

## Beveiligingsmaatregelen Digitale Veiligheid

Voor midden- en kleinbedrijf

**De Risicoklassenindeling Digitale Veiligheid midden- en kleinbedrijf is een instrument waarmee een risico-inschatting op een cyberincident wordt gemaakt. Deze inschatting bepaalt in welke risicoklasse een onderneming valt. De hoogte van deze klasse leidt tot een set aan bijbehorende maatregelen.**

Dit is een pdf met alle huidige maatregelen voor risicoklasse 1 t/m 4 van de RKIDV.

Als ondernemer ben je zelf verantwoordelijk voor een goede beveiliging van je bedrijf. Digitale beveiliging is een aparte tak van sport. Daarom raden we je aan om bij bepaalde beveiligingsmaatregelen een expert in te schakelen.

De beveiligingsmaatregelen richten zich in eerste instantie op het op orde brengen en houden van een veilige basis. De maatregelen sluiten aan op de basisprincipes van het Nationaal Cyber Security Centrum. Per maatregel wordt aangegeven of de maatregel door je onderneming zelf zou kunnen (of moeten) worden uitgevoerd, of dat wordt geadviseerd dit samen met of door een erkende leverancier te (laten) doen.

Ter inspiratie is bij de samenstelling van de maatregelen gebruik gemaakt van de CIS Controls® van het Center for Internet Security®.

Note: aanvullend op de set aan beveiligingsmaatregelen van de Risicoklassenindeling Digitale Veiligheid kunnen per branche specifieke wettelijke vereisten, richtlijnen en normen van toepassing zijn op informatiebeveiliging en digitale veiligheid, zoals in de zorg en bij ondernemingen werkzaam in vitale sectoren. Deze worden in dit overzicht buiten beschouwing gelaten.

### LEGENDA



Advies om door onderneming zelf uit te voeren



Advies om door ondernemer en leverancier samen uit te voeren





Advies om door leverancier uit te voeren




Organisatie	.....
KVK	.....
Versie	1.4
Datum	februari 2026










V N O N C W













# Beveiligingsmaatregelen Risicoklasse 1



<b>1</b>	<b>Breng je risico's in kaart</b>	
	Door in kaart te brengen wat jouw kroonjuwelen zijn en hoe de toegang hiertoe is ingericht, ontdek je mogelijk zwakke plekken. Welke risico's bestaan er in en rondom belangrijke IT-systemen? Kun je deze risico's verkleinen? Goed inzicht in je risico's maakt dat je zelf een afgewogen keuze kunt maken in de te nemen maatregelen en bijbehorende investeringen om de cyberweerbaarheid te vergroten.	
	<b>Inventarisatie van kwetsbaarheden</b>	
<b>1a</b> 	Maak en onderhoud een inventarisatielijst van alle computers, software, clouddiensten, slimme apparaten etc., voorzien van bijbehorende software-versies en serienummers. Zie voor een voorbeeld bijlage 1. Maak deze inventarisatie ook als je zaken hebt uitbesteed aan een leverancier.	Actualiseer minimaal elke 12 maanden.
<b>1b</b> 	Controleer of onbekende apparaten en software in de omgeving aanwezig zijn en geef hier opvolging aan.	Controleer elke maand en volg indien nodig op.
<b>1c</b> 	Maak een inventarisatie van onderdelen en informatie die bedrijfskritisch en gevoelig zijn. Denk hierbij aan persoonsgegevens, eigen vindingen, formules, modellen en andere concurrentiegevoelige informatie.	Actualiseer minimaal elke 12 maanden.

<b>2</b>	<b>Bevorder veilig gedrag</b>	
	Het is belangrijk om veilig gedrag te stimuleren om weerbaarder te worden tegen digitale dreigingen. Dit kan door medewerkers bewust te maken van risico's, ze te trainen in het omgaan met incidenten en een cultuur te creëren waarin mensen veilig melding kunnen maken als er onverhoopt iets misgaat. Technische oplossingen kunnen hierbij helpen. Denk aan spamfilters om phishing te herkennen, inloggen in 2 stappen of het gebruik van wachtwoordmanagers. Door te investeren in je mensen maak je van hen een sterke eerste schakel in jouw cybersecurityketen.	
	<b>Organisatorische maatregelen</b>	
<b>2a</b> 	Wijs een vast contactpersoon binnen de organisatie aan voor het melden van verdachte situaties. Denk aan verlies van een laptop, een e-mail die naar de verkeerde persoon is verstuurd, misschien toch op een verdachte link geklikt etc.	Informeert nieuwe medewerkers hierover en evalueer deze maatregel jaarlijks.
<b>2b</b> 	Zorg voor duidelijke vastgelegde afspraken met je ICT-toeleveranciers met betrekking tot informatiebeveiliging.	Controleer dit bij leverancierselectie en contractverlenging.
<b>2c</b> 	Stimuleer veilig gedrag van medewerkers. Daarbij kan worden gedacht aan phishing acties, awareness filmpjes, awareness spellen.	Bij indiensttreding een awareness briefing en elke zes maanden een awareness oefening.

