

Handreiking beveiliging

voor bijeenkomsten in het Hoger Onderwijs

Titel document	Handreiking Beveiliging - voor bijeenkomsten in het Hoger Onderwijs
Organisatie	IV-community Integraal Veilig Hoger Onderwijs (IVHO)
Opsteller	Leo Harskamp
Datum eerste versie	7 april 2025
Versie	1.0
Status	Definitief
Citeertitel	Harskamp, L. J. T. (4 april 2025). <i>Handreiking beveiliging – voor bijeenkomsten in het Hoger Onderwijs</i> . Integrale Veiligheid Hoger Onderwijs (IVHO)
Bijdragen gevraagd aan	Leden bestuur IV-community Leden IV-community Contactpersonen VH en UNL PBNU (platform beveiliging NL universiteiten) Platform Veiligheid & Beveiliging HBO Deskundigen in enkele instellingen Deskundigen in Particuliere Beveiligingsorganisaties (PBO)

INHOUDSOPGAVE

Handreiking beveiliging	1
1. Aanleiding en doelstelling	3
2. Uitgangspunten, verantwoordelijkheden en bevoegdheden	4
3. Informatie en veiligheid	5
4. Werkwijze.....	6
5. Scenariodenken.....	6
6. Instrumenten / maatregelen.....	7
7. Samenwerking met de politie.....	9
8. Fasen	10
9. Slotopmerkingen.....	10
Bijlage 1. Aanbevelingen bij het gebruik van deze handreiking.....	11
Bijlage 2. Stappenplan.....	12
1. Voorbereiding & risicoanalyse	12
2. Beveiligingsstrategie & besluitvorming.....	12
3. Operationele uitvoering	12
4. Nazorg & evaluatie	12
Bijlage 3. Raamwerk operatieplan (NATO standard order)	13
Bijlage 4. Raamwerk operatieplan (5WH).....	14

1. Aanleiding en doelstelling

In 2024 is de handreiking 'Governance en inrichting van integrale veiligheid'¹ gepubliceerd. Eerder in datzelfde jaar is vanuit de koepelorganisaties Vereniging Hogescholen (VH) en Universiteiten van Nederland (UNL) de richtlijn 'Protesten'² gepresenteerd. De handreiking die nu voor u ligt, biedt een uitwerking van het thema **beveiliging bij bijeenkomsten**. Deze kan ook gebruikt worden voor protesten maar is breder opgezet.

Na de handreiking 'controversiële sprekers'³ in maart 2020, heeft de ontwikkeling van handreikingen binnen het Platform Integrale Veiligheid Hoger Onderwijs (IVHO) niet stilgestaan. De subsidieperiode van het platform door OCW is eind december 2023 beëindigd en vanaf 2024 ondersteunt de hoger onderwijssector zelf het platform en de community van Integrale Veiligheidsadviseurs van zelf, structureel ondergebracht bij SURF. Platform IVHO ondersteunt de leden met actuele bijdragen, gebaseerd op praktijkervaringen in instellingen.

Tot het opstellen van deze handreiking is besloten naar aanleiding van recente protesten en verstoringen bij sprekers, debatten en overige bijeenkomsten. Onder het begrip 'bijeenkomst' wordt in deze handreiking verstaan: alle soorten samenkomsten, variërend van lezingen en debatten tot conferenties en evenementen van studieverenigingen. De handreiking richt zich op de voorbereiding en uitvoering van beveiligingsmaatregelen. Of het nu gaat om een bezoek van de minister-president of een kleinschalige bijeenkomst van een studievereniging: de structuur van de voorbereiding is vergelijkbaar. Wat telt, zijn de voorbereidingen die in alle gevallen genomen kunnen worden en bijdragen aan een betere beheersing van risico's. Er bestaan diverse methodieken voor risicoanalyse⁴ die voor dit onderwerp vaak prima toepasbaar zijn.

Wij willen instellingen helpen bij het vinden van een balans tussen academische vrijheid, vrijheid van meningsuiting, de veiligheid van studenten, medewerkers en bezoekers, en de naleving van wet- en regelgeving zoals de zorgplicht. Veel principes uit deze handreiking zijn ook bruikbaar voor gebouwbeveiliging buiten bijeenkomsten. Sommige instellingen hanteren al dagelijkse toegangscontroles, wat bij bijeenkomsten een voordeel kan zijn doordat deze controles al ingeburgerd zijn. Kern van toegangscontrole is het buitenhouden van ongewenste elementen.

