



Digitaal noodpakket

Maak zelf snel een digitaal noodpakket!

Een digitaal noodpakket hoeft geen ingewikkeld plan te zijn.
Met deze 8 stappen heeft u de belangrijkste zaken snel geregeld.

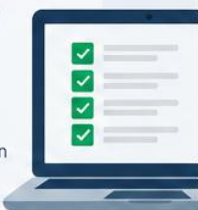
www.samendigitaalveilig.nl

1 Overzicht kritieke systemen

Welke digitale systemen heeft u nodig om uw bedrijf draaiende te houden?

Voorbeelden

- ☐ E-mail (bijv. Microsoft 365)
- ☐ Boekhouding (bijv. Exact)
- ☐ Planning (bijv. AFAS)
- ☐ Kassasysteem
- ☐ Website en webshop
- ☐ Klantendossiers (CRM)
- ☐ Productie- of OT-systemen
- ☐ Bestellingen / logistiek
- ☐ Andere: _____



2 Belangrijke contactgegevens offline

Zet de belangrijkste contactgegevens op papier. Vul zelf de telefoonnummers en e-mailadressen in.

Voorbeelden (zelf invullen)

- ☐ IT-beheerder: _____
- ☐ Softwareleverancier: _____
- ☐ Hostingprovider: _____
- ☐ Telecomprovider: _____
- ☐ Cyberverzekeraar: _____
- ☐ Belangrijke leveranciers: _____
- ☐ Andere: _____



3 Back-ups controleren

Zorg dat uw gegevens veilig zijn opgeslagen en dat u ze daadwerkelijk kunt herstellen.

Voorbeelden

- ☐ Waar staan de back-ups? (cloud en/of offline)
- ☐ Wanneer is de laatste hersteltest gedaan?
- ☐ Welke gegevens worden dagelijks geback-up?
- ☐ Hoe lang worden back-ups bewaard?
- ☐ Wie kan een herstel uitvoeren?



4 Alternatieve werkwijze

Hoe werkt u verder als e-mail, internet, boekhouding of planning niet beschikbaar is?

Voorbeelden

- ☐ Bestellingen telefonisch aannemen
- ☐ Papieren klantenlijst gebruiken
- ☐ Planning op papier of in een ander systeem
- ☐ Bonnen en facturen later invoeren
- ☐ Werkinstructies lokaal beschikbaar
- ☐ Medewerkers kunnen doorwerken zonder internet
- ☐ Andere: _____



5 Verantwoordelijkheden

Wie neemt bij een incident beslissingen en wie doet wat?

Voorbeelden

- ☐ Incidentleider
- ☐ Contact IT-leverancier
- ☐ Interne communicatie
- ☐ Klanten informeren
- ☐ Besluit uitzetten systemen
- ☐ Besluit weer opstarten
- ☐ Andere: _____



6 Belangrijkste leveranciers

Van welke externe partijen bent u afhankelijk en wat hebben zij geregeld voor calamiteiten?

Voorbeelden

- ☐ IT-beheerder (beheer, support, herstel)
- ☐ Cloudleverancier (bijv. Microsoft, AWS)
- ☐ Softwareleverancier (bijv. Exact, AFAS)
- ☐ Telecomprovider (internet, telefonie)
- ☐ Betalingsprovider (bijv. Mollie, Adyen)
- ☐ Logistieke partner
- ☐ Productieleverancier
- ☐ Wat is hun noodprocedure?
- ☐ Krijgen we tijdig informatie?
- ☐ Andere: _____



7 Eerste uur: wat doen we?

Zorg dat medewerkers weten wat ze direct moeten doen als er iets ernstigs gebeurt.

Voorbeeld stappen

- 1 Blijf rustig en ga niet zelf experimenteren.
- 2 Koppel verdachte computer los van het netwerk.
- 3 Meld het bij de incidentleider.
- 4 Neem contact op met de IT-leverancier.
- 5 Informeer medewerkers en (indien nodig) klanten.
- 6 Leg vast wat er is gebeurd.



8 Test het één keer

Oefen of de afspraken ook in de praktijk werken.

Voorbeeld oefening

- ☐ Stel: internet en belangrijke systemen zijn de hele dag niet beschikbaar.
- ☐ Loop met een paar medewerkers door de stappen.
- ☐ Komen we overal bij?
- ☐ Werken de noodnummers?
- ☐ Kunnen we doorwerken?
- ☐ Wat ontbreekt nog?