3	<b>Bescherm systemen, apparaten en applicaties</b> Door het gebruik van standaardinstellingen ontstaat het risico dat systemen, applicaties en apparaten toegankelijker zijn dan gewenst. Onnodige functionaliteiten vergroten bovendien het aanvalsoppervlak waardoor je organisatie meer risico loopt op beveiligingslekken. Daarom is het zinvol om te kijken naar de instellingen van de ICT-middelen die je gebruikt.	
<b>Updates</b>		
3a 	Maak een stappenplan om alle apparaten en software up-to-date te brengen. Zorg hierbij dat je weet hoe je per apparaat en per software moet updaten.	Actualiseer elke 12 maanden of bij grote wijzigingen.
3b 	Richt een proces in om op de hoogte te blijven van kritieke beveiligingsupdates (zogenaamde (nood)patches) die leveranciers uitbrengen. Voer deze zo spoedig mogelijk uit om misbruik van kwetsbaarheden te voorkomen.	Controleer maandelijks.
3c 	Schakel waar mogelijk automatische updates in zodat je apparaten en software voortaan altijd draaien op de laatste versie. Denk daarbij ook aan je eigen werkcomputer, je MS Office installatie, je modem, printer, firewall, beveiligingscamera's, deurbel, telefoons, etc. Maak afspraken met leveranciers over het installeren van updates, ook van verbonden systemen zoals: aico's, alarmssystemen en gebouwbeheersystemen. Overweeg systemen die niet met andere systemen hoeven te communiceren te isoleren doormiddel van netwerksegmentatie.	Controleer bij aanschaf/installatie.
3d 	Controleer of je eigen software op het internet up-to-date is. Denk daarbij bijvoorbeeld aan je CMS website.	Voer dit minimaal iedere maand uit.
3e 	Vervang apparaten of software als updates van leveranciers niet meer beschikbaar zijn of ondersteund worden.	Controleer elke 6 maanden of je apparaten en software nog ondersteund worden.
<b>Beveilig tegen virussen en malware</b>		
3f 	Gebruik een antivirusprogramma op de computer van de medewerkers en zorg dat deze up-to-date blijft, ook in de virus definities.	Op iedere computer geïnstalleerd en geconfigureerd om up-to-date te blijven.
3g 	Installeer apps op tablets of smartphones bewust. Installeer alleen noodzakelijke applicaties. Sommige applicaties doen meer dan je verwacht.	Bij indiensttreding een awareness briefing ,onderteken gedragscode en elke zes maanden een awareness oefening.
3h 	Gebruik veilige en moderne toepassingen om internet informatie en toepassingen te benaderen. Gebruik bijvoorbeeld zo actueel mogelijke browsers en ieder geval geen browsers die geen support meer ontvangen.	Neem dit mee bij applicatieselectie.
3i 	Maak gebruik van de beveiligingsvoorzieningen van je internetabonnement. Overweeg eventuele betaalde voorzieningen van de aanbieder. Zorg ervoor dat deze beveiliging correct is ingeschakeld.	Instellen bij nieuw abonnement en iedere zes maanden controleren of er nieuwe beveiligingsvoorzieningen bijgekomen zijn.

3j 	Gebruik een firewall. Verbind systemen nooit direct met het internet, maar zorg ervoor dat er een firewall voor staat dat ongewenste inkomende verbindingen tegenhoudt.	Gebruik de apparatuur van de telecom leverancier. Zet de firewall op de werkplek aan. De firewallsoftware en firmware worden actueel gehouden door het installeren van updates.
--	---	---

4	<b>Beheer toegang tot data en diensten</b> Het beheer van toegang moet goed geregeld zijn. Dit verkleint de kans op fouten door gebruikers. Het zorgt er ook voor dat kwaadwillenden minder kunnen doen als ze binnenkomen. Zij kunnen dan alleen bij wat past bij de rol waarmee ze zijn binnengekomen. Ook de toegang van service-accounts, machine-accounts en functionele accounts moet beperkt blijven tot wat nodig is.	
	<b>Veilige instellingen</b>	
4a 	Controleer de instellingen van jouw apparatuur, software en netwerk- en internetverbindingen. Pas standaardinstellingen aan voordat je ze aansluit op internet. Kijk kritisch naar functies en diensten die automatisch 'aan' staan, terwijl je ze misschien niet nodig hebt of gebruikt. Test je op het internet aangesloten systemen (web en e-mail), bijvoorbeeld via internet.nl.	Controleer bij aanschaf/installatie.
	<b>Toegangsbeperking</b>	
4b 	Definieer per medewerker tot welke systemen en data zij toegang zouden moeten hebben om hun werk te kunnen doen.	Bij indiensttreding, verandering van functie en uitdiensttreding van medewerkers.
4c 	Zorg er vervolgens voor dat een medewerker kan inloggen op de systemen en zich kan identificeren als die medewerker met bijbehorende toegangsrechten. Daarbij is het belangrijk dat iedere medewerker zijn eigen account heeft.	Bij indiensttreding van een nieuwe medewerker en controleer dit elke 6 maanden (bijvoorbeeld na vakanties).
4d 	Gebruik veilige en sterke wachtwoorden (minimaal 14 tekens) en realiseer inloggen door middel van tweestapsverificatie voor belangrijke systemen en data.	Implementeer bij aanschaf/installatie.
4e 	Beperk de fysieke toegang van medewerkers tot ruimtes waar systemen draaien (zoals servers) of apparaten (zoals externe harde schijven en USB-sticks) waarop documenten zijn opgeslagen.	Implementeer bij aanschaf/installatie.
4f 	Zorg dat op alle systemen een persoonlijk wachtwoord nodig is om toegang te krijgen tot het systeem.	Implementeer bij aanschaf/installatie.
4g 	Zorg dat systemen (computer, laptop, telefoons) automatisch na een aantal minuten vergrendelen (locken) zodat deze niet toegankelijk zijn voor onbevoegden.	Implementeer bij aanschaf/installatie.
4h 	Maak afspraken met medewerkers dat zij hun systeem zelf vergrendelen wanneer zij even van hun werkplek weglopen.	Bij indiensttreding van een nieuwe medewerker en controleer dit elke 6 maanden.
4i 	Zorg ervoor dat toegang tot applicaties en belangrijke data versleuteld zijn. Denk hierbij aan verbindingen naar (cloud)applicaties via https (herkenbaar aan een slotje in de webbrowser) en voor belangrijke data op systemen aan volledige schijfversleuteling (bijvoorbeeld Bitlocker).	Controleer bij aanschaf/installatie.