De handreiking biedt houvast aan bestuurders en veiligheidsmedewerkers, geeft inzicht aan andere betrokkenen en draagt bij aan een professionele invulling van beveiligingsverantwoordelijkheden. Dit laat onverlet dat ook andere partijen binnen en buiten de instelling verantwoordelijkheden dragen, zoals organisatoren, lokale overheden en beveiligingsdiensten.

Deze productie is gemaakt door de veiligheidsadviseurs binnen IVHO, en besproken met hoogleraren, docenten en beveiligingsexperts uit zowel de publieke als particuliere sector. We wensen u succes bij het gebruik.

Het bestuur van de IV-community,
Marieke de Boer en Leo Harskamp

¹ <https://integraalveilig-ho.nl/wp-content/uploads/Handreiking-Governance-van-Integrale-Veiligheid-.pdf>

² https://www.universiteitenvannederland.nl/files/publications/Richtlijn%20protesten%20%20UNL%20%26%20VH_2.pdf

³ <https://integraalveilig-ho.nl/wp-content/uploads/Handreiking-controversi%C3%ABle-spreker-hoger-onderwijs-IV-HO.pdf>

⁴ <https://www.naris.com/nl/10-risicomanagement-modellen-die-je-moet-kennen/>

2. Uitgangspunten, verantwoordelijkheden en bevoegdheden

- Het CvB van de instelling is eindverantwoordelijk voor de veiligheid tijdens bijeenkomsten die zijn georganiseerd door of uit naam, of op het terrein van de instelling, ongeacht waar deze bijeenkomst plaatsvindt;
- Niemand kan de primaire verantwoordelijkheid van de instelling overnemen;
- In gevallen bij wet geregeld overtreft de bevoegdheid van de Burgemeester die van het College van Bestuur, zonder diens verantwoordelijkheden over te nemen;
- In het publieke domein vormen het Openbaar Ministerie en het lokaal bestuur (Burgemeester) het gezag en zijn belangrijke samenwerkingspartners, net als de politie;
- Het invullen van beveiligingsverantwoordelijkheid kan niet zonder ambtenaren van de gemeente, veelal de ambtenaren openbare orde en veiligheid (OOV) en van de politie;
- Beveiliging vindt plaats volgens het principe van de ui: om de kern liggen ringen die als bescherming dienen voor die kern. Een datacenter zet men niet midden op straat, maar pleegt men diep in een gebouw te plaatsen, met diverse ringen van beveiliging daar omheen. Elke beveiligingsmaatregel ondersteunt de andere, zodat een optelsom van maatregelen ontstaat. Zo werkt het ook met (gevoelige) bijeenkomsten;
- Het CvB is bekend met de eigen verantwoordelijkheden, zoals de zorgplicht medewerkers (Arbowet) en de benodigde zorg voor studenten en derden zoals vastgelegd in de WHW, diverse regelingen en de code goed bestuur;
- De veiligheidsverantwoordelijke en de organisator weten hoe de bevoegdheden en mandaten zijn verdeeld zodat niemand op cruciale momenten hoeft te twijfelen. Van de organisator van de bijeenkomst wordt maximale openheid verwacht, terwijl de instelling verantwoordelijk is en blijft voor de uitvoering. Sommige taken worden door de organisator vervuld, maar altijd na vaststelling van de risicoanalyse, de maatregelen en verkregen toestemming. Toestemming voor het houden van een evenement hangt vooral af van de mogelijkheid tot het maken van duidelijke afspraken vooraf;
- Vanuit het eigenaarschap van een gebouw is de eigenaar of rechthebbende bevoegd om voorwaarden te stellen aan de toegang en kan mensen aanwijzen om in dat kader taken uit te voeren, dit geldt ook voor door de instelling gehuurde ruimte of gebouwen;
- Als een bijeenkomst op andermans grondgebied, in andermans ruimte plaatsheeft, dienen afspraken te zijn gemaakt over mandatering. Huurder en verhuurder maken duidelijke afspraken over de verantwoordelijkheden voor beveiliging;
- Aangewezen functionarissen zijn bevoegd tot alles waar de eigenaar/rechthebbende, doorgaans het CvB, hen voor aanwijst, zoals bijvoorbeeld:
 - Controleren identiteit
 - Vastleggen bezoekersgegevens
 - Controleren van tassen
 - Visiteren van bezoekers
 - Geven van aanwijzingen
 - Ontzeggen van de toegang of beëindigen van bestaande toegang
- Bezoekers, of zij nu medewerkers, studenten of externen zijn, zijn niet verplicht om bij aankomst aan de eerste beveiligingsmaatregelen mee te werken. Omgekeerd is de instelling dan niet verplicht de persoon toe te laten. De persoon die al binnen is, moet zich wel houden aan de huisregels, waarin onder meer is opgenomen de plicht om aanwijzingen op te volgen;
- Conform de huisregels die de meeste instellingen hebben vastgesteld en aanbevolen worden om die op te stellen, moeten alle aanwezigen de aanwijzingen van functionarissen daartoe aangesteld, opvolgen. Het niet opvolgen van aanwijzingen kan reden zijn om een

