INTEGRALE BEDRIJFSNOODORGANISATIE VU CAMPUS

UITGANGSPUNTEN, OPSCHALINGSPRINCIPES EN WERKWIJZE

VU VRIJE UNIVERSITEIT AMSTERDAM

IS VERDER KIJKEN

LEESWIJZER

Het voorliggende stuk Integrale Bedrijfsnoodorganisatie (iBNO) VU Campus is een rompdocument waarin uitgangspunten, opschalingsprincipes en werkwijze beschreven worden. Samen met de noodplannen van de eenheden vormt dit rompdocument het Bedrijfsnoodplan VU.

De beschreven uitgangspunten, opschalingsprincipes en werkwijze sluiten aan bij de aanpak van het Programma Integrale Veiligheid in het Hoger Onderwijs.

COLOFON
De Integrale bedrijfsnoodhulporganisatie VU Campus is een uitgave van de Vrije Universiteit

Uitgave 2018
Auteurs VU-brede projectgroep Integrale Bedrijfsnoodorganisatie
Vormgeving Haagsblauw
Beelden
Yvonne Compier, Caren Huygelen, Peter Valckx, Too van Velzen
Projectnummer 2044929

INHOUDSOPGAVE

1 INLEIDING

1. INLEIDING

Als maatschappelijk betrokken instelling, volgt de VU nauwgezet de veranderingen in de wereld en in de directe omgeving van de universiteit. Niet alleen vanuit de kernactiviteiten onderzoek, onderwijs en maatschappelijke dienstverlening, maar ook voor wat deze ontwikkelingen betekenen voor de organisatie en haar kernwaarden. Maatschappelijke en technologische ontwikkelingen hebben direct invloed op de situatie van de VU. Nieuwe ontwikkelingen bieden kansen maar ook risico's. Door het open karakter van de VU is de organisatie in belangrijke mate een 'spiegel van de samenleving'. De VU is als organisatie dan ook zeker niet immuun voor veranderingen in risico's en risicoperceptie.

Recent zijn door de TU Delft, in opdracht van de VSNU, de trends in kaart gebracht die invloed hebben op de universitaire campus[1]. Dit zijn (1) globalisatie en internationalisering, (2) diversiteit en demografie, (3) de sneller veranderende context, (4) de samenwerking buiten de universiteit, (5) de veranderende werkomgeving, (6) digitalisering, (7) verschuiving in financiering en (8) onderwijs- en onderzoeksvernieuwing.

Een groot aantal van deze trends hebben ook impact op de veiligheidssituatie op de universitaire campus: toenemende digitalisering bijvoorbeeld heeft geleid tot een sterk vergrote aandacht voor informatieveiligheid.

[1] Campus NL. Investeren in de toekomst. TUDelft 2016

Naast deze (internationale) trends zijn er ook een aantal kenmerken die specifiek zijn voor de VU en invloed hebben op de integrale veiligheid op de campus:

- Het open karakter van de universiteit;
- De omvang en diversiteit van de medewerkers- en studentenpopulatie;
- Snelle wisselingen in de populatie door kortdurende betrokkenheid;
- De grootstedelijke omgeving van de Zuidas waarin de Campus zich bevindt;
- Het internationale karakter en werkveld van onze academische gemeenschap;
- De digitalisering van werkwijzen en informatie;
- Het belang van academische vrijheid en autonomie;
- De verscheidenheid aan wetenschappelijke disciplines en werkzaamheden;
- De diversiteit aan disciplines en functies van – en binnen – de gebouwen op de Campus;
- De innovatieve aard van het wetenschappelijke onderzoek dat wordt verricht;
- Het bewust werken met een grote verscheidenheid aan gevaarlijke stoffen en onder risicovolle condities;
- De toenemende integratie op de campus met andere (publieke) activiteiten zoals wonen, sporten en winkels.

Bovenstaande trends hebben samen met de specifieke VU-kenmerken geleid tot de Veiligheidsvisie VU, die kaderstellend is voor de uitgangspunten en opschalingsprincipes van de integrale bedrijfsnoodorganisatie. De Veiligheidsvisie sluit aan bij het Programma Integrale Veiligheid Hoger Onderwijs.

Op de VU Campus onderscheiden we drie veiligheidsdomeinen: informatieveiligheid, sociale veiligheid en fysieke veiligheid. Binnen deze domeinen wordt in de lijnorganisatie actief gewerkt aan het voorkomen van veiligheidsrisico's. Steeds meer wordt er daarbij ook domeinoverstijgend gewerkt, bijvoorbeeld als het gaat om (preventie van) datalekken of ongewenst gedrag.