4j 	Zorg ervoor dat toegang tot bedrijfstoepassingen via het internet, bijvoorbeeld bij thuiswerken, altijd versleuteld zijn. Dit kan bijvoorbeeld door middel van een beveiligde VPN verbinding naar kantoor.	Maak gebruik van een beveiligde VPN oplossing op eigen apparatuur.
4k 	Beperk de installatiemogelijkheden van software op bedrijfscomputers.	Zorg ervoor dat alleen beheerders kunnen beschikken over een account met local administrator rechten op de bedrijfscomputers.



## 5 **Bereid je voor op incidenten**

Het is niet de vraag of, maar wanneer je te maken krijgt met een digitaal incident. Elke seconde telt op het moment dat je getroffen bent. Je wil dan geen tijd verliezen aan het bepalen van een strategie, die moet er al zijn. Door vooraf na te denken over hoe je reageert op incidenten, hoe je daarvan kunt herstellen en door regelmatig scenario's met digitale aanvallen te oefenen, ben je beter voorbereid op een digitaal incident.

### Weet hoe je op incidenten moet reageren




5a 	Maak, onderhoud en oefen een cyberincident-stappenplan. Zorg voor een offline contactpersonenlijst, en bereid crisiscommunicatie voor. Zie bijlage 2 voor voorbeelden van draaiboeken per onderwerp en zie tips op <a href="https://hackhelpdesk.nl">hackhelpdesk.nl</a> voor het opstellen van een draaiboek. Neem bij een incident contact op met je IT leverancier/dienstverlener en overweeg een externe cybersecurity expert in te schakelen. Denk hierbij ook aan stappen als het doen van aangifte bij de politie, het doen van een melding bij de Autoriteit Persoonsgegevens, contact opnemen met het computer emergency response team (CERT) voor je sector en als je een cyberverzekering hebt het informeren van je verzekeraar.	Actualiseer en oefen elke 12 maanden. Verandert er veel in je omgeving? Pas het cyberincident-stappenplan daarop aan en toets het een keer extra.
--	--	---










### Back-up strategie


5b 	Maak back-ups aan de hand van de inventarisatielijst en bepaal met welke frequentie dit plaats moet vinden. Neem hierbij ook applicaties en data in de cloud mee.	Zorg dat minimaal 1 back-up op een andere locatie wordt opgeslagen en dat deze back-up immutabel is.
5c 	Test terugzetten van de back-ups. Controleer daarbij de inhoud op volledigheid en correctheid. Bepaal de maximale tijd dat je data kunt missen en stem daar je testprocedure op af.	Test iedere zes maanden. Test ook of een systeem na opnieuw installeren volledig hersteld kan worden.








# Beveiligingsmaatregelen Risicoklasse 2





<b>1</b>	<b>Breng je risico's in kaart</b>	
	Door in kaart te brengen wat jouw kroonjuwelen zijn en hoe de toegang hiertoe is ingericht, ontdek je mogelijk zwakke plekken. Welke risico's bestaan er in en rondom belangrijke IT-systemen? Kun je deze risico's verkleinen? Goed inzicht in je risico's maakt dat je zelf een afgewogen keuze kunt maken in de te nemen maatregelen en bijbehorende investeringen om de cyberweerbaarheid te vergroten.	
	<b>Inventarisatie van kwetsbaarheden</b>	
<b>1a</b> 	Maak en onderhoud een inventarisatielijst van alle computers, software, clouddiensten, slimme apparaten etc., voorzien van bijbehorende software-versies en serienummers. Zie voor een voorbeeld bijlage 1. Maak deze inventarisatie ook als je zaken hebt uitbesteed aan een leverancier.	Actualiseer minimaal elke 6 maanden.
<b>1b</b> 	Controleer of onbekende apparaten en software in de omgeving aanwezig zijn en geef hier opvolging aan.	Controleer elke week en volg indien nodig op.
<b>1c</b> 	Maak een inventarisatie van onderdelen en informatie die bedrijfskritisch en gevoelig zijn. Denk hierbij aan persoonsgegevens, eigen vindingen, formules, modellen en andere concurrentiegevoelige informatie.	Actualiseer minimaal elke 6 maanden.