persoon niet toe te laten of de inmiddels verkregen toegang ongedaan te maken. Het niet opvolgen van een vordering om te vertrekken is een misdrijf onder artikelen 138 en 138a Wetboek van Strafrecht (lokaalvredebreuk). Zelfs als de politie daar niet direct op acteert, geeft dat de instelling het recht om betrokkene voortaan niet meer toe te laten, bijvoorbeeld tot duidelijke afspraken met betrokkene kunnen worden gemaakt over het gedrag;

- Een CvB geeft haar veiligheidsmedewerkers rugdekking en zorgt dat beveiligers op basis van de eerder gemaakte afspraken kunnen, mogen en durven ingrijpen. Een beveiligers die bang is voor de consequenties van ingrijpen kan de door (namens) het CvB gemaakte afspraken niet professioneel handhaven. De veiligheidsverantwoordelijke stelt vooraf zeker dat deze bestuurlijke rugdekking er is. Rugdekking betekent ook dat wordt opgetreden als de beveiligers kwalijk worden behandeld.

3. Informatie en veiligheid

- Een onderschat aspect is het belang van het samenspel tussen veiligheid en informatie. Om een goede risicoanalyse te kunnen doen is een informatiepositie over eventuele op handen zijnde dreigingen en risico's erg belangrijk. Input voor een risicoanalyse is niet alleen informatie over mogelijk toekomstige risico's, maar vooral ook incidenten die zich in de eigen instelling en vergelijkbare omgevingen al eerder voordeden;
- Er is een eenheid nodig die de instelling voorziet van **informatie** over (mogelijk) op handen zijnde dreigingen en risico's. Dit laat onverlet ieders verantwoordelijkheid, in het bijzonder die van de organisator om op mogelijke risico's en dreigingen te anticiperen.
- Er is een deskundige nodig voor het doen van **risicoanalyses** en voor het doen van voorstellen voor en het uitvoeren van **beveiligingsmaatregelen**;
- In sommige grotere instellingen worden deze twee gecombineerd in een afdeling Integrale Veiligheid, maar soms is een separate beveiligingsafdeling ingericht. Die beiden werken samen om maximaal effectief te kunnen zijn. Idealiter stuurt de afdeling of functionaris Integrale Veiligheid (IV-er) de afdeling beveiliging functioneel aan: de IV-er heeft voeling met de bestuurlijke intentie en escalatiemogelijkheid en de afdeling beveiliging geeft aan die intentie vorm en inhoud. In de instellingen waar deze afdelingen in het geheel niet ingericht zijn, moeten de taken over de bestaande functionarissen verdeeld worden, taken en rollen blijven immers dezelfde.

Voor kleine organisaties die niet over bovenstaande structuur beschikken, is het nog niet eenvoudig om dergelijke afwegingen en organisatorische stappen goed te kunnen nemen. In sommige gevallen is clustering gekozen als oplossing om schaarse capaciteiten gezamenlijk in te richten. In andere gevallen worden taken ingehuurd bij een marktpartij of collega instelling.

4. Werkwijze

De instelling legt in haar interne procedures vast hoe bijeenkomsten tot stand komen. Zodra duidelijk is dat een bijeenkomst plaatsvindt die veiligheidsrisico's kan meebrengen, start de samenwerking tussen de organisator en de veiligheidsverantwoordelijke. De risicoanalyse is leidend en wordt opgesteld op basis van beschikbare informatie over het onderwerp, de sprekers, deelnemers en eventuele actiegroepen.

De veiligheidsverantwoordelijke adviseert vooraf over passende beveiligingsmaatregelen. Dit kan leiden tot wijziging, verplaatsing of annulering van de bijeenkomst. Afstemming vindt plaats met betrokkenen zoals gemeente, politie en – indien van toepassing – de beveiliging van sprekers of hoogwaardigheidsbekleders. Ook inzet van OSINT-teams en proactieve observatie kunnen deel uitmaken van de voorbereiding.