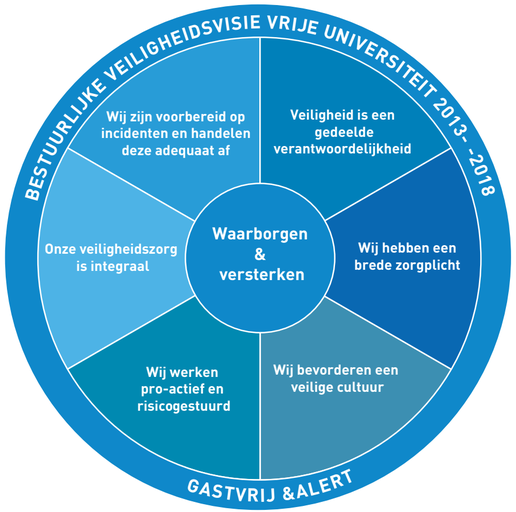
Het integraal benaderen van situaties die inbreuk maken op de normale bedrijfsvoering is de basis van de integrale bedrijfsnoodorganisatie.

2 VEILIGHEIDSVISIE

2. VEILIGHEIDSVISIE

In december 2013 is door het College van Bestuur (CvB) VU de Veiligheidsvisie Vrije Universiteit Amsterdam vastgesteld. Deze visie is kaderstellend en biedt richtlijnen, waarbinnen faculteiten, diensten en andere betrokkenen zelf afwegingen over veiligheid kunnen maken.

Figuur 1. Richtinggevende principes Veiligheidsvisie VU



Bij de veiligheidsvisie horen een aantal richtinggevende principes:

1. VEILIGHEID IS EEN GEDEELDE VERANTWOORDELIJKHEID

Medewerkers, studenten en gasten verbonden aan onze universiteit zijn in beginsel verantwoordelijk voor de eigen én andermans veiligheid. De eind-verantwoordelijkheid voor veiligheidszorg ligt bij het College van Bestuur. De afzonderlijke faculteiten en diensten zijn medeverantwoordelijk voor de veiligheidszorg binnen hun domein.

2. WIJ HEBBEN EEN BREDE ZORGPLICHT

De VU accepteert een brede zorgplicht voor de veiligheid van studenten, medewerkers en gasten verbonden aan de VU. Kortom, tot diegenen die vanuit studie, onderzoek of andere werkzaamheden waar ook ter wereld aan de VU zijn verbonden.

3. WIJ BEVORDEREN EEN 'VEILIGE CULTUUR', VEILIGHEIDS-BEWUSTZIJN EN GEVEN DUIDELIJK HANDELINGSPERSPECTIEF

De VU werkt actief aan het bevorderen en behouden van een gezonde veilig-heidscultuur. Het College van Bestuur, decanen en directeuren vervullen hierin een voorbeeldfunctie. De VU spant zich in om het veiligheidsbewustzijn van alle betrokkenen op het gewenste niveau te brengen en biedt hen handelings-perspectief voor onveilige situaties. Het is voor medewerkers (en studenten) duidelijk hoe de VU omgaat met incidenten en waar zij terecht kunnen voor ondersteuning.

4. WE WERKEN PROACTIEF EN RISICO GESTUURD

De VU neemt een actieve houding aan in het herkennen, voorkomen en beheersen van veiligheidsrisico's, incidenten en crises. De veiligheidszorg van de VU is in een goede balans met de menselijke maat, de academische waarden en privacybelangen. Onze veiligheidszorg is niet onnodig belastend voor de openheid en gastvrijheid van ons academisch instituut.

5. ONZE VEILIGHEIDSZORG IS INTEGRAAL, SAMENHANGEND, AANTOONBAAR EN STUURBAAR

De VU benadert veiligheidszorg integraal. Integraal betekent in samenhang met verschillende belangen, disciplines, niveaus en personen. Aan de veiligheidszorg liggen heldere normen, doelen en tijdlijnen ten grondslag.

6. WE ZIJN VOORBEREID OP INCIDENTEN EN HANDELEN DEZE ADEQUAAT AF

We beseffen dat niet alle onveiligheid is te voorkomen. We investeren daarom in de veerkracht van de organisatie en onze mensen, om de impact van incidenten, calamiteiten en crises te beperken, als ook een spoedig herstel mogelijk te maken. We oefenen en trainen onze mensen en maken hen duidelijk wat er van hen wordt verwacht.