<b>2</b>	<b>Bevorder veilig gedrag</b>	
	Het is belangrijk om veilig gedrag te stimuleren om weerbaarder te worden tegen digitale dreigingen. Dit kan door medewerkers bewust te maken van risico's, ze te trainen in het omgaan met incidenten en een cultuur te creëren waarin mensen veilig melding kunnen maken als er onverhoopt iets misgaat. Technische oplossingen kunnen hierbij helpen. Denk aan spamfilters om phishing te herkennen, inloggen in 2 stappen of het gebruik van wachtwoordmanagers. Door te investeren in je mensen maak je van hen een sterke eerste schakel in jouw cybersecurityketen.	
	<b>Organisatorische maatregelen</b>	
<b>2a</b> 	Wijs een vast contactpersoon binnen de organisatie aan voor het melden van verdachte situaties. Denk aan verlies van een laptop, een e-mail die naar de verkeerde persoon is verstuurd, misschien toch op een verdachte link geklikt etc.	Informeert nieuwe medewerkers hierover en evalueer deze maatregel ieder half jaar.
<b>2b</b> 	Zorg voor duidelijke vastgelegde afspraken met je ICT-toeleveranciers met betrekking tot informatiebeveiliging.	Zorg dat er contracten zijn die ten grondslag liggen aan de samenwerking met leveranciers. Neem cybersecurity afspraken en rapportage van genomen maatregelen hierin op.
<b>2c</b> 	Stimuleer veilig gedrag van medewerkers. Daarbij kan worden gedacht aan phishing acties, awareness filmpjes, awareness spellen.	Bij indiensttreding een awareness briefing en elke drie maanden een awareness oefening.

3	<b>Bescherm systemen, apparaten en applicaties</b> Door het gebruik van standaardinstellingen ontstaat het risico dat systemen, applicaties en apparaten toegankelijker zijn dan gewenst. Onnodige functionaliteiten vergroten bovendien het aanvalsoppervlak waardoor je organisatie meer risico loopt op beveiligingslekken. Daarom is het zinvol om te kijken naar de instellingen van de ICT-middelen die je gebruikt.	
	<b>Updates</b>	
3a 	Maak een stappenplan om alle apparaten en software up-to-date te brengen. Zorg hierbij dat je weet hoe je per apparaat en per software moet updaten.	Actualiseer elke 12 maanden of bij grote wijzigingen.
3b 	Richt een proces in om op de hoogte te blijven van kritieke beveiligingsupdates (zogenaamde (nood)patches) die leveranciers uitbrengen. Voer deze zo spoedig mogelijk uit om misbruik van kwetsbaarheden te voorkomen.	Controleer continue/dagelijks.
3c 	Schakel waar mogelijk automatische updates in zodat je apparaten en software voortaan altijd draaien op de laatste versie. Denk daarbij ook aan je eigen werkcomputer, je MS Office installatie, je modem, printer, firewall, beveiligingscamera's, deurbel, telefoons, etc. Maak afspraken met leveranciers over het installeren van updates, ook van verbonden systemen zoals: aico's, alarmssystemen en gebouwbeheersystemen. Overweeg systemen die niet met andere systemen hoeven te communiceren te isoleren doormiddel van netwerksegmentatie.	Controleer bij aanschaf/installatie plus controle per kwartaal.
3d 	Controleer of je eigen software op het internet up-to-date is. Denk daarbij bijvoorbeeld aan je CMS website.	Voer dit minimaal iedere maand uit.
3e 	Vervang apparaten of software als updates van leveranciers niet meer beschikbaar zijn of ondersteund worden.	Controleer elke 3 maanden of je apparaten en software nog ondersteund worden.
	<b>Beveilig tegen virussen en malware</b>	
3f 	Gebruik een antivirusprogramma op de computer van de medewerkers en zorg dat deze up-to-date blijft, ook in de virus definities.	Gebruik op iedere computer een professioneel antivirusprogramma danwel endpoint-protection. Zorg voor centrale vastlegging en opvolging van incidenten.
3g 	Installeer apps op tablets of smartphones bewust. Installeer alleen noodzakelijke applicaties. Sommige applicaties doen meer dan je verwacht.	Bij indiensttreding een awareness briefing ,onderteken gedragscode en elke drie maanden een awareness oefening.
3h 	Gebruik veilige en moderne toepassingen om internet informatie en toepassingen te benaderen. Gebruik bijvoorbeeld zo actueel mogelijke browsers en ieder geval geen browsers die geen support meer ontvangen.	Neem dit mee bij applicatieselectie.
3i 	Maak gebruik van de beveiligingsvoorzieningen van je internetabonnement. Overweeg eventuele betaalde voorzieningen van de aanbieder. Zorg ervoor dat deze beveiliging correct is ingeschakeld.	Instellen bij nieuw abonnement en iedere zes maanden controleren of er nieuwe beveiligingsvoorzieningen bijgekomen zijn.