Het stappenplan in bijlage 2 biedt een praktisch overzicht van de noodzakelijke fasen en acties.

5. Scenariodenken

Scenariodenken is een gestructureerde methode om mogelijke dreigingen en verstoringen vooraf in kaart te brengen en beheersmaatregelen te ontwikkelen. Door verschillende scenario's – van verstoringen door activisme tot fysieke dreiging – te analyseren, kunnen beveiligingsmaatregelen doelgericht en proportioneel worden ingezet. Dit verhoogt de weerbaarheid en zorgt voor een soepele voorbereiding, waardoor incidenten beter beheersbaar zijn, omdat het handelingsperspectief hierop reeds bekend is. Scenariodenken helpt bij het verdelen van middelen, trainen van personeel en verminderen van verrassingen. Bij gevoelige bijeenkomsten draagt scenariodenken bij aan risicobeheersing en de-escalatie, wat essentieel is voor een veilig en ordelijk verloop zonder onnodige verstoringen. Een bijkomend voordeel van scenariodenken voor bestuurders is dat zij zijn voorbereid op het ergste. Dit bevordert besluitvorming op cruciale momenten.

Vaak wordt gebruikgemaakt van drie of vier uitgewerkte scenario's. In diverse instellingen is sprake van de volgende drie scenario's:

1. Scenario 1 'zoals gepland'

In dit scenario gaat de bijeenkomst volgens plan. Dit is tevens het te bereiken scenario als 2 of 3 in werking treden;

2. Scenario 2 'geringe verstoring'

In scenario 2 is een verstoring die uiteindelijk de voortgang van de bijeenkomst niet belemmert. Het is even lastig, er is heel even overlast, maar na enig geduld of na enig ingrijpen is de situatie terug bij scenario 1. Scenario 2 is het moeilijkste scenario, omdat met afgestemd optreden moet worden bereikt dat we teruggaan naar 1 in plaats van verder door te escaleren naar scenario 3.

3. Scenario 3 'grote verstoring'

Dit is het scenario waarin de bijeenkomst geen voortgang kan vinden. Dit is ook het scenario dat we graag willen voorkomen. In de fase dat het zich voordoet, moeten er plannen klaarliggen voor een veilige aftocht. In deze fase is het te laat om nog te corrigeren. De preventieve maatregelen om dit scenario te voorkomen liggen, zoals het woord 'preventief' al aangeeft: aan de voorkant. In de preparatie moet een zo gunstig mogelijk arrangement worden gekozen of gecreeerd zodat externen (of internen) niet dit effect kunnen hebben op de bijeenkomst.

Het is primair de organisator die bepaalt welk scenario op welk moment van toepassing is. Bij bijeenkomsten vanuit de instelling is dit veelal een persoon in een leidinggevende positie, ondersteund en geadviseerd door de veiligheidsverantwoordelijke. Bij bijeenkomsten georganiseerd door studenten zal de veiligheidsverantwoordelijke hierin

een steviger rol moeten pakken en de organisator 'aan de hand meenemen'. Immers, de instelling blijft verantwoordelijk voor de veiligheid en die verantwoordelijkheid is niet overdraagbaar.

Wel kunnen externen in sommige gevallen invloed hebben: als de Burgemeester, bijvoorbeeld op basis van de WOM, aanwijzingen geeft, dienen deze aanwijzingen opgevolgd te worden.

6. Instrumenten / maatregelen

Elke veiligheidsverantwoordelijke heeft een reeks aan instrumenten die kunnen worden ingezet om een bijeenkomst veilig te laten verlopen. Deze instrumenten kunnen op zichzelf of in combinatie groot positief effect hebben op bijeenkomsten. Een aantal van deze instrumenten zijn:

- **De inzet van gekwalificeerd beveiligingspersoneel**
Beveiligers hebben instructie nodig. De veiligheidsverantwoordelijke dient ervoor te zorgen dat de instructies helder zijn. Niet alleen moeten instructies worden beschreven voor het gewenste scenario, maar ook voor de scenario's van escalatie en eventueel afbreken of ontruimen.
- **Toegang reguleren**
Alleen toegang verlenen aan eigen medewerkers en studenten. Externen hebben veel minder een band met de instelling en dragen niet zelden bij aan escalatie, maar kunnen vervolgens veel moeilijker gepakt aangesproken en gecorrigeerd worden. Reden om bij eventuele dreiging de categorie externen niet of uitsluitend op persoonlijke uitnodiging toe te laten.
- **Bezoekersregistratie**
Voorafgaande registratie dient twee doelen:
 1. Organisator en instelling weten wie op het evenement afkomen;
 2. Kwaadwillende bezoekers worden afgeschrikt, want door registratie worden zij uit de anonimiteit gehaald.Technologische vooruitgang helpt, sommige instellingen werken met een QR-code systeem ter bescherming van de privacy van bezoekers. Doorgaans hoeft iemand die een QR-code heeft, niet ook nog een legitimatiebewijs te laten zien. In bijzondere gevallen kan daar overigens wel naar worden gevraagd;
- **Toegangscontrole**
Toegangscontrole kan op meerdere punten tegelijkertijd worden ingezet. Meest laagdrempelig is het als deze plaatsvindt bij de ingang van de zaal waarin de bijeenkomst plaatsheeft. Alle anderen in een gebouw worden dan niet getroffen door de 'overlast' die een bijeenkomst met zich meebrengt.
Een andere mogelijkheid is om de toegangscontrole behalve bij de zaal ook bij de hoofdentree van een compartiment, complex of gebouw uit te voeren. Dan is niet alleen de zaal gecontroleerd op legale aanwezigheid, maar ook de omgeving;
- **Het achterlaten van jassen en tassen**
Een ander instrument is het al dan niet toelaten van tassen en jassen in de zaal. Door het achterlaten van jassen en tassen is het voor het beveiligingspersoneel eenvoudiger om overzicht te houden. Laptops of schrijfmateriaal en een flesje water worden uiteraard

toegelaten. Alles wat men achterlaat hoeft bovendien niet te worden gecontroleerd. Dit is een maatregel die vaak verlangd wordt bij bezoeken van hoofden van staat.

- **Communicatie**

Communicatie is een van de meest invloedrijke instrumenten. De instelling kan in haar communicatie duidelijkheid geven over gewenst gedrag, over consequenties bij ongewenst gedrag en meer specifiek rond bijeenkomsten kan communicatie helderheid geven over afspraken en voorwaarden om deel te kunnen nemen. Ook kunnen intern betrokkenen door communicatie worden gewaarschuwd voor wat zich in hun gebouw kan voordoen;

- **Briefings**

Tijdens het voorbereidingstraject worden betrokkenen bijgepraat over de ontwikkelingen en de voorbereidingen;

Direct voorafgaand aan de bijeenkomst worden alle betrokkenen, zoals de beveiligers, facilitair medewerkers en hosts gebriefd in bijzijn van de organisator en eventuele andere betrokkenen zoals geluids- en cameramensen, moderators etc.

- **Beveiligingsmindset**

Een sterke beveiligingsmindset draait om meer dan alleen protocollen; het is een houding van waakzaamheid, verantwoordelijkheid en de bereidheid in te grijpen waar nodig. Het betekent risico's herkennen voordat het escaleert, orde handhaven, kleine dingen klein houden en standvastig blijven in moeilijke situaties. Beveiliging vereist niet alleen scherpste, maar ook morele moed en tactisch inzicht. Die inzet wordt niet altijd standaard geleverd als in een aanbesteding de laagst biedende partij wordt gecontracteerd.

- **Maak gebruik van gebouw, terrein of hindernis**

Een bijeenkomst die van buiten zichtbaar is, kan verstoord worden van buitenaf. Gebouwen bieden allerlei mogelijkheden om bijeenkomsten dieper in dat gebouw te laten plaatsvinden, zodat er omheen ringen kunnen worden gemaakt, al naar gelang het risico van de bijeenkomst. Het te beveiligen gebied of object dient zo klein mogelijk te worden gekozen om efficiënt te kunne beveiligen en om de impact op (andere) primaire processen zoveel mogelijk te voorkomen.

- **Cameratoezicht**

Camera's, inclusief bodycams, kunnen een toevoeging zijn aan een beveiligingsplan. Beveiligingsmedewerkers kunnen niet op elke plaats tegelijk zijn. Ook kunnen camerabeelden achteraf worden gebruikt om de toedracht van incidenten te onderzoeken. Van belang is dat de instelling ervoor zorgt dat het camerabeleid voldoet aan de eisen die de Algemene verordening gegevensbescherming (AVG) daaraan stelt.

- **Misleiding**

Als verstoring verwacht wordt, bestaat de mogelijkheid om de aanvangstijd iets eerder te stellen dan de daadwerkelijke aanvangstijd en na aankomst de gewenste bezoekers naar een andere locatie over te (laten) brengen, waarna zij nog op tijd zijn om de bijeenkomst (op die andere locatie) bij te wonen.

