ALLEMAAL VEILIG

BEDRIJFSNOODPLAN

Praktisch invul- en actieplan voor zzp, kleine en middelgrote bedrijven

Bedrijfsveiligheid | crisisorganisatie | noodvoorzieningen | bedrijfscontinuïteit

Gegeven	In te vullen
Bedrijfsnaam	_____
Vestiging / locatie	_____
Planbeheerder	_____
Versie en vaststellingsdatum	_____
Volgende evaluatiedatum	_____

Belangrijk: dit sjabloon is een hulpmiddel en vervangt geen bedrijfsspecifieke risico-inventarisatie en -evaluatie (RI&E;), BHV-organisatie, wettelijke voorschriften of aanwijzingen van hulpdiensten. Bel bij direct levensgevaar 112.

1. Documentbeheer en gebruik

Vul de tabellen per vestiging in, wijs eigenaren toe en bespreek de afspraken met medewerkers. Bewaar een papieren exemplaar op een bekende plaats en een beveiligde offline kopie. Leg persoonsgegevens alleen vast als noodzakelijk en bescherm toegang.

Gegeven	In te vullen
Documenteigenaar / functie	_____
Goedgekeurd door	_____
Datum laatste oefening	_____
Locatie papieren kopie	_____
Locatie offline kopie	_____
Wie ontvangt updates?	_____

Versie	Datum	Wijziging	Akkoord
____	____	_____	____
____	____	_____	____
____	____	_____	____
____	____	_____	____

Snelle gebruiksinstructie

1. Vul eerst hoofdstuk 2 t/m 6 in. 2. Kies relevante scenario’s uit hoofdstuk 7 t/m 12. 3. Controleer voorraden en herstelopties. 4. Oefen het plan. 5. Actualiseer na wijzigingen of incidenten.

2. Bedrijfsprofiel en kritieke activiteiten

Gegeven	In te vullen
Adres en toegang / verdieping	_____
Algemeen telefoonnummer	_____
Aantal medewerkers op locatie	_____
Gemiddeld aantal bezoekers / klanten	_____
Openingstijden / ploegendiensten	_____
Bijzondere hulpbehoeften (zonder onnodige medische details)	_____
Belangrijkste producten / diensten	_____

Kritiek proces	Max. aanvaardbare onderbreking	Afhankelijkheden	Alternatieve werkwijze
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

3. Crisisorganisatie en bevoegdheden

Bij zzp kan één persoon meerdere rollen vervullen. Bij grotere bedrijven zijn vervangers noodzakelijk. Benoem wie mag besluiten tot ontruiming, werkonderbreking, externe communicatie en hersteluitgaven.

Rol	Naam / vervanger	Bereikbaar via	Beslisbevoegdheid
Crisisleider	_____	_____	_____
BHV / ontruiming	_____	_____	_____
Communicatie	_____	_____	_____
ICT / informatiebeveiliging	_____	_____	_____
Facilitair / techniek	_____	_____	_____
Continuïteit / leveranciers	_____	_____	_____

Opschalen

Activeer dit plan bij gevaar voor personen, uitval van een kritiek proces, verlies van toegang tot de locatie of een incident dat niet met normale werkafspraken kan worden beheerst. De crisisleider beoordeelt elk incident, registreert besluiten en schakelt zo nodig hulpdiensten in.

Gegeven	In te vullen
Verzamelpunt crisisoverleg	_____
Vervangende overleglocatie	_____
Noodbudget / akkoordprocedure	_____

4. Noodcontacten en alarmering

Contact	Naam / organisatie	Telefoon / alternatief
112 (spoed)	_____	_____
Huisarts / huisartsenpost	_____	_____
BHV / beheerder gebouw	_____	_____
Politie (niet-spoed)	_____	_____
Netbeheerder / storingsdienst	_____	_____
ICT / cybersecurity-partner	_____	_____
Verzekeraar / tussenpersoon	_____	_____
Verhuurder / beheerder	_____	_____
Belangrijke leverancier	_____	_____
Gemeente / veiligheidsregio	_____	_____

Bij spoed: vermeld adres, aard van het incident, slachtoffers en actuele gevaren. Wijs iemand aan om hulpdiensten op te vangen. Leg offline contactgegevens vast en controleer ze periodiek.