3j 	Gebruik een firewall. Verbind systemen nooit direct met het internet, maar zorg ervoor dat er een firewall voor staat dat ongewenste inkomende verbindingen tegenhoudt.	Maak je informatiestromen inzichtelijk en implementeer deze op de netwerk firewall. Controleer op uitzonderingen elke maand. Zet de firewall op de werkplek aan. De firewallsoftware en firmware worden actueel gehouden door het installeren van updates.
--	---	--

4	<b>Beheer toegang tot data en diensten</b> Het beheer van toegang moet goed geregeld zijn. Dit verkleint de kans op fouten door gebruikers. Het zorgt er ook voor dat kwaadwillenden minder kunnen doen als ze binnenkomen. Zij kunnen dan alleen bij wat past bij de rol waarmee ze zijn binnengekomen. Ook de toegang van service-accounts, machine-accounts en functionele accounts moet beperkt blijven tot wat nodig is.	
	<b>Veilige instellingen</b>	
4a 	Controleer de instellingen van jouw apparatuur, software en netwerk- en internetverbindingen. Pas standaardinstellingen aan voordat je ze aansluit op internet. Kijk kritisch naar functies en diensten die automatisch 'aan' staan, terwijl je ze misschien niet nodig hebt of gebruikt. Test je op het internet aangesloten systemen (web en e-mail). bijvoorbeeld via internet.nl.	Controleer bij aanschaf/installatie.
	<b>Toegangsbeperking</b>	
4b 	Definieer per medewerker tot welke systemen en data zij toegang zouden moeten hebben om hun werk te kunnen doen.	Bij indiensttreding, verandering van functie en uitdiensttreding van medewerkers. Toets minimaal eens per jaar of de rechten ingericht zijn zoals bedoeld.
4c 	Zorg er vervolgens voor dat een medewerker kan inloggen op de systemen en zich kan identificeren als die medewerker met bijbehorende toegangsrechten. Daarbij is het belangrijk dat iedere medewerker zijn eigen account heeft.	Bij indiensttreding van een nieuwe medewerker en controleer dit elke 6 maanden (bijvoorbeeld na vakanties).
4d 	Gebruik veilige en sterke wachtwoorden (minimaal 14 tekens) en realiseer inloggen door middel van tweestapsverificatie voor belangrijke systemen en data.	Implementeer bij aanschaf/installatie plus controle per kwartaal.
4e 	Beperk de fysieke toegang van medewerkers tot ruimtes waar systemen draaien (zoals servers) of apparaten (zoals externe harde schijven en USB-sticks) waarop documenten zijn opgeslagen.	Implementeer bij aanschaf/installatie plus controle per kwartaal.
4f 	Zorg dat op alle systemen een persoonlijk wachtwoord nodig is om toegang te krijgen tot het systeem.	Implementeer bij aanschaf/installatie plus controle per kwartaal.
4g 	Zorg dat systemen (computer, laptop, telefoons) automatisch na een aantal minuten vergrendelen (locken) zodat deze niet toegankelijk zijn voor onbevoegden.	Implementeer bij aanschaf/installatie plus controle per kwartaal.

4h 	Maak afspraken met medewerkers dat zij hun systeem zelf vergrendelen wanneer zij even van hun werkplek weglopen.	Bij indiensttreding van een nieuwe medewerker en controleer dit elke 6 maanden.
4i 	Zorg ervoor dat toegang tot applicaties en belangrijke data versleuteld zijn. Denk hierbij aan verbindingen naar (cloud)applicaties via https (herkenbaar aan een slotje in de webbrowser) en voor belangrijke data op systemen aan volledige schijfversleuteling (bijvoorbeeld Bitlocker).	Controleer bij aanschaf/installatie plus controle per kwartaal.
4j 	Zorg ervoor dat toegang tot bedrijfstoepassingen via het internet, bijvoorbeeld bij thuiswerken, altijd versleuteld zijn. Dit kan bijvoorbeeld door middel van een beveiligde VPN verbinding naar kantoor.	Maak gebruik van een beveiligde VPN oplossing op eigen apparatuur.
4k 	Beperk de installatiemogelijkheden van software op bedrijfscomputers.	Zorg ervoor dat alleen beheerders kunnen beschikken over een account met local administrator rechten op de bedrijfscomputers.



## 5 **Bereid je voor op incidenten**

Het is niet de vraag of, maar wanneer je te maken krijgt met een digitaal incident. Elke seconde telt op het moment dat je getroffen bent. Je wil dan geen tijd verliezen aan het bepalen van een strategie, die moet er al zijn. Door vooraf na te denken over hoe je reageert op incidenten, hoe je daarvan kunt herstellen en door regelmatig scenario's met digitale aanvallen te oefenen, ben je beter voorbereid op een digitaal incident.