- **Verplaatsen – van locatie wisselen**

Als een evenement verstoord wordt (scenario 2 of 3), is het veelal mogelijk waar te nemen (eventueel vast te leggen) welke deelnemers verantwoordelijk zijn voor de verstoring. Vervolgens kan het evenement in een andere ruimte voortgezet worden, waarbij de deelnemers die het oorspronkelijke evenement verstoord hebben, worden geweigerd. Uiteraard door de alternatieve ruimte te voorzien van toegangscontrole.

7. Samenwerking met de politie

- **Relatie**

Een veiligheidsverantwoordelijke onderhoudt een netwerk. Onderdeel daarvan is de politie in de eenheid / gemeente waar de instelling gevestigd is. Goed stakeholdermanagement werkt op tijd aan relaties, zodat op cruciale momenten, zoals bij een verhoogd risicobeeld of incident, er al samenwerkingsrelaties bestaan en bekend is wie waarvoor aan beide zijden verantwoordelijk is;

- **Verantwoordelijkheid**

De politie kan door het gezag worden ingezet, soms zelfs in de instelling, maar het is de instelling die verantwoordelijk is voor veiligheid. Veiligheidspartners als de politie werken graag samen met bedrijven en instellingen die hun zaakjes op orde hebben: politiemensen herkennen het als er wordt gewerkt op basis van risicomanagement en scenariodenken, dit is wat zij immers dagelijks doen. Hoewel de instellingen geen veiligheidsorganisaties zijn, moeten er in de instelling enkelen zijn die deze taal spreken. Behoorlijke voorbereiding op (gevoelige) bijeenkomsten is anders niet mogelijk;

- **Escalatie**

De politie heeft taken rond onze bijeenkomsten, maar dat is niet het enige dat zij doen. De hoofdtaken van de politie zijn beschreven in de Politiewet 2012. Zodra strafbare feiten worden gepleegd of mensen moeten worden geholpen kan de politie worden ingezet. Soms zal de politie uit de aard van de eigen preparatie (deels) opschalen en zijn zij al in de omgeving van een bijeenkomst aanwezig. Echter, als zij niet zijn meegenomen in de voorbereidingen, kunnen instellingen niet verwachten dat binnen een uur ingrijpende inzetten worden gedaan. Ook de politie heeft gezags- en commandostructuren. Hoofdzaak bij escalatie is daarom: mogelijke escalatie moet worden voorbereid met de politie. Een belangrijke vraag die de instelling zelf zowel als de stakeholders daarbij kan helpen:

- o Welke tolerantiegrenzen kent de instelling?

- De politie heeft die informatie nodig, want ook zij monitoren informatiekanalen. Soms ziet de politie dingen die wij niet kunnen zien. Het is voor de politie van belang te weten tot hoever wij het willen laten komen om de noodzaak van het eigen optreden te kunnen inschatten en voorbereiden.

8. Fasen

We onderscheiden de volgende fasen, gebaseerd op de PDCA-cyclus:

1. De voorbereiding. Deze fase start bij de eerste kenbare intentie om een (gevoelige) bijeenkomst te houden;
2. De risicoanalyse. Deze fase is een doorlopende activiteit van het verzamelen en analyseren van risico's;
3. De adviesfase. In deze fase worden op basis van de risicoanalyse adviezen voorgelegd aan het gezag;
4. De besluitvorming. In de besluitvormingsfase geeft het gezag de richting aan en worden besluiten genomen. In het geval dat wordt gewerkt met een protocol, worden eerder genomen besluiten opgevolgd die zijn vastgelegd in dit protocol;
5. De operationele fase. Deze fase omvat alle facetten van de uitvoering, niet alleen de maatregelen, maar ook het monitoren en het evt. aanpassen van de plannen op basis van ontwikkelingen, het veiligstellen van eventueel bewijs, het doen of plannen van aangifte en het begeleiden van degene die aangifte doet en het eventueel voeren van gesprekken met overtreders en opleggen van sancties, wat wordt gedaan door de verantwoordelijke voor de bijeenkomst, bijvoorbeeld de opleiding;
6. De nazorgfase. In deze fase wordt geëvalueerd, worden lessen getrokken, plannen bijgesteld en nazorg of hulp verleend als daaraan behoefte is.

