Een bestuursmanifest

voor informatieveiligheid

Maart, 2020 [v1.1]

Titel	Een bestuursmanifest voor informatieveiligheid
Opdrachtgever	Centrum Informatiebeveiliging en Privacybescherming
Status	Versie 1.1
Auteurs en reviewers	CIP: Leden van de CIP-Domeingroep
Bijdrage van	
Datum	20 maart 2020
Filenaam	

Considerans

Met het doel informatie-uitwisseling en kennisdeling te bevorderen wil CIP onder andere 'good practices' ter beschikking stellen. Dit kunnen praktijkvoorbeelden zijn, handreikingen voor beleid, beschrijvingen van de stand van zaken in bepaalde ontwikkelingen, en dergelijke. De herkomst is van oorsprong een reflectie op een onderwerp door mensen uit de CIP-netwerk, maar het kunnen ook notities zijn uit de praktijk van de CIP-organisaties die zonder verder commentaar worden gepubliceerd. De kern is dat de bijdragen altijd zijn gebaseerd op de expertise van de opstellers en deelnemende reviewers en/of het idee dat wat in één organisatie goed werkt, ook voor andere organisaties nuttig kan zijn. Soms is het resultaat dus de uitkomst van een groepsproces en in andere gevallen wordt iets 'as is' ter kennisneming of overname aangeboden. CIP heeft categorieën geformuleerd waarmee reikwijdte, intentie, status en/of draagvlak van CIP-publicaties wordt aangegeven. Een nadere uitleg hiervan staat op www.cip-overheid.nl.

De CIP-documenten hebben geen ander doel dan kennisoverdracht en reflecteren niet noodzakelijk de opvattingen van alle contribuanten, CIP-deelnemers en/of alle CIP-partijen. Publicatie vindt plaats op zowel de openbare website www.cip-overheid.nl als de besloten community site cip.pleio.nl.

Principes voor informatieveiligheid

Het thema Informatiebeveiliging is de laatste jaren sterk op de voorgrond gekomen. Door de toegenomen digitalisering zijn onze de kwetsbaarheden toegenomen en zal permanente aandacht nodig blijven voor informatieveiligheid. Terwijl we weten dat Informatieveiligheid een zaak is van de business/de lijnorganisatie en daarmee is verankerd in de bestuursverantwoordelijkheid van de organisatie, zien we tevens dat dit vakgebied is doortrokken van vakjargon en dat het vele technische specialismen omvat. In het algemeen geldt dat dit niet op natuurlijke wijze aansluit bij de wereld van de bestuurder. De VNG-IBD heeft tien principes opgesteld die behulpzaam kunnen zijn bij het beantwoorden van de vraag hoe de bestuurder zich kan verhouden tot het thema informatieveiligheid. Het zijn tips die hij kan gebruiken bij de invulling van zijn rol. Het document is te vinden achter de volgende link: https://www.informatiebeveiligingsdienst.nl/product/de-10-bestuurlijke-principes-voor-informatiebeveiliging/.

In onderstaande vijf ik-boodschappen zijn de tien principes gebundeld tot een 'manifest' dat de rol van de bestuurder bij Informatieveiligheid kort samenvat.

1. Ik bevorder een veilige cultuur

Ik ben mij bewust van de voorbeeldfunctie van een bestuurder en ik draag uit dat risicomanagement van iedereen is. Ik zorg daarom voor een cultuur waarin iedereen vrij is om dreigingen waar te nemen en te melden. In eerste instantie bij de verantwoordelijke, maar indien nodig ook bij mij als bestuurder. Ik spoor managers aan om voorwaarden te scheppen zodat iedereen binnen de organisatie deelgenoot wordt van het proces van risicomanagement. Ik zorg ervoor dat fouten besproken kunnen worden en dat daarmee een lerende organisatie ontstaat. Ten slotte geef ik in mijn eigen doen en laten het goede voorbeeld van hoe je verantwoordelijk omgaat met informatie.

2. Ik stel risicomanagement centraal

Ik zorg ervoor dat risicomanagement geformaliseerd wordt binnen de hele organisatie en in de ketens waarin wij werken, met een duidelijke verdeling van verantwoordelijkheden en heldere besluitvorming. Ik draag er zorg voor dat besluiten ten aanzien van de omgang met risico's expliciet genomen en vastgelegd worden. Ik laat risicomanagement naadloos aansluiten op de strategische en beleidsmatige doelstellingen van de organisatie. Op deze wijze bied ik een duidelijk kader waarbinnen mijn medewerkers kunnen opereren.

3. Ik zie informatiebeveiliging als een proces

Ik zorg ervoor dat risicomanagement cyclisch is en daarmee kan ik reageren op veranderingen en toekomstgericht sturen. Het staat daarom regelmatig op de agenda. Hiermee adresseer ik het gegeven dat omstandigheden en dientengevolge risico's voortdurend wijzigen en regelmatig nopen

tot her-evaluatie. Daarnaast bevorder ik hiermee ook het proces van leren en verbeteren in de organisatie.

4. Ik zorg voor toereikend budget

Ik zorg ervoor dat er voldoende resources beschikbaar zijn om de onderkende risico's op een adequate manier te behandelen. Als gebleken is dat een risico een bedreiging is voor de organisatie doelstellingen en er maatregelen genomen moeten worden, dan zorg ik er ook voor dat de middelen beschikbaar zijn of komen om deze maatregelen uit te voeren.

5. Ik controleer en evalueer

Ik controleer actief binnen mijn organisatie doordat ik opdracht geef om de werking van risicomanagement binnen mijn organisatie op effectiviteit en efficiency te (laten) controleren. Naast management rapportages zijn (externe) controles de manier om te weten te komen of en hoe mijn uitgedragen beleid in de praktijk werkt. Als bestuurder weeg ik goed geïnformeerd risico's en belangen af en neem ik mijn verantwoordelijkheid om knopen door te hakken.