### Weet hoe je op incidenten moet reageren




5a 	Maak, onderhoud en oefen een cyberincident-stappenplan. Zorg voor een offline contactpersonenlijst, en bereid crisiscommunicatie voor. Zie bijlage 2 voor voorbeelden van draaiboeken per onderwerp en zie tips op <a href="http://hackhelpdesk.nl">hackhelpdesk.nl</a> voor het opstellen van een draaiboek. Neem bij een incident contact op met je IT leverancier/dienstverlener en overweeg een externe cybersecurity expert in te schakelen. Denk hierbij ook aan stappen als het doen van aangifte bij de politie, het doen van een melding bij de Autoriteit Persoonsgegevens, contact opnemen met het computer emergency response team (CERT) voor je sector en als je een cyberverzekering hebt het informeren van je verzekeraar.	Actualiseer en oefen elke 12 maanden. Verandert er veel in je omgeving? Pas het cyberincident-stappenplan daarop aan en toets het een keer extra.
--	---	---









### Back-up strategie



5b 	Maak back-ups aan de hand van de inventarisatielijst en bepaal met welke frequentie dit plaats moet vinden. Neem hierbij ook applicaties en data in de cloud mee.	Pas passende maatregelen toe, bijvoorbeeld het 3-2-1 backup principe (3 kopieën van data, op 2 verschillende media, met 1 off-site), waarbij je ervoor zorgt dat in elk geval één van de back-ups immutabel is.
5c 	Test terugzetten van de back-ups. Controleer daarbij de inhoud op volledigheid en correctheid. Bepaal de maximale tijd dat je data kunt missen en stem daar je testprocedure op af.	Test iedere drie maanden. Test ook of een systeem na opnieuw installeren volledig hersteld kan worden.







# Beveiligingsmaatregelen Risicoklasse 3






<b>1</b>	<b>Breng je risico's in kaart</b>	
	Door in kaart te brengen wat jouw kroonjuwelen zijn en hoe de toegang hiertoe is ingericht, ontdek je mogelijk zwakke plekken. Welke risico's bestaan er in en rondom belangrijke IT-systemen? Kun je deze risico's verkleinen? Goed inzicht in je risico's maakt dat je zelf een afgewogen keuze kunt maken in de te nemen maatregelen en bijbehorende investeringen om de cyberweerbaarheid te vergroten.	
	<b>Inventarisatie van kwetsbaarheden</b>	
<b>1a</b> 	Maak en onderhoud een inventarisatielijst van alle computers, software, clouddiensten, slimme apparaten etc., voorzien van bijbehorende software-versies en serienummers. Zie voor een voorbeeld bijlage 1. Maak deze inventarisatie ook als je zaken hebt uitbesteed aan een leverancier.	Actualiseer minimaal elke 6 maanden.
<b>1b</b> 	Controleer of onbekende apparaten en software in de omgeving aanwezig zijn en geef hier opvolging aan.	Controleer in een continue proces en volg indien nodig op.
<b>1c</b> 	Maak een inventarisatie van onderdelen en informatie die bedrijfskritisch en gevoelig zijn. Denk hierbij aan persoonsgegevens, eigen vindingen, formules, modellen en andere concurrentiegevoelige informatie.	Actualiseer minimaal elke 3 maanden.

<b>2</b>	<b>Bevorder veilig gedrag</b>	
	Het is belangrijk om veilig gedrag te stimuleren om weerbaarder te worden tegen digitale dreigingen. Dit kan door medewerkers bewust te maken van risico's, ze te trainen in het omgaan met incidenten en een cultuur te creëren waarin mensen veilig melding kunnen maken als er onverhoopt iets misgaat. Technische oplossingen kunnen hierbij helpen. Denk aan spamfilters om phishing te herkennen, inloggen in 2 stappen of het gebruik van wachtwoordmanagers. Door te investeren in je mensen maak je van hen een sterke eerste schakel in jouw cybersecurityketen.	
	<b>Organisatorische maatregelen</b>	
<b>2a</b> 	Wijs een vast contactpersoon binnen de organisatie aan voor het melden van verdachte situaties. Denk aan verlies van een laptop, een e-mail die naar de verkeerde persoon is verstuurd, misschien toch op een verdachte link geklikt etc.	Informeert nieuwe medewerkers hierover en evalueer deze maatregel ieder kwartaal.
<b>2b</b> 	Zorg voor duidelijke vastgelegde afspraken met je ICT-toeleveranciers met betrekking tot informatiebeveiliging.	Zorg dat er contracten zijn die ten grondslag liggen aan de samenwerking met leveranciers. Neem cybersecurity afspraken en rapportage van genomen maatregelen hierin op.
<b>2c</b> 	Stimuleer veilig gedrag van medewerkers. Daarbij kan worden gedacht aan phishing acties, awareness filmpjes, awareness spellen.	Bij indiensttreding een awareness briefing en elke twee maanden een awareness oefening.