Leg het noodpakket ook offline klaar

Bewaar de belangrijkste informatie niet alleen digitaal.
Maak een map of envelop en leg deze op een bekende en veilige plaats.

Voorbeeld inhoud:

- Lijst kritieke systemen
- Noodtelefoonnummers
- Verantwoordelijke personen

- Belangrijkste leveranciers
- Eerste-uur-instructies
- Alternatieve werkwijzen
- Eventuele papieren werkinstructies

Maak zelf snel een digitaal noodpakket!

Een digitaal noodpakket hoeft geen ingewikkeld plan van tientallen pagina's te zijn. Zorg vooral dat u bij een storing of cyberincident niet eerst hoeft uit te zoeken wie u moet bellen en wat u moet doen.

1. Schrijf op welke systemen echt noodzakelijk zijn

Maak een korte lijst van de systemen die u nodig heeft om uw bedrijf draaiende te houden. Denk aan e-mail, boekhouding, planning, bestellingen, productie, kassasysteem, website of klantendossiers. Vraag vervolgens per systeem: wat gebeurt er als dit morgen een hele dag niet werkt?

2. Zet belangrijke telefoonnummers op papier

Bewaar de belangrijkste contactgegevens ook buiten uw computer en telefoon. Denk aan uw IT-beheerder, softwareleverancier, hostingbedrijf, telecomprovider, cyberverzekeraar en belangrijke leveranciers. Als uw computer of internet niet werkt, moet u deze mensen nog steeds kunnen bereiken.

3. Controleer uw back-ups

Vraag uw IT-leverancier waar uw back-ups staan en wanneer voor het laatst is getest of ze daadwerkelijk kunnen worden teruggezet. Een back-up hebben is niet voldoende. U moet zeker weten dat u ermee kunt herstellen.

4. Bedenk hoe u tijdelijk zonder systemen kunt werken

Wat doet u als e-mail, internet, planning of boekhouding een dag niet beschikbaar is? Kunt u bestellingen telefonisch aannemen? Heeft u een papieren lijst met belangrijke klanten en leveranciers? Kan de planning tijdelijk op papier of in een ander systeem? Kunnen medewerkers doorwerken als internet uitvalt? Schrijf voor uw belangrijkste processen een eenvoudige noodoplossing op.

5. Spreek af wie beslist

Bepaal vooraf wie de leiding neemt bij een ernstig digitaal incident. Wie mag besluiten een systeem uit te schakelen? Wie belt de IT-leverancier? Wie informeert medewerkers? Wie belt belangrijke klanten? En wie bepaalt wanneer het bedrijf weer normaal gaat werken? Zet namen en telefoonnummers op één A4.

6. Kijk naar uw belangrijkste leveranciers

Uw bedrijf kan ook stilvallen doordat een leverancier wordt getroffen. Maak daarom een lijst van leveranciers waarvan u echt afhankelijk bent. Denk aan uw IT-bedrijf, cloudleverancier, softwareleverancier, telecomprovider, logistieke partner of betalingsprovider. Vraag hen bijvoorbeeld: "Wat gebeurt er met onze dienstverlening als jullie worden getroffen door een cyberincident?"

7. Maak een 'eerste uur'-kaart

Zorg dat medewerkers weten wat ze direct moeten doen als er iets ernstigs gebeurt. Bijvoorbeeld: niet zelf gaan experimenteren, verdachte computer loskoppelen, IT-beheerder bellen, verantwoordelijke binnen het bedrijf waarschuwen en vastleggen wat er is gebeurd. Zet deze instructies op één A4 en zorg dat medewerkers weten waar die ligt.

8. Test het één keer

Doe een simpele oefening: "Het internet en onze belangrijkste systemen vallen nu uit en zijn waarschijnlijk de rest van de dag niet beschikbaar. Wat doen we?" Loop met een paar medewerkers door de stappen. U ontdekt meestal binnen een half uur welke telefoonnummers, afspraken, back-ups of noodprocedures nog ontbreken. Leg het noodpakket ook offline klaar. Bewaar de belangrijkste informatie niet alleen digitaal. Maak een map of envelop met bijvoorbeeld: kritieke systemen + noodtelefoonnummers + verantwoordelijke personen + belangrijkste leveranciers + eerste-uur-instructies + alternatieve werkwijzen. Leg één exemplaar op een bekende en veilige plaats. Dan heeft u in feite al een eenvoudig digitaal noodpakket.