9. Slotopmerkingen

De veiligheidsverantwoordelijke, veelal de functionaris met de rol van IV-er (adviseur integrale veiligheid), is degene die het bovenstaande dient te beheersen. Hij of zij kan de omstandigheden zodanig lezen dat een passend beveiligingsontwerp wordt gemaakt. De kracht hiervan is gelegen in de goede voorbereiding.

Dit is in het belang van onze medewerkers, studenten en bezoekers. Sommigen van hen voelen zich niet elke dag veilig genoeg om naar de campus te gaan of zich uit te spreken. Reden voor het platform IV-HO om deze handreiking op te stellen.

Bildungsman Alexander von Humboldt: 'zonder veiligheid geen vrijheid'. Wij voegen daar in onze context aan toe: zonder veiligheid ook geen openheid of academische vrijheid. Voor de mooiste dingen in het hoger onderwijs is eerst en vooral enig niveau van veiligheid nodig.

Bijlage 1. Aanbevelingen bij het gebruik van deze handreiking

- Voorzie in een leertraject, cursus of webinar voor bestuurders, veiligheidspersoneel en andere betrokkenen: 'de basis van beveiliging'. Een goed voorbeeld van een opleiding voor veiligheidsverantwoordelijken in dit kader is de post-HBO opleiding Security & Recht⁵;
- Beleg informele bijeenkomsten met ketenpartners en geef elkaar inzicht in de eigen processen, besluitvormingsprocedures en belangen;
- Kies de bij de instelling passende methode uit de bijlagen. Sommigen willen werken met een stappenplan of checklist, anderen vullen het liefst een raamwerk in. In crisisomgevingen wordt vaak gebruik gemaakt van de 'nato standard order', in politieomgevingen wordt het 5WH (5 wat / hoe) model gebruikt. Elke methode die leidt tot overzicht is goed;
- Leg de verbinding met crisismanagement. In geval van verstoring is er ergens een moment dat mogelijk de crisisstructuur in werking treedt. Hoe meer ervaring wordt opgedaan hoe minder snel naar een crisisstructuur hoeft te worden geschakeld;
- Wissel in het ambtelijk netwerk Integrale Veiligheid van UNL of in de IV-community van het Platform of in kleiner verband casussen met elkaar uit ter lering en verbetering.

⁵ <https://www.soba.nl/opleidingen/post-hbo-en-management/post-hbo-registeropleiding-security-en-recht>

Bijlage 2. Stappenplan

1. Voorbereiding & risicoanalyse

- Identificeer de bijeenkomst: Bepaal het type bijeenkomst en de gevoeligheid van aanwezigen (bijvoorbeeld controversiële spreker, maatschappelijk thema, politieke lading).
- Dreigingsanalyse: Verzamel informatie over potentiële risico's via OSINT (open source intelligence), eerdere incidenten, openbare bronnen en overleg met interne en externe partners (zoals politie, gemeente, OOV).
- Stakeholdermanagement: Betrek het College van Bestuur (of mandaatdrager), afdeling Integrale Veiligheid, politie, OOV-functionarissen en andere relevante actoren.
- Scenariodenken: Werk met drie standaardscenario's (normale voortgang, geringe verstoring, grote verstoring) en bepaal de tolerantiegrenzen.
- Besluitvorming over opzet: De veiligheidsverantwoordelijke kan adviseren over verplaatsing, aanpassing of annulering indien veiligheid niet kan worden gegarandeerd.

2. Beveiligingsstrategie & besluitvorming

- Selecteer maatregelen en instrumenten: Stel een maatregelpakket op, op basis van de risicoanalyse, zie hoofdstuk 6 'Instrumenten'.
- Voorzie in alternatieven: Denk vooruit over noodmaatregelen en verplaatsingsopties bij escalatie (zoals locatie wisselen).
- Beveiligingslagen (Ui-model): Ontwerp meerdere controlelagen rond de kernactiviteit, met oplopende en elkaar versterkende maatregelen.
- Formalisatie: Leg maatregelen vast in een beveiligingsplan en stem dit af met het bestuurlijk gezag (mandaat of formele besluitvorming).

3. Operationele uitvoering

- Briefing en instructie: Informeer beveiligers, facilitair personeel, hosts en andere betrokkenen over hun rol en instructies.
- Actieve monitoring: Beveiligingspersoneel voert zowel statische als mobiele observaties uit in en rond de locatie.
- OSINT-monitoring: Zet een (tijdelijk) OSINT-team in dat vooraf en tijdens het evenement open bronnen monitort op signalen van mogelijke verstoring of escalatie.
- Bijstelling maatregelen: Gebruik informatie van fysieke en digitale observaties om maatregelen indien nodig bij te stellen tijdens de bijeenkomst.
- Escalatievoorbereiding: Stem vooraf af met politie over mogelijke inzet, escalatiescenario's en communicatielijnen.