5. Risicoanalyse en prioriteiten

Beoordeel per risico de kans en impact op een schaal van 1 (laag) tot 5 (hoog). Vermenigvuldig beide waarden als eenvoudige prioriteringshulp; dit is geen vervanging van de RI&E.; Noteer bestaande maatregelen en resterende acties.

Risico	Kans	Impact	Maatregel / eigenaar
Brand / rook	__	__	_____
Medisch incident	__	__	_____
Stroomuitval	__	__	_____
Internet / telefonie uitval	__	__	_____
Cyberaanval / datalek	__	__	_____
Extreem weer / wateroverlast	__	__	_____
Inbraak / agressie	__	__	_____
Leveranciersuitval	__	__	_____
Personeelsuitval	__	__	_____
Gevaarlijke stoffen (indien relevant)	__	__	_____

Gegeven	In te vullen
Drie hoogste prioriteiten	_____
Actiehouder / deadline	_____
Acceptabel restrisico / akkoord	_____

6. Ontruiming, schuilen en BHV

Controlepunt	Status / afspraak
Vluchtroutes en nooduitgangen zijn vrij en bekend	[ ] Ja [ ] Nee [ ] N.v.t. _____
Ontruimingsplattegrond en verzamelplaats zijn vastgesteld	[ ] Ja [ ] Nee [ ] N.v.t. _____
BHV-bezetting sluit aan op risico's en aanwezigheid	[ ] Ja [ ] Nee [ ] N.v.t. _____
EHBO-koffer, AED (indien aanwezig) en blusmiddelen zijn gecontroleerd	[ ] Ja [ ] Nee [ ] N.v.t. _____
Procedure voor bezoekers en minder mobiele personen is afgesproken	[ ] Ja [ ] Nee [ ] N.v.t. _____
Afsluiten gas / elektra is alleen toegewezen aan bevoegde personen	[ ] Ja [ ] Nee [ ] N.v.t. _____
Er is een aanwezigheids- en vermistencontrole	[ ] Ja [ ] Nee [ ] N.v.t. _____

Gegeven	In te vullen
Verzamelplaats buiten	_____
Alternatieve verzamelplaats	_____
Schuilruimte binnen (indien relevant)	_____
Wie telt medewerkers / bezoekers?	_____
Wie geeft vrijgave voor terugkeer?	_____

Actie bij brand of direct gevaar: alarmeer 112, waarschuw aanwezigen, verlaat het gebouw via veilige routes, gebruik geen lift bij brand en volg de aanwijzingen van BHV en hulpdiensten. Blussen uitsluitend als dit veilig en passend is.

7. Actiekaarten voor acute incidenten

Incident	Directe eerste acties
Brand / rook	Alarmeer 112; waarschuw anderen; ontruim; sluit deuren indien veilig; meld vermisten.
Medisch noodgeval	Bel 112 bij levensgevaar; laat BHV / getrainde hulpverlener handelen; zorg voor vrije toegang.
Agressie / geweld	Breng mensen in veiligheid; vermijd confrontatie; bel 112 bij acuut gevaar; registreer feiten.
Gaslucht / chemisch incident	Verlaat gevarenzone; vermijd ontstekingsbronnen; bel 112; volg deskundige instructies.
Overstroming / extreem weer	Volg NL-Alert en veiligheidsregio; vermijd gevaarlijke ruimtes en water; beslis over schuilen of evacueren.
Verdacht pakket / dreiging	Raak niets aan; houd afstand; volg politie-instructies; voorkom verspreiding van onbevestigde informatie.

Incidentlog

Tijd	Gebeurtenis / besluit	Eigenaar	Vervolg
____	_____	_____	_____
____	_____	_____	_____
____	_____	_____	_____
____	_____	_____	_____
____	_____	_____	_____

8. Stroom, internet en communicatie

Controlepunt	Status / afspraak
Essentiële apparatuur en minimale stroombehoefte zijn bepaald	[ ] Ja [ ] Nee [ ] N.v.t. _____
UPS / noodstroom voor kritieke systemen is getest	[ ] Ja [ ] Nee [ ] N.v.t. _____
Veilige noodverlichting en zaklampen zijn beschikbaar	[ ] Ja [ ] Nee [ ] N.v.t. _____
Mobiele telefoons / powerbanks zijn opgeladen	[ ] Ja [ ] Nee [ ] N.v.t. _____
Offline adressen en telefoonnummers zijn beschikbaar	[ ] Ja [ ] Nee [ ] N.v.t. _____
Alternatief internet of telefonie is getest	[ ] Ja [ ] Nee [ ] N.v.t. _____
Handmatige order-, betaal- en registratieprocedure bestaat	[ ] Ja [ ] Nee [ ] N.v.t. _____
Aggregaten worden alleen veilig, buiten en volgens voorschrift gebruikt	[ ] Ja [ ] Nee [ ] N.v.t. _____