3	<b>Bescherm systemen, apparaten en applicaties</b> Door het gebruik van standaardinstellingen ontstaat het risico dat systemen, applicaties en apparaten toegankelijker zijn dan gewenst. Onnodige functionaliteiten vergroten bovendien het aanvalsoppervlak waardoor je organisatie meer risico loopt op beveiligingslekken. Daarom is het zinvol om te kijken naar de instellingen van de ICT-middelen die je gebruikt.	
	<b>Updates</b>	
3a 	Maak een stappenplan om alle apparaten en software up-to-date te brengen. Zorg hierbij dat je weet hoe je per apparaat en per software moet updaten.	Actualiseer elke 12 maanden of bij grote wijzigingen.
3b 	Richt een proces in om op de hoogte te blijven van kritieke beveiligingsupdates (zogenaamde (nood)patches) die leveranciers uitbrengen. Voer deze zo spoedig mogelijk uit om misbruik van kwetsbaarheden te voorkomen.	Controleer continue/dagelijks.
3c 	Schakel waar mogelijk automatische updates in zodat je apparaten en software voortaan altijd draaien op de laatste versie. Denk daarbij ook aan je eigen werkcomputer, je MS Office installatie, je modem, printer, firewall, beveiligingscamera's, deurbel, telefoons, etc. Maak afspraken met leveranciers over het installeren van updates, ook van verbonden systemen zoals: aico's, alarmssystemen en gebouwbeheersystemen. Overweeg systemen die niet met andere systemen hoeven te communiceren te isoleren doormiddel van netwerksegmentatie.	Controleer bij aanschaf/installatie plus controle per kwartaal.
3d 	Controleer of je eigen software op het internet up-to-date is. Denk daarbij bijvoorbeeld aan je CMS website.	Voer dit minimaal iedere maand uit.
3e 	Vervang apparaten of software als updates van leveranciers niet meer beschikbaar zijn of ondersteund worden.	Controleer elke 3 maanden of je apparaten en software nog ondersteund worden.
	<b>Beveilig tegen virussen en malware</b>	
3f 	Gebruik een antivirusprogramma op de computer van de medewerkers en zorg dat deze up-to-date blijft, ook in de virus definities.	Gebruik op iedere computer een professioneel antivirusprogramma danwel endpoint-protection. Zorg voor centrale vastlegging en opvolging van incidenten.
3g 	Installeer apps op tablets of smartphones bewust. Installeer alleen noodzakelijke applicaties. Sommige applicaties doen meer dan je verwacht.	Bij indiensttreding een awareness briefing ,onderteken gedragscode en elke twee maanden een awareness oefening.
3h 	Gebruik veilige en moderne toepassingen om internet informatie en toepassingen te benaderen. Gebruik bijvoorbeeld zo actueel mogelijke browsers en ieder geval geen browsers die geen support meer ontvangen.	Neem dit mee bij applicatieselectie.

3i 	Maak gebruik van de beveiligingsvoorzieningen van je internetabonnement. Overweeg eventuele betaalde voorzieningen van de aanbieder. Zorg ervoor dat deze beveiliging correct is ingeschakeld.	Instellen bij nieuw abonnement en iedere zes maanden controleren of er nieuwe beveiligingsvoorzieningen bijgekomen zijn.
3j 	Gebruik een firewall. Verbind systemen nooit direct met het internet, maar zorg ervoor dat er een firewall voor staat dat ongewenste inkomende verbindingen tegenhoudt.	Maak je informatiestromen inzichtelijk en implementeer deze op de netwerk firewall. Controleer op uitzonderingen elke maand. Zet de firewall op de werkplek aan. De firewallsoftware en firmware worden actueel gehouden door het installeren van updates.

4	<b>Beheer toegang tot data en diensten</b> Het beheer van toegang moet goed geregeld zijn. Dit verkleint de kans op fouten door gebruikers. Het zorgt er ook voor dat kwaadwillenden minder kunnen doen als ze binnenkomen. Zij kunnen dan alleen bij wat past bij de rol waarmee ze zijn binnengekomen. Ook de toegang van service-accounts, machine-accounts en functionele accounts moet beperkt blijven tot wat nodig is.	
	<b>Veilige instellingen</b>	
4a 	Controleer de instellingen van jouw apparatuur, software en netwerk- en internetverbindingen. Pas standaardinstellingen aan voordat je ze aansluit op internet. Kijk kritisch naar functies en diensten die automatisch 'aan' staan, terwijl je ze misschien niet nodig hebt of gebruikt. Test je op het internet aangesloten systemen (web en e-mail). bijvoorbeeld via internet.nl.	Controleer bij aanschaf/installatie.
	<b>Toegangsbeperking</b>	
4b 	Definieer per medewerker tot welke systemen en data zij toegang zouden moeten hebben om hun werk te kunnen doen.	Bij indiensttreding, verandering van functie en uitdiensttreding van medewerkers. Toets minimaal eens per jaar of de rechten ingericht zijn zoals bedoeld.
4c 	Zorg er vervolgens voor dat een medewerker kan inloggen op de systemen en zich kan identificeren als die medewerker met bijbehorende toegangsrechten. Daarbij is het belangrijk dat iedere medewerker zijn eigen account heeft.	Bij indiensttreding van een nieuwe medewerker en controleer dit elke 6 maanden (bijvoorbeeld na vakanties).
4d 	Gebruik veilige en sterke wachtwoorden (minimaal 14 tekens) en realiseer inloggen door middel van tweestapsverificatie voor belangrijke systemen en data.	Implementeer bij aanschaf/installatie plus maandelijkse controle.
4e 	Beperk de fysieke toegang van medewerkers tot ruimtes waar systemen draaien (zoals servers) of apparaten (zoals externe harde schijven en USB-sticks) waarop documenten zijn opgeslagen.	Implementeer bij aanschaf/installatie plus maandelijkse controle.
4f 	Zorg dat op alle systemen een persoonlijk wachtwoord nodig is om toegang te krijgen tot het systeem.	Implementeer bij aanschaf/installatie plus maandelijkse controle.