4. Nazorg & evaluatie

- Incidentrapportage: Documenteer verstoringen, genomen maatregelen, eventuele escalatie en handhaving.
- Evaluatie met stakeholders: Evalueer met betrokkenen de uitvoering en identificeer verbeterpunten.
- Opvolging en nazorg: Spreek indien nodig deelnemers aan, doe aangifte, biedt nazorg aan betrokkenen (inclusief personeel en studenten).
- Herziening & training: Werk protocollen bij op basis van leerpunten en zorg voor herhaalde training en opleiding van betrokken functionarissen.

Bijlage 3. Raamwerk operatieplan (NATO standard order)

Dit format wordt in militaire en crisisomgevingen gebruikt om op gestructureerde wijze een operatiebevel vorm te geven. Een volledig ingevuld raamwerk behelst alle relevante aspecten.

1. Situatie analyse

Dreigingen & risico's: Potentiële verstoringen zoals protesten, fysieke dreiging, cyberdreiging.
 Omgevingsfactoren: Locatie, publiek, externe factoren zoals demonstraties.
 Stakeholders: CvB, politie, gemeente, OOV, beveiligingsteams, organisator.

2. Opdracht

Veilig organiseren van bijeenkomst [...]:
 Veiligheid van alle deelnemers.
 Zorgen voor een evenwicht tussen toegankelijke deelname en beveiligingsmaatregelen.
 Voorkomen van escalatie in geval van incidenten.

3. Uitvoering

Operatieconcept:
 Beschrijf instrumenten en maatregelen zoals toegangscontrole, bezoekersregistratie – zie hoofdstuk 6 'instrumenten'.
 Scenarioplanning (normale voortgang, geringe verstoring, grote verstoring).
 Beveiligingslagen (Ui-model: buitenring, tussenring, kernbescherming).
 Samenwerking met politie en noodplan voor escalaties.

Taken en verantwoordelijkheden:

CvB:	Besluitvorming / toezicht
Organisator	Het evenement zoveel mogelijk uitvoeren als afgesproken
Veiligheidsverantw:	Geeft leiding aan het proces van risicoanalyse en uitvoering
Beveiligingscoördinator:	Coördineert inzet beveiligingsmaatregelen en escalatie
Beveiligers	Uitvoering van instrumenten / maatregelen
Communicatieteam:	Zorgt voor informatievoorziening en coördinatie met externe partijen
OSINT-team:	Monitort vooraf en tijdens de bijeenkomst op verstoringindicatoren

4. Logistiek & middelen

Fysieke middelen: Camera's, toegangsbarrières, bezoekersregistratiesystemen
 Personele inzet: Gekwalificeerde beveiligers, crisiscoördinator, communicatiemedewerker
 Externe ondersteuning: Politie, OOV-functionaris gemeente, adviseur burgemeester

5. Commandovoering & communicatie

Commandostructuur:
 CvB → Veiligheidsverantwoordelijke → Coördinator Beveiliging → Beveiligingsteam.

Communicatie en verbindingen:

Communicatielijnen tussen intern en extern betrokkenen.

Bijlage 4. Raamwerk operatieplan (5WH)

Dit format wordt in diverse omgevingen gebruikt om een operatie uit te werken. Een volledig ingevuld raamwerk behelst alle relevante aspecten.

Vraag	Antwoord (voorbeeld)
Wie	CvB (eindverantwoordelijk), Integrale Veiligheid, Beveiligingscoördinator, politie, OOV-functionaris, beveiligers, facilitair personeel, communicatieteam.
Wat	Beveiligingsmaatregelen om bijeenkomsten veilig te laten verlopen, incl. toegangscontrole, scenarioplanning, OSINT-monitoring en crisisbeheersing.
Waar	Op locatie van de bijeenkomst (zaal, campus, externe locaties). Meerdere beveiligingsringen om kerngebied te beschermen.
Wanneer	Vanaf de eerste plannen van de bijeenkomst tot en met de evaluatiefase na afloop.
Waarom	Om escalaties te voorkomen, academische vrijheid te waarborgen en deelnemers veilig te houden.
Hoe	Via risicobeoordeling, scenarioplanning, inzet van beveiligingsteams, samenwerking met politie en crisisplannen voor escalatie.