Storing	Starttijd / grens	Alternatief	Verantwoordelijke
Stroomuitval	_____	_____	_____
Internetstoring	_____	_____	_____
Telefonie-uitval	_____	_____	_____
Pin / betaaluitval	_____	_____	_____

9. Cyberincidenten, privacy en IT-herstel

Denk aan phishing, ransomware, verlies van apparaten, onbereikbare cloudsoftware en mogelijke datalekken. Houd het herstelplan gescheiden van de systemen die getroffen kunnen worden.

Controlepunt	Status / afspraak
MFA is ingeschakeld op kritieke accounts	[ ] Ja [ ] Nee [ ] N.v.t. _____
Back-ups zijn geïsoleerd / offline en herstel is getest	[ ] Ja [ ] Nee [ ] N.v.t. _____
Lijst met kritieke systemen en beheerders is beschikbaar	[ ] Ja [ ] Nee [ ] N.v.t. _____
Meldroute naar ICT-partner en leidinggevende is bekend	[ ] Ja [ ] Nee [ ] N.v.t. _____
Getroffen systemen kunnen veilig worden geïsoleerd	[ ] Ja [ ] Nee [ ] N.v.t. _____
Datalekbeoordeling en eventuele meldplicht zijn belegd	[ ] Ja [ ] Nee [ ] N.v.t. _____
Noodaccounts en herstelcodes zijn beveiligd opgeslagen	[ ] Ja [ ] Nee [ ] N.v.t. _____

Actie bij vermoedelijke cyberaanval

1. Stop risicovolle handelingen en meld het incident. 2. Isoleer getroffen apparaten of accounts volgens instructie van de ICT-verantwoordelijke. 3. Bewaar relevante informatie en logboeken. 4. Beoordeel persoonsgegevens, meldplichten en communicatie. 5. Herstel uitsluitend uit gecontroleerde, schone bronnen.

Gegeven	In te vullen
ICT-noodnummer	_____
Back-uplocatie (geen wachtwoorden)	_____
Laatste hersteltest	_____
Verantwoordelijke datalekbeoordeling	_____

10. Noodpakket en zelfredzaamheid

Stem voorraden af op het aantal aanwezigen, de risico's, mogelijke schuilduur en specifieke behoeften. Een voorbereiding van 72 uur kan als uitgangspunt dienen, maar is geen universele wettelijke norm voor alle bedrijven. Voor drinkwater wordt vaak 3 liter per persoon per dag als planningsrichtlijn gebruikt.

Categorie	Voorbeelden / aandachtspunten	Aantal / locatie / datum
Water en voedsel	Drinkwater, houdbaar eten, dieetwensen	_____
Licht en energie	Zaklampen, batterijen, powerbanks	_____
Communicatie	Noodradio, contactlijsten, portofoons indien nodig	_____
EHBO en hygiëne	EHBO, handschoenen, sanitair, persoonlijke benodigdheden	_____
Warmte en beschutting	Dekens, kleding, schuilvoorzieningen	_____
Werkcontinuïteit	Papieren formulieren, sleutels, hulpmiddelen	_____
Documentatie	Plan, plattegronden, instructies, verzekeringsgegevens	_____

Gegeven	In te vullen
Maximaal aantal personen	_____
Gewenste overbrugging (uren)	_____
Drinkwaterberekening	_____
Voorraadbeheerder	_____
Volgende houdbaarheidscontrole	_____

11. Leveranciers, personeel en alternatieve locatie

Afhankelijkheid	Primaire oplossing	Terugvaloptie	Contact
Kritieke leverancier 1	_____	_____	_____
Kritieke leverancier 2	_____	_____	_____
Transport / logistiek	_____	_____	_____
Betaalverkeer	_____	_____	_____
Werkplek / gebouw	_____	_____	_____
Sleutelfunctie personeel	_____	_____	_____

