

dialogic

Onderzoek voor *onderbouwd* beleid.



Dialogic innovatie & interactie

Informatiebeveiligingsbeleid

Versie:

1.0

Goedgekeurd door management:

Per 1 juli 2026

Inhoud

1	Context en doelen	3
2	Scope	3
3	Stakeholderanalyse	4
4	Leiderschap	4
5	Middelen, awareness en training	5
6	Planning	5
7	Prestatie-evaluatie	6
8	Continue verbetering	6
	Colofon	6

1 Context en doelen

Dit beleidsdocument beschrijft het informatiebeveiligingsmanagementsysteem (ISMS) dat onze organisatie gebruikt. Iedereen in onze organisatie (of op sleutelposities bij leveranciers) die vertrouwelijke of gevoelige gegevens verwerkt, moet op de hoogte zijn van dit beleid en handelen in overeenstemming met het beleid. Als iemand iets waarneemt dat niet in overeenstemming is met dit beleid, moet hij of zij dit onmiddellijk melden. Dit kan worden gedaan door ons Informatiebeveiligingsteam op de hoogte te stellen.

Het volledige managementteam van ons bedrijf is betrokken bij het opstellen van dit beleid, en zet zich volledig in om ervoor te zorgen dat we ons aan de regels houden.

Over Dialogic

Dialogic *innovatie & interactie* vof (hierna: Dialogic) is een onafhankelijk onderzoeks- en adviesbureau dat werkt aan vraagstukken in het publieke domein. Wij ondersteunen overheden, kennisinstellingen en intermediaire organisaties door middel van beleidsonderzoek en strategisch advies. Daarnaast ontwikkelen en implementeren we innovatieve methoden voor dataverzameling, data-analyse en datavisualisatie.

Dialogic is eigendom van, en wordt geleid door, de partners van Dialogic. Zij werken naast hun managementtaken op dagelijkse basis mee aan onderzoeksprojecten. Met deze structuur kunnen we onafhankelijk blijven opereren en borgen we dat kwaliteit van ons onderzoek voorop blijft staan. Het managementteam (MT) heeft de dagelijkse leiding.

2 Scope

De scope van het ISMS is: **informatiebeveiliging gerelateerd aan het uitvoeren van onderzoeks- en adviesprojecten en het leveren van onderzoeksproducten.**

In deze scope bieden wij de volgende hoofdactiviteiten en diensten aan klanten:

- Het uitvoeren van onderzoeks- en adviesprojecten, waarin sprake kan zijn van gegevensverzameling en -verwerking.
- Het leveren van producten op basis van onderzoeksresultaten, zoals rapporten en online dashboards.

De volgende afdelingen zijn in scope van dit beleid:

- Alle onderzoekers van Dialogic (er zijn geen afdelingen)

Op dit moment zijn er geen afdelingen of bedrijfsactiviteiten specifiek buiten de scope van dit beleid verklaard. Ons bedrijf heeft de volgende kantoorlocaties en werklocaties die binnen het bereik van dit beleid vallen:

- Hoofdkantoor: Hooghiemstraplein 33, 3514 AX Utrecht.
- Werkplekken op afstand (zoals thuis) van medewerkers

Dialogic managet haar data (niet) volledig direct. Microsoft 365 wordt gebruikt voor de kern van de kantoorautomatisering. Dialogic heeft daarnaast enkele eigen applicaties in beheer, op basis van (virtuele) servers bij een leverancier. Daarnaast is er ICT-infrastructuur aanwezig op het kantoor van Dialogic.

3 Stakeholderanalyse

Het managementteam (MT) is verantwoordelijk voor het onderhouden van regelmatig contact met belanghebbenden, het begrijpen van de informatiebeveiligingseisen en verwachtingen van belanghebbenden en ervoor te zorgen dat het ISMS hierop is afgestemd. De resulterende informatie is gedocumenteerd in de stakeholderanalyse, die jaarlijks zal worden bijgewerkt.