3 UITGANGSPUNTEN

3. UITGANGSPUNTEN

Vanuit eerdergenoemde richtinggevende principes uit de Veiligheidsvisie VU zijn de noodplannen van de decentrale eenheden gevormd. Faculteiten, diensten en de BHV-organisatie hebben ieder voor de eigen specifieke risico's een noodplan opgesteld.

Het voorliggende stuk Integrale Bedrijfsnoodorganisatie VU Campus is een rompdocument waarin uitgangspunten en opschalingsprincipes beschreven staan. Tezamen met de noodplannen van de eenheden vormt dit rompdocument het Bedrijfsnoodplan VU.

Daarbij geldt ten aanzien van de decentrale noodplannen:

- faculteiten, diensten en de BHV-organisatie zijn verantwoordelijk voor het inrichten van eigen decentrale noodplannen gerelateerd aan de eigen specifieke risico's;
- faculteiten, diensten en de BHV-organisatie richten deze decentrale noodplannen in conform de uitgangspunten en opschalingsprincipes van dit rompdocument;
- faculteiten, diensten en de BHV-organisatie zijn verantwoordelijk voor het toepassen van de algemene opschalingsprincipes en de invulling van de verantwoordelijkheden en mandaten om te schakelen van de organisatie in normaal bedrijf naar de integrale bedrijfsnoodorganisatie.

Voor risico's gerelateerd aan het domein informatieveiligheid (zoals bijvoorbeeld cybersecurity, fraude, privacyrisico's) geldt daarnaast dat de noodplannen moeten voorzien in het treffen en onderhouden van een samenhangend pakket aan maatregelen om de kwaliteitsaspecten beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening te garanderen. Daarbij gaat het om:

- de mate waarin gegevens of functionaliteit op de juiste momenten beschikbaar zijn voor gebruikers;
- de mate waarin gegevens of functionaliteit blijvend juist en volledig zijn ingevuld;
- de mate waarin de toegang tot gegevens of functionaliteit beperkt is tot degenen die daartoe bevoegd zijn;
- de controleerbaarheid van de maatregelen die genomen zijn om deze kwaliteitsaspecten te borgen.

4 SCOPE

4. SCOPE

De in dit rompdocument beschreven uitgangspunten en aanpak zijn van toepassing op alle gebeurtenissen die op de campus plaatsvinden of die buiten de VU-organisatie de bedrijfscontinuïteit mogelijk verstoren en/of het imago van de VU schade toebrengen. Deze gebeurtenissen hebben betrekking op fysieke-, sociale- of informatieveiligheid van mensen of middelen.

In het datadomein worden met partijen – te denken valt aan externe rechtspersonen die gebruik maken van de VU-infrastructuur – individuele (contract) afspraken gemaakt ten aanzien van de verantwoordelijkheid van de VU daarin.

Daarbij vallen gebeurtenissen in de persoonlijke leefomgeving van studenten en medewerkers buiten scope, tenzij de VU incident-eigenaar wordt of kan worden.

5 WIE ZIJN BETROKKEN BIJ DE INTEGRALE BEDRIJFSNOODORGANISATIE?

5. WIE ZIJN BETROKKEN BIJ DE INTEGRALE BEDRIJFSNOODORGANISATIE?

In het normale bedrijf zijn rollen en taken die het primaire proces ondersteunen, belegd bij diensten en faculteiten.

Voor informatieveiligheid, sociale veiligheid en fysieke veiligheid is er specifieke expertise aanwezig binnen de diensten:

- *Bestuurszaken:* gegevensbescherming, privacy, klachtenregelingen, integriteit, audit, juridisch advies, bestuursfraude, aansprakelijkheid;
- *Communicatie en Marketing:* woordvoerder, veiligheids- en crisis-communicatie;
- *HRMAM:* veiligheid en gezondheid, risicoinventarisaties en evaluaties (RIE's), BHV-beleid, opleiding en instructie;
- *HRMAM en FCO*: BHV;
- *FCO:* beveiliging, meldkamer, veiligheidssystemen, toegang;
- *IT*: Security Operations Center, monitoring, analyse, informatie & databeleid, audits;
- *Student en Onderwijszaken*: coördinator diversiteit, internationale mobiliteit;
- *Financiën*: verzekeringen.

Bovenstaande expertises hebben ook een belangrijke rol in de bedrijfsnood-organisatie. Daarnaast zijn er een aantal specifieke veiligheidsrollen belegd:

- CFO: chief financial officer;
- CISO: chief information security officer;
- BHV: hoofd bedrijfshulpverlening VU;
- FG: functionaris voor de gegevensbescherming.

