kan de aandacht van terroristen op u vestigen.
- Maak samen met uw medewerkers procedures over het omgaan met informatie.
- Geef uw medewerkers alleen toegang tot informatie dat zij voor de daadwerkelijke uitoefening van hun functies nodig hebben.
- Basisveiligheidsmaatregelen, zoals het gebruik van beveiligde kasten en/of kluisen, zijn goed om vertrouwelijke informatie op te slaan.
- Houd de beveiliging van uw digitale bestanden up-to-date.
- Vernietig gevoelige informatie op een correcte manier.
- Schakel experts in als u gelooft te worden afgeluisterd.

## Trefwoordenlijst

Aanhouding	11, 12
Aanname personeel	16, 17
Afluisterapparatuur	26
Afvalverwijderingsbedrijf	26
Alarmsystemen	10, 12
Antivirus software	24
Attitude-assessment	17
Autobom	9
Autorisatie	10, 24
Betrouwbaarheidscheck	16
Beveiligingsbedrijf	5, 13
Bewustwording personeel	7, 15, 22
Bezoekersregistratie	10
Bommelding	8
Bouwtechnische maatregelen	7
Bouwvergunning	8
Brandpreventie	14
Bureau Krediet Registratie	18
Camera's	9, 11, 12, 13
Centraal Krediet Informatiesysteem	18
Centraal Orgaan Verklaringen omtrent het Gedrag	17, 20
Centrum voor criminaliteitspreventie	5
Coderen	24
Computers	23, 24
Computervirus	24
Concurrentiebeding	17
Contractanten	18, 19
Criminaliteitsbestrijding	6



## Trefwoordenlijst

Crisisbeheer	5
Curriculum vitae	17
Digitaal afval	25
Documentbeheer	22
Electronische aanvallen	23
Extern personeel	15, 18
Fotograferen	9, 11
Fouilleren	11
Functieomschrijvingen	16
Fysieke maatregelen	7, 23
Gebouwen	7
Gebruiksvergunning	6
Geheimhoudingsverklaring	17
Gevaarlijke stoffen	14
Glas	7, 8
Goed schoon- en onderhouden	8
Horecavergunning	6
Huishoudelijk reglement	11
Huisregels	11
Huisvredebreuk	12
ID-plicht	19
Inbeslaggenomen	12
Informatie	22
Informatiebeveiliging	22
Insiders	15, 25
Internet	24
IT-beveiliging	23
Jobrotation	16

## Trefwoordenlijst

Keurmerk Veilig Ondernemen	5
Klokkenluiders	15
Kosten	5, 22
Kwetsbaarheden	4, 7, 15, 22
Lastige bezoeker	11
Logistiek	13
Milieuvergunning	6
Mobiele telefoons	11
Niet-integer gedrag	16
Ontruimingsplan	14
Openingsprocedure	9
Papierafval	25
Partners	19, 20
Pasjessysteem	10, 19
Personeel	15
Preventieve maatregelen	6
Procedures	9, 13, 17, 18, 19, 22, 25, 26
Publieksingang	9
Rampalen	8
Risicoladingen	14
Rolluiken	8
Samenwerking	5, 15
Selectieprocedures	18
Sleutelbeheerplan	10
Slimme camera's	13
Sluitingsprocedure	9
Sollicitant(en)	16, 17
Tassencontrole	11



## Trefwoordenlijst

Telefoon	11, 23, 26
Terrorisme	4
Toegang terrein	8
Uitstallingsvergunning	8
Uitzendorganisaties	18
Veiligheid personeel	7, 15, 20
Veiligheid receptie	10
Veiligheidsglas	8
Verdachte	11, 12
Vergunningen	6
Verklaring Omtrent het Gedrag	17, 20
Verklaring Omtrent het Gedrag voor Rechtspersonen	19, 20
Verlichting	12
Vernietigen informatie	25
Vernietigingsapparaat	25
Vertrouwelijk afval	25
Vervoer	14, 21
Vluchtroutes	14
Vorbewerkte ramen en deuren	9
Vorraadregistratiesysteem	13
Vordering	11
Vrijheid van meningsuiting	21
Waakzaam	15
Waarschuwingssysteem	20
Wachtwoorden	24
Wettelijke eisen	5
Zakenrelaties	19

# Gebruikte en relevante bronnen

- Notitie uitgangspunten aanpak terrorisme regiopolitie Amsterdam-Amstelland 2004 - Regiopolitie Amsterdam-Amstelland
- Notitie uitgangspunten bij de aanpak van terrorisme in Amsterdam - Directie Openbare Orde en Veiligheid, Operationeel Team Bestuursdienst 2004
- Overvallen Preventiepakket Amsterdam - uitgave regiopolitie Amsterdam-Amstelland
- Security Mainport Rotterdam, een betrouwbare logistieke keten - uitgave Regionaal Platform Criminaliteitsbeheersing Rotterdam
- Brochure Veilig Ondernemen - uitgave van het VAKcentrum voor zelfstandige ondernemers in de detailhandel.
- Brochure Keurmerk Veilig Ondernemen - uitgave van Centrum voor Criminaliteitspreventie en Veiligheid.
- Handboek voor het Keurmerk Veilig Ondernemen voor bestaande Bedrijventerreinen - uitgave Centrum voor Criminaliteitspreventie en Veiligheid
- Handboek voor het Keurmerk Veilig Ondernemen Bedrijventerreinen Nieuwbouw - uitgave Centrum voor Criminaliteitspreventie en Veiligheid
- Actieplan Veilig Ondernemen - uitgave Centrum voor Criminaliteitspreventie en Veiligheid
- Publicatie Aanpak criminaliteit op bedrijvenlocaties - uitgave van Ministerie van Economische Zaken.
- Publicatie Aanpak criminaliteit in winkelgebieden - uitgave van Ministerie van Economische Zaken.
- Wegwijzer Winkelcriminaliteit - gezamenlijke uitgave van Centrum voor Criminaliteitspreventie en Veiligheid, het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties en het Ministerie van Justitie.
- Business Response to Terrorism - uitgave Metropolitan Police London
- Extremism, protecting people and property - uitgave Home Office
- Bombs, protecting people and property - uitgave Home Office
- Business as usual, maximising business resilience to terrorist bombings - uitgave Home Office
- [www.politie.nl](http://www.politie.nl)
- [www.politie-amsterdam-amstelland.nl](http://www.politie-amsterdam-amstelland.nl)
- [www.aivd.nl](http://www.aivd.nl)
- [www.amsterdam.nl](http://www.amsterdam.nl)
- [www.eenveiligamsterdam.nl](http://www.eenveiligamsterdam.nl)



# Gebruikte en relevante bronnen

- [www.overheid.nl](http://www.overheid.nl)
- [www.justitie.nl](http://www.justitie.nl)
- [www.bzk.nl](http://www.bzk.nl)
- [www.ez.nl](http://www.ez.nl)
- [www.belastingdienst.nl](http://www.belastingdienst.nl)
- [www.ccv.nu](http://www.ccv.nu)
- [www.vakcentrum.nl](http://www.vakcentrum.nl)
- [www.kvk.nl](http://www.kvk.nl)
- [www.bkr.nl](http://www.bkr.nl)
- [www.pcr.rotterdam.nl](http://www.pcr.rotterdam.nl)
- [www.mi5.gov.uk](http://www.mi5.gov.uk)
- [www.homeoffice.gov.uk](http://www.homeoffice.gov.uk)
- [www.pfe.gov.uk](http://www.pfe.gov.uk)
- [www.ready.gov](http://www.ready.gov)