4g 	Zorg dat systemen (computer, laptop, telefoons) automatisch na een aantal minuten vergrendelen (locken) zodat deze niet toegankelijk zijn voor onbevoegden.	Implementeer bij aanschaf/installatie plus maandelijkse controle.
4h 	Maak afspraken met medewerkers dat zij hun systeem zelf vergrendelen wanneer zij even van hun werkplek weglopen.	Bij indiensttreding van een nieuwe medewerker en controleer dit elke 6 maanden.
4i 	Zorg ervoor dat toegang tot applicaties en belangrijke data versleuteld zijn. Denk hierbij aan verbindingen naar (cloud)applicaties via https (herkenbaar aan een slotje in de webbrowser) en voor belangrijke data op systemen aan volledige schijfversleuteling (bijvoorbeeld Bitlocker).	Controleer bij aanschaf/installatie plus maandelijkse controle.
4j 	Zorg ervoor dat toegang tot bedrijfstoepassingen via het internet, bijvoorbeeld bij thuiswerken, altijd versleuteld zijn. Dit kan bijvoorbeeld door middel van een beveiligde VPN verbinding naar kantoor.	Maak gebruik van een beveiligde VPN oplossing op eigen apparatuur.
4k 	Beperk de installatiemogelijkheden van software op bedrijfscomputers.	Zorg ervoor dat alleen beheerders kunnen beschikken over een account met local administrator rechten op de bedrijfscomputers.

<b>5</b>	<b>Bereid je voor op incidenten</b>
<p>Het is niet de vraag of, maar wanneer je te maken krijgt met een digitaal incident. Elke seconde telt op het moment dat je getroffen bent. Je wil dan geen tijd verliezen aan het bepalen van een strategie, die moet er al zijn. Door vooraf na te denken over hoe je reageert op incidenten, hoe je daarvan kunt herstellen en door regelmatig scenario's met digitale aanvallen te oefenen, ben je beter voorbereid op een digitaal incident.</p>	

<b>Weet hoe je op incidenten moet reageren</b>	
--	--

5a 	Maak, onderhoud en oefen een cyberincident-stappenplan. Zorg voor een offline contactpersonenlijst, en bereid crisiscommunicatie voor. Zie bijlage 2 voor voorbeelden van draaiboeken per onderwerp en zie tips op <a href="http://hackhelpdesk.nl">hackhelpdesk.nl</a> voor het opstellen van een draaiboek. Neem bij een incident contact op met je IT leverancier/dienstverlener en overweeg een externe cybersecurity expert in te schakelen. Denk hierbij ook aan stappen als het doen van aangifte bij de politie, het doen van een melding bij de Autoriteit Persoonsgegevens, contact opnemen met het computer emergency response team (CERT) voor je sector en als je een cyberverzekering hebt het informeren van je verzekeraar.	Actualiseer en oefen elke 12 maanden. Verandert er veel in je omgeving? Pas het cyberincident-stappenplan daarop aan en toets het een keer extra.
--	---	---

<b>Back-up strategie</b>	
--------------------------	--

5b 	Maak back-ups aan de hand van de inventarisatielijst en bepaal met welke frequentie dit plaats moet vinden. Neem hierbij ook applicaties en data in de cloud mee.	Pas passende maatregelen toe, bijvoorbeeld het 3-2-1 backup principe (3 kopieën van data, op 2 verschillende media, met 1 off-site), waarbij je ervoor zorgt dat in elk geval één van de back-ups immutabel is
5c 	Test terugzetten van de back-ups. Controleer daarbij de inhoud op volledigheid en correctheid. Bepaal de maximale tijd dat je data kunt missen en stem daar je testprocedure op af.	Test iedere drie maanden. Test ook of een systeem na opnieuw installeren volledig hersteld kan worden.

---

## CYRA

Heb je de digitale basis op orde en wil je een stap verder?  
Ontdek de CYRA-methode. [Klik hier](#)

# Beveiligingsmaatregelen Risicoklasse 4

**Volgens de risicobepaling behoort je onderneming tot risicoklasse 4. Dat betekent een hoog risico. De aard van je onderneming en de daarbij behorende risico's vragen om een maatwerkoplossing.**

Naast algemene beveiligingsmaatregelen zijn er ook specifieke, aanvullende maatregelen noodzakelijk. Het gaat om beveiligingsmaatregelen die speciaal zijn afgestemd op jouw situatie en die naadloos aansluiten op het risicoprofiel van je onderneming. Om te bepalen welke maatregelen onmisbaar zijn voor

de digitale beveiliging van je onderneming, raden we je aan een (externe) expert in te schakelen. Samen met deze Cybersecurity-deskundige bepaal je welke beveiligingsmaatregelen je minimaal moet nemen om je onderneming adequaat te beschermen tegen cyberincidenten.

Als je een cyberverzekering hebt of overweegt deze aan te schaffen, dan kun je ook met je verzekeraar en/of tussenpersoon overleggen over wat de beste aanpak is.

## CYRA

**Heb je de digitale basis op orde en wil je een stap verder?  
Ontdek de CYRA-methode. [Klik hier](#)**