Naast bovenstaande rollen is de Commissie Integrale Veiligheid (CIV) een belangrijk platform om beleid en kennis rondom integrale veiligheid te delen. In de CIV worden thema's op het gebied van veiligheid besproken, afgestemd en getoetst aan de Veiligheidsvisie VU. De CIV heeft een initiatiefnemende, beleidsvoorbereidende en adviserende taak voor het CvB en een monitorende en evaluerende rol ten aanzien van veiligheidsmanagementsystemen en de borging van de samenhang.

De bemensing en taken van deze rollen zijn te vinden in de bij dit rompdocument horende protocollen van de eenheden.

6 ONTSTAAN VAN EEN NOODSITUATIE

6. HET ONTSTAAN VAN EEN NOODSITUATIE

Op verschillende manieren kan een situatie ontstaan waardoor de normale bedrijfsvoering getroffen wordt of gevaar loopt. Binnen de organisatie bestaan protocollen en systemen die een noodsituatie in de vorm van een melding kunnen registreren, herkennen of ontvangen. De meest voorkomende meldingen zijn weergegeven in onderstaande tabel.

De ontstane situatie kan leiden tot het inzetten van de integrale bedrijfsnoodorganisatie: *er wordt een bewuste keuze gemaakt om uit de normale bedrijfssituatie te stappen*. Naast de integrale bedrijfsnoodorganisatie gaat in de rest van de organisatie het normale bedrijf door.

Tabel 1. Meest voorkomende meldingen van een noodsituatie of een ongewenste/onveilige situatie

DIGITALE MELDING	BALIE MELDING	TELEFONISCHE MELDING
Meld-en adviespunt ongevallen en incidenten	IT Servicedesk	Alarmnummer 020-5982222 /22222
Klachtenformulier HAM	Securitydesk	
Meldingsformulier servicedesk FCO	Studenten service desk	
Formulier Melding Ombudsman personeel	HR service desk	
Formulier Melding Vertrouwenspersoon personeel		
vu.nl/veiligheid	Secretariaat CvB	
vu.nl/vucert	Secretariaat BZ	
vu.nl/diversiteit		

EMAIL MELDING	MELDING NAV CONTROLE	PERSOONLIJKE MELDING
vucert@vu.nl	Bewaking	Vertrouwenspersoon
soc@vu.nl	Monitoring IT systemen	Coördinator diversiteit
servicedesk.it@vu.nl	Audit	Ombudsman
ombudsmanpersoneel@vu.nl	Storingsmelding	Studiebegeleider
vertrouwenspersonen.personeel@vu.nl	Controleproces	BHV-er
vertrouwenspersonen-studenten.dsz@vu.nl	Veiligheidsinstallaties (brandmeld-systeem/CCTV)	Bedrijfsarts
servicedesk.fco@vu.nl		Functionaris Gegevensbescherming
persoonlijke email		Beveiliging
		Auditor
		CvB
		Decaan of (dienst)directeur
		P&O adviseur

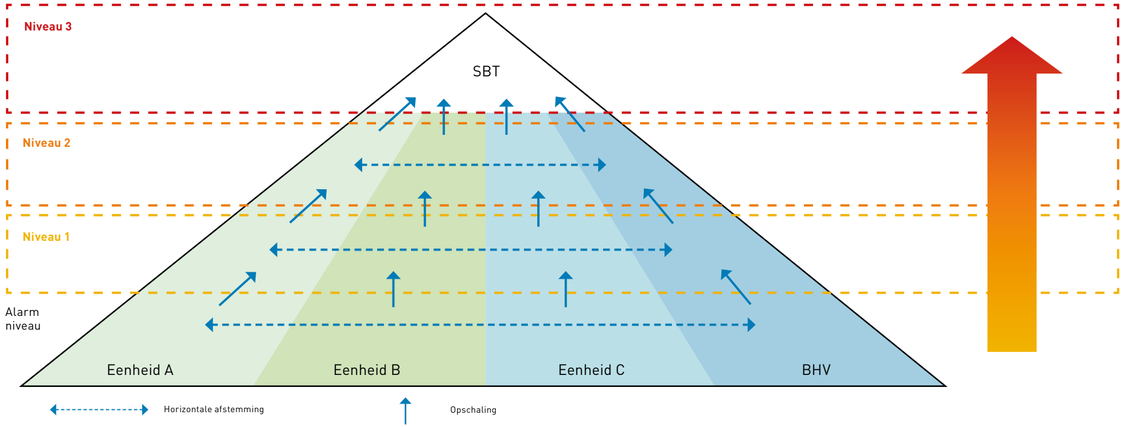
7 OPSCHALINGSPRINCIPES

7. OPSCHALINGSPRINCIPES

Het inzetten van de bedrijfsnoodorganisatie kan op verschillende niveaus: operationeel, tactisch of strategisch. Binnen de bedrijfsnoodorganisatie wordt indien nodig opgeschaald naar het bovenliggende niveau.