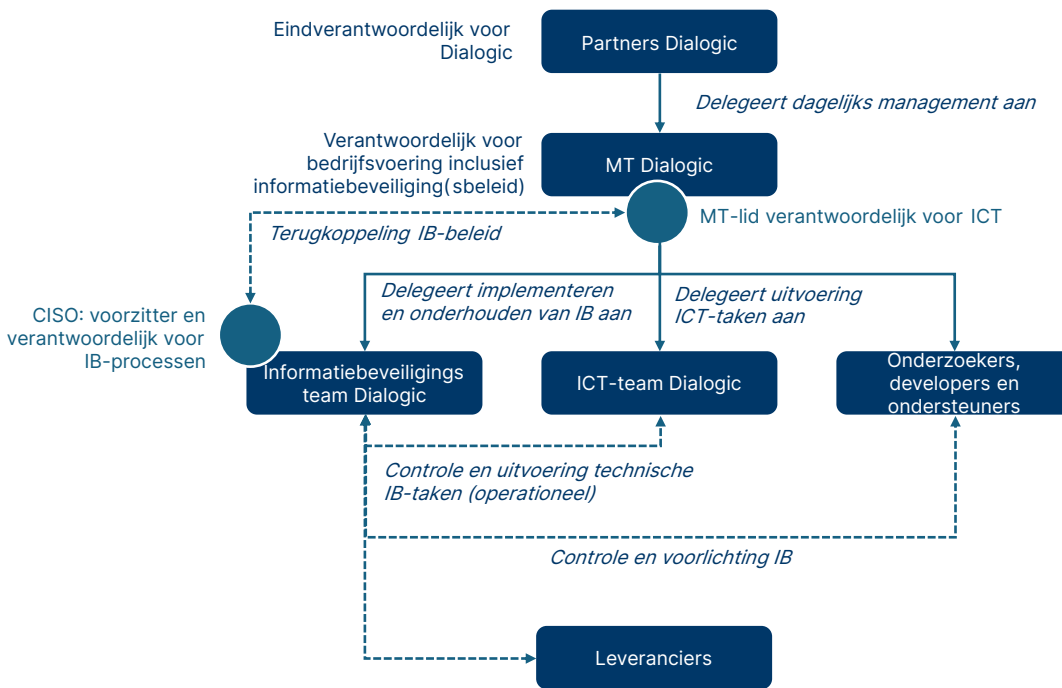
4 Leiderschap

Het gehele management is op de hoogte van het informatiebeveiligingsbeleid en is vastbesloten om deze inspanning op permanente basis te ondersteunen.

De partners van Dialogic zijn eindverantwoordelijk voor de informatiebeveiliging. Het dagelijks management is gedelegeerd naar het managementteam (MT). Daarvan is één MT-lid verantwoordelijk voor ICT. De verantwoordelijkheid voor informatiebeveiligingsprocessen is belegd bij de CISO (*information security officer*).

Er is een Informatiebeveiligingsteam dat verantwoordelijk is voor het implementeren en onderhouden van informatiebeveiliging. De verantwoordelijkheden van dit team en andere rollen zijn vastgelegd. Het Informatiebeveiligingsteam wordt geleid door de CISO.

Alle personeelsleden van de organisatie worden regelmatig ingelicht door het informatiebeveiligingsteam en zijn verantwoordelijk voor het volgen van het beleid en de richtlijnen.



5 Middelen, awareness en training

Het management is ervoor verantwoordelijk dat alle medewerkers kennis hebben van hun verantwoordelijkheden ten aanzien van informatiebeveiliging, en hoe deze in te vullen. Bij indiensttreding ontvangen zij daarom een (online) *security awareness*-training. De training wordt jaarlijks herhaald voor alle medewerkers.

Voor medewerkers die (geprivilegieerde) informatiebeveiligingstaken uitvoeren (het ICT-team) zijn specifieke werkinstructies opgesteld. Voor aanvang van de werkzaamheden worden zij getraind. Jaarlijks wordt de training herhaald.

6 Planning

Het management stelt doelen en KPI's vast om de effectiviteit van het ISMS te meten. De CISO initieert en faciliteert dit proces.

De CISO zorgt ervoor dat de metingen worden uitgevoerd, en zorgt dat meetresultaten worden besproken in het MT.

Er is een jaarplanning waarin terugkerende overleggen en acties zijn vastgelegd.

7 Prestatie-evaluatie

Het MT zal de effectiviteit van het ISMS jaarlijks beoordelen in een *management review*.

Indien nodig zal ondersteuning door externe partners worden gezocht, zoals aanvullend technisch advies, onafhankelijke beveiligingstests of audits door onafhankelijke partijen.

8 Continue verbetering

Het management is eraan gecommitteerd om het ISMS continu te verbeteren. Dit wordt gedaan door belanghebbenden te documenteren en te analyseren en externe bronnen van expertise te raadplegen.

Colofon

Dit document is gebaseerd op een sjabloon van ICT Institute, dat met toestemming is gebruikt. De auteursrechten liggen voor het overige volledig bij Dialogic.

Eenieder die het document leest wordt uitgenodigd vragen, voorstellen ter verbetering, of signalen over de naleving van het beleid te melden bij de CISO.

Foto voorblad: Dialogic (Tommy van der Vorst).

dialogic

Onderzoek voor *onderbouwd* beleid.

Dialogic innovatie & interactie

Hooghiemstraplein 33

3514 AX Utrecht

030-2150580

www.dialogic.nl