Controlepunt	Status / afspraak
Alternatieve leveranciers zijn vooraf beoordeeld	[ ] Ja [ ] Nee [ ] N.v.t. _____
Vervanging bij uitval van sleutelpersonen is geregeld	[ ] Ja [ ] Nee [ ] N.v.t. _____
Thuiswerk / uitwijklocatie is praktisch getest	[ ] Ja [ ] Nee [ ] N.v.t. _____
Klanten kunnen bij vertraging geïnformeerd worden	[ ] Ja [ ] Nee [ ] N.v.t. _____
Contractuele verplichtingen en verzekeringen zijn bekeken	[ ] Ja [ ] Nee [ ] N.v.t. _____

12. Crisiscommunicatie

Doelgroep	Wie communiceert?	Kanaal 1 / reserve	Frequentie
Medewerkers	_____	_____	_____
Klanten	_____	_____	_____
Leveranciers	_____	_____	_____
Verhuurder / buren	_____	_____	_____
Pers / publiek	_____	_____	_____
Toezichthouder indien vereist	_____	_____	_____

Berichtsjabloon

Onderwerp: tijdelijke verstoring bij [bedrijf]. Op [datum/tijd] is [feitelijke situatie] vastgesteld. Onze eerste prioriteit is [veiligheid/continuïteit]. [Gevolg voor ontvanger]. De volgende update volgt uiterlijk [tijd] via [kanaal]. Contact: [naam / nummer].

Communiceer uitsluitend bevestigde feiten, deel geen gevoelige persoonsgegevens en verwijs voor publieke veiligheidsinstructies naar bevoegde instanties.

13. Herstel, evaluatie en nazorg

Controlepunt	Status / afspraak
Veiligheid van locatie en personen is bevestigd	[ ] Ja [ ] Nee [ ] N.v.t. _____
Schade en gevolgen zijn vastgelegd	[ ] Ja [ ] Nee [ ] N.v.t. _____
Verzekeraar en relevante partijen zijn geïnformeerd	[ ] Ja [ ] Nee [ ] N.v.t. _____
IT en gegevens zijn gecontroleerd vóór hervatting	[ ] Ja [ ] Nee [ ] N.v.t. _____
Kritieke processen zijn volgens prioriteit herstart	[ ] Ja [ ] Nee [ ] N.v.t. _____
Medewerkers hebben informatie en passende nazorg gekregen	[ ] Ja [ ] Nee [ ] N.v.t. _____
Incident, besluiten en verbeterpunten zijn geëvalueerd	[ ] Ja [ ] Nee [ ] N.v.t. _____

Herstelactie	Eigenaar	Deadline	Gereed
_____	_____	_____	[ ]
_____	_____	_____	[ ]
_____	_____	_____	[ ]
_____	_____	_____	[ ]
_____	_____	_____	[ ]
_____	_____	_____	[ ]

14. Oefeningen, inspecties en onderhoud

Onderdeel	Voorstel frequentie	Eigenaar / datum
Noodcontacten	Elk kwartaal en bij wijzigingen	_____
Noodpakket en houdbaarheid	Elk kwartaal	_____
Batterijen en noodstroom	Volgens fabrikant; periodiek testen	_____
BHV / ontruiming	Risicogericht en volgens organisatiebeleid	_____
Back-upherstel	Periodiek en na grote wijzigingen	_____
Volledig plan	Minstens jaarlijks en na incident	_____

Oefenregistratie

Datum	Scenario	Wat ging goed?	Verbeteractie / eigenaar
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

15. Snelle crisiskaart - uitknippen of apart bewaren

1. Veiligheid eerst: bij direct gevaar 112; waarschuw aanwezigen; ontruim of schuil volgens situatie en officiële instructies.

2. Meld: locatie, incident, slachtoffers, gevaren en contactpersoon.

3. Organiseer: crisisleider activeert plan; wijs rollen toe; controleer aanwezigen.

4. Beperk schade: schakel bevoegde specialisten in; neem geen onveilige maatregelen.

5. Communiceer: geef feitelijke updates en noteer besluiten.

6. Herstel: hervat werk pas na veiligheidscontrole en beoordeling van kritieke systemen.

Gegeven	In te vullen
Exact adres / ingang hulpdiensten	_____
Verzamelplaats	_____
Crisisleider + reserve	_____
BHV-contact	_____
ICT-noodnummer	_____
Locatie noodpakket	_____
Locatie papieren plan	_____

Officiële informatie: NL-Alert, veiligheidsregio, gemeente en hulpdiensten. Dit document moet lokaal worden ingevuld en gevalideerd voordat het operationeel wordt gebruikt.