Bij het opschalen binnen de bedrijfsnoodorganisatie handelt er uiteindelijk op het hoogste niveau een klein team, ondersteund door bredere operationele en tactische teams, afhankelijk van het incident. Dit is schematisch weergegeven in figuur 2.

Figuur 2. Met opschalen en oppakken van de calamiteit wordt een bewuste keuze gemaakt om uit de normale situatie te stappen.



In figuur 3 zijn de drie niveaus van de integrale bedrijfsnoodorganisatie schematisch weergegeven, alsook de noodsituaties waarop deze van toepassing zijn. In figuur 4 zijn de gebieden waar de meeste incidenten voorkomen opgenomen (BHV, IT, Privacy, Informatieveiligheid, Zorgwekkend gedrag, Internationale mobiliteit en Fraude/Integriteit), en wordt voor alle opschalingniveaus aangegeven wie de betrokkenen zijn.

Niveau 1 (operationeel) wordt ingezet bij melding van een situatie met een beperkte complexiteit, met geringe impact op personen en/of gebouwen, met een korte afhandelingsduur en met geringe reputatieschade. Een melding kan op meerdere manieren binnenkomen (tabel 1) en binnen meerdere domeinen tegelijkertijd worden opgepakt: iBNO-brede gerichte afspraken zijn dan belangrijk. Niveau 1 incidenten worden in principe afgehandeld door een operationeel team uit de lijnorganisatie.

Opschalen naar niveau 2
Als een noodsituatie zwaarder is of wordt dan niveau 1 wordt er opgeschaald naar niveau 2. Daarbij worden de volgende vragen beantwoord:
- Zijn er iBNO-breed afspraken gemaakt waar nodig?
- Wie voert de regie?

Niveau 2 (tactisch) wordt ingezet bij een noodsituatie met grote complexiteit, met grote impact op personen en/of gebouwen, met een langere afhandelingsduur en met mogelijke reputatieschade. Niveau 2 incidenten worden afgehandeld door een incidentafhankelijk team waarbij iBNO breed wordt samengewerkt. Het team wordt in de meeste gevallen ondersteund door het niveau 1 team uit de operationele lijnorganisatie.
De regievoerder van het incidentafhankelijke team:
- informeert de directeur (niveau 3): 'ik informeer je maar je hoeft niets doen', die op zijn/haar beurt CvB-lid met piket informeert;
- schaalt op indien nodig;
- zorgt voor verslaglegging / data-logging;
- evalueert en deelt lessons learned.

Bij een niveau 2 incident kan er door een directeur of Cvb-lid met piket de afweging gemaakt worden om externe stakeholders of Raad van Toezicht te informeren over het incident. *Dit betekent echter niet dat er opgeschaald wordt naar niveau 3!*

Opschalen naar niveau 3
Als een noodsituatie zwaarder is of wordt dan niveau 2 wordt er opgeschaald naar niveau 3. De regievoerder:
- informeert portefeuillehouder CvB;
- roept Strategisch Beleidsteam (SBT) op;
- informeert SBT.

Niveau 3 (strategisch) wordt ingezet bij een noodsituatie met zeer grote complexiteit, met zeer grote impact op personen en/of gebouwen, met lange afhandelingsduur of met reputatieschade. Niveau 3 incidenten worden afgehandeld door het Strategisch Beleidsteam (SBT), bestaande uit het kernteam, incidentafhankelijke aanvulling en administratieve ondersteuning. Het SBT wordt ondersteund door het incidentafhankelijk niveau 2 team.

Bij de beveiliging en bij het Meld- en Bedieningscentrum (MBC) zijn calamiteitenbellijsten van alle diensten en faculteiten beschikbaar om ingezet te worden bij overleg en/of opschaling.

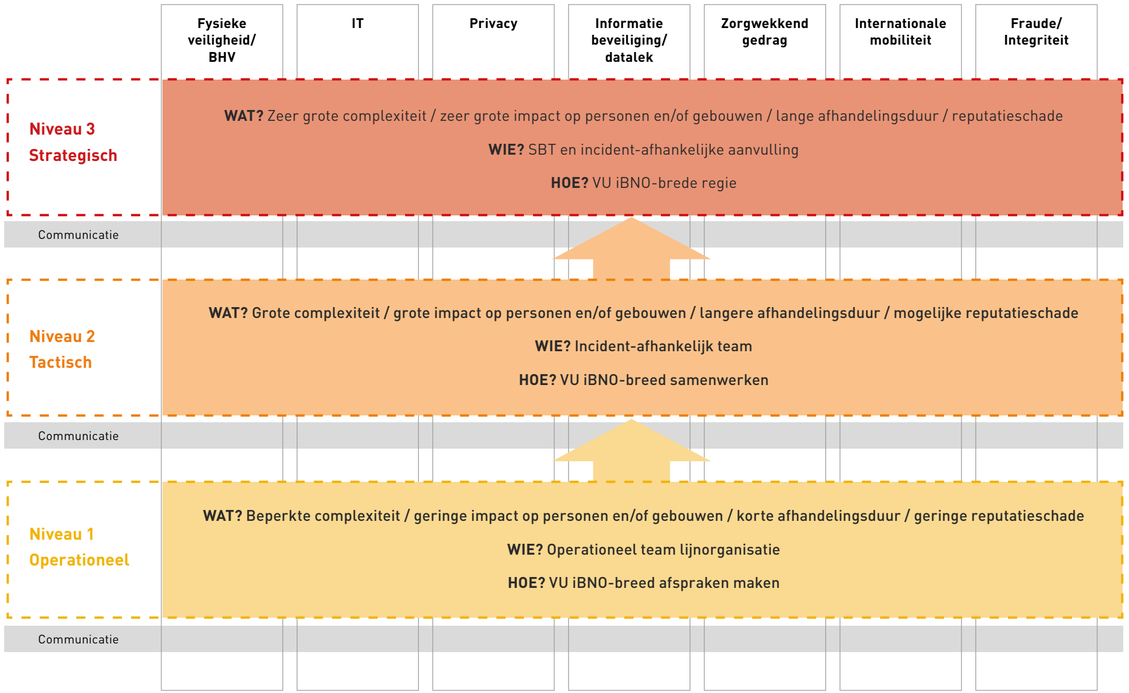
Communicatie rondom niveau 2 incident

CVB-LID MET PIKET:
- Informeert college-CvB leden waar nodig
- Informeert stakeholders buiten instelling waar nodig
- Informeert RvT waar nodig

DIRECTEUR:
- Informeert portefeuillehouder CvB
- Informeert (indien nodig) SBT
- Roept SBT op indien nodig

VOORZITTER/REGIEVOERDER:
- Informeert directeur (niveau 3)
- Schaalt op indien nodig
- Zorgt voor verslaglegging/logging
- Is verantwoordelijk voor de evaluatie en delen lessons learned (na afloop)

Figuur 3. Opschalingsprincipes iBNO



Figuur 4. Betrokkenen iBNO

Niveau 3 Strategisch = iBNO brede regie

Kernteam
Voorzitter
Secretaris
Communicatie

Dienstdoend piket CvB lid
Secretaris CvB
Directeur C&M

Administratieve ondersteuning
Plotter
Admin mw

Medewerker BZ
Medewerker BZ

Afhankelijk van calamiteit
Fysieke veiligheid/vastgoed
Informatiebeveiliging
Juridische zaken en privacy
Financien
HRMAM
Fraude/integriteit
Faculteit/dienst
Aanvullend

Directeur FCO
CISO / Directeur IT
Hoofd BJZ / FG / directeur BZ
Directeur Financien
Directeur HRMAM
Interne auditor
Decaan/directeur
(specifieke) Deskundigen/medewerkers

	Fysieke veiligheid/ BHV	IT	Privacy	Informatie beveiliging/ datalek	Zorgwekkend gedrag	Internationale mobiliteit	Fraude/ Integriteit
Niveau 2 Tactisch = iBNO brede samenwerking	**Operationeel crisisteam (OCT)** Hoofd BHV Plv hoofd BVH	**Crisismanager** Afdelingshoofden IT	**Jurist** Privacyjurist	**SOC/CERT** Coordinator SOC Coordinator CERT	**Kernteam zorgwekkend gedrag** Directeur FCO Hoofd Services FCO Hoofd beveiliging Selectie expertteam	**Tactisch Crisisteam Internationale Mobiliteit (TCIM)** Directeur IO Dir BV Faculteit OCIM	**Interne auditor** Dir. Financien Hfd Beveiliging Dir. HRMAM Hfd BJZ SOC
Communicatie	Woordvoerder						
Afhankelijk van calamiteit	Directeur/ dienst bedrijfsvoeringdirecteur						
Niveau 1 Operationeel = iBNO brede afstemming	**BHV'ers**	**Calamiteiten coordinatoren** Teamleiders	**Jurist** Privacyjurist	**SOC/CERT**	**Beveiliging** Directeur bedrijfsvoering of dienst	**Operationeel Crisisteam Internationale Mobiliteit (OCIM)** Hoofd mobility Teamleiders mobility	**Interne auditor**
Communicatie	Leidinggevende eenheid	Leidinggevende eenheid	Leidinggevende eenheid	Leidinggevende eenheid	Leidinggevende eenheid	Leidinggevende eenheid	Leidinggevende eenheid

8 KRITIEKE BESLUITEN

8. KRITIEKE BESLUITEN

Tijdens het inzetten van de integrale bedrijfsnoodorganisatie kunnen zich situaties voordoen waarin kritieke besluiten genomen moeten worden. Deze besluiten hebben een dusdanig grote impact op de organisatie dat vooraf doordacht is:

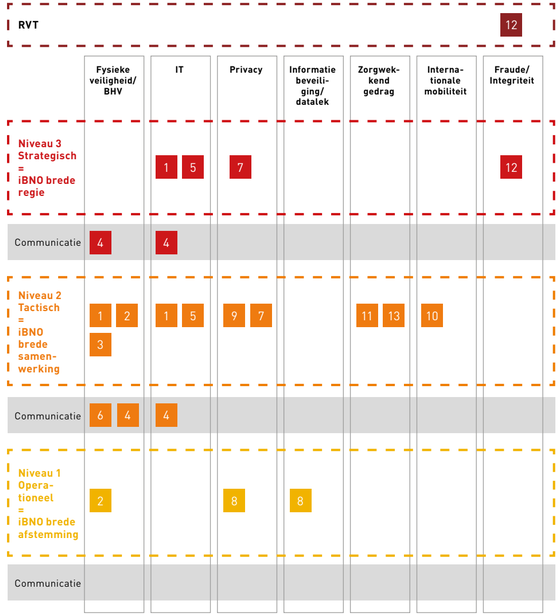
- wie (functie) het besluit neemt;
- of activering iBNO noodzakelijk is;
- op welk niveau iBNO ingezet wordt.

De meest voorkomende kritieke besluiten zijn:

1. Stopzetten (delen van) van onderwijs (langer dan 1 uur) als gevolg van een niet-onderwijskundige factor (bv. dreiging, suïcide, ontruiming, datalek, weersomstandigheden);
2. Acute ontruiming van een locatie;
3. Niet-acute ontruiming van een locatie;
4. Bekendmaken van nieuws met grote impact;
5. Stopzetten gebruik van een vitaal systeem (SAP, Canvas …) /het bewust verstoren van de dienstverlening / het blokkeren van accounts;
6. Interne communicatie over (zeer) gevoelige kwestie;
7. Verstrekken privacygevoelige gegevens;
8. Beoordeling wel/geen datalek;
9. Melding datalek bij AP;
10. Terughalen van medewerkers/studenten uit het buitenland (bevel/faciliteren);
11. Het doen van aangifte;
12. Vermoeden van directie- of bestuursfraude;
13. Op non-actief zetten medewerker/student;

In figuur 5 is aangegeven op welk opschalingsniveau van de iBNO het kritieke besluit genomen wordt: veel van de kritieke besluiten worden op niveau 2 afgehandeld.

Figuur 5. Overzicht kritieke besluiten

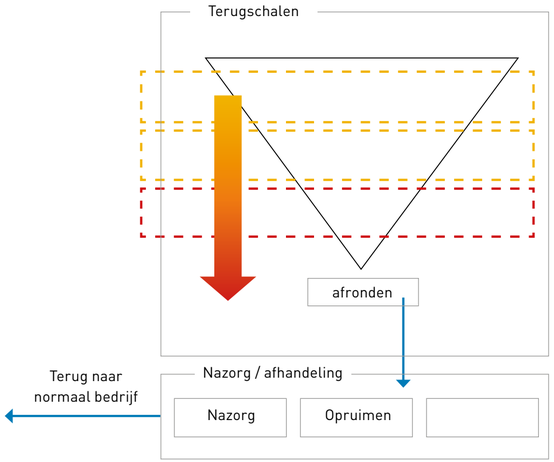


9 AFSCHALEN, VASTLEGGEN EN EVALUEREN

9. AFSCHALEN, VASTLEGGEN EN EVALUEREN

Op het moment dat er geen sprake meer is van een noodsituatie kan er afgeschaald worden, om zo snel mogelijk terug te keren naar het normale bedrijf. Daarbij hoort continuering van de bedrijfsvoering, nazorg, het vastleggen van het incident en de evaluatie. Nazorg of herstel kan langere tijd vragen van bijvoorbeeld een operationeel team, die parallel aan normaal bedrijf kan worden uitgevoerd. In figuur 6 is de afschaling schematisch weergegeven.

Figuur 6 Afschalen na een incident



In de noodplannen van de decentrale eenheden staat omschreven:

- welke (psychosociale) nazorg voor slachtoffers/betrokkenen en hulpverleners er georganiseerd moet worden;
- richtlijnen over herstel van schade;
- hoe omgegaan wordt met juridische aspecten, aansprakelijkheid, het verhalen van schade.

Alle situaties waarbij de iBNO ingezet wordt, worden door de niveau 2 regievoerder vastgelegd in de integrale incidentendatabase en waar nodig van context voorzien. Daarnaast zorgt de regievoerder voor een korte evaluatie naar de CIV.

Lessons learned over veiligheidssituaties worden periodiek gedeeld in het niveau 2 iBNO overleg, waaruit aanbevelingen voor de CIV kunnen volgen.

De CIV is eigenaar van dit rompdocument en draagt zorg voor het iBNO-breed evalueren van veiligheidssituaties en, naar aanleiding daarvan, het bijstellen van beleid, organisatie, processen en procedures.

BIJLAGE: DECENTRALE NOODPLANNEN EN PROTOCOLLEN

1. STRATEGISCH BELEIDSTEAM

1.1	Beleidsdocument IBNO (2017)
1.2	Crisiscommunicatie - Draaiboek Calamiteiten 2015
1.3	Calamiteitenplan Zuidas
1.4	IVHO-formats voor SITraps, BOB methode en SBT-agenda

2. BHV

2.1	Beleidsdocument BNO VU (2015)
2.2	Factsheets met scenario's (fysieke en sociale incidenten)
2.3	Actiekaarten voor de generieke operationele BHV taken (EHBO, ontruimers, VURIT, ploegleider etc.)
2.4	Checklists OCT BHV en SBT BHV
2.5	Oproepschema MBC
2.6	Specifieke draaiboeken en noodplannen

3. IT

3.1	Calamiteitenprotocol IT (september 2016)
3.2	Quick reference card calamiteit P1
3.3	Business Continuiteit management beleid (niet vastgesteld)

4. PRIVACY

4.1	Protocol Meldplicht datalekken

5. INFORMATIE BEVEILIGING / DATALEK

5.1	Informatie-beveiligingsbeleid 2016-2018
5.2	Beleid toegangsbeveiliging informatie en systemen
5.3	Protocol Meldplicht datalekken

6. ZORGWEKKEND GEDRAG

6.1	Procesbeschrijving zorgwekkend gedrag

7. INTERNATIONALE MOBILITEIT

7.1	Handboek crisismanagement (mei 2011)
7.2	Beleidsrichtlijn uitgaande mobiliteit (samenvatting handboek)
7.3	Memo Crisis management policy CIS april 2016

8. FRAUDE / INTEGRITEIT

8.1	Fraudeprotocol VU
8.2	Klachtenregeling Wetenschappelijke Integriteit VU-VUMC (jan 2016)
8.3	Commissie Wetenschappelijke integriteit VU-VUmc (CWI)
8.4	Vertrouwenspersonen WI
8.5	Regeling ongewenst gedrag
8.6	Code Goed Bestuur Universiteiten (VSNU 2017)
8.7	Regeling nevenwerkzaamheden
8.8	Klokkenluidersregeling 1 november 2016
8.9	Reglement van de Raad van Toezicht
8.10	Hooglerarenbeleid 2016
8.11	Bijeenkomst nieuwe VU medewerkers met daarbij aandacht voor integriteit van handelen
8.12	Enquête over wetenschappelijke integriteit
8.13	Integriteitscode Facilitaire Campus Organisatie Vrije Universiteit (februari 2014)
8.14	Studentenstatuut
8.15	Inkoop- & aanbestedingsbeleid VU, inclusief uitvoeringsregels (jan 2015)
8.16	Gedragscode computer- en netwerkgebruik (2011)

INTEGRALE BEDRIJFSNOODORGANISATIE VU CAMPUS

VU VRIJE UNIVERSITEIT AMSTERDAM