

Informatie-beveiligingsbeleid

[BEDRIJF]

Versie: 0.5

Goedgekeurd door management: NOG NIET GOEDGEKEURD

# Context en doelen

[BESCHRIJVING BEDRIJF]

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. Ook als iemand iets in ons bedrijf waarneemt dat niet in overeenstemming is met dit beleid, moet hij of zij dit onmiddellijk melden. Dit kan worden gedaan door onze Security Officer of een lid van het beveiligingsteam op de hoogte te stellen. Het volledige managementteam van ons bedrijf is betrokken geweest bij het opstellen van dit beleid en zet zich volledig in om ervoor te zorgen dat we ons aan de regels houden.

# Scope

De scope van het ISMS is:

Informatiebeveiliging gerelateerd aan het maken/leveren van XYZ aan …

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

* A
* B
* C

De volgende afdelingen zijn in scope van dit beleid:

* A
* B
* C
* D

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: [ADDRES]
* B
* C

[BEDRIJF] managet haar data centrum (niet) direct. Amazon Web Services/Azure/Google Cloud/IBM wordt gebruikt als leverancier van de IT infrastructuur.

# Stakeholder analyse

Het managementteam 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.

# Leiderschap

Het gehele management is op de hoogte van het informatiebeveiligingsbeleid en is vastbesloten om deze inspanning op permanente basis te ondersteunen. [MGMT\_VERANTW] is de managementvertegenwoordiger die rechtstreeks in contact staat met het beveiligingsteam.

Er is een informatiebeveiligingsteam (IB-team) dat verantwoordelijk is voor het implementeren en onderhouden van informatiebeveiliging. De verantwoordelijkheden van het informatiebeveiligingsteam en andere rollen zijn vastgelegd.

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

# Middelen, awareness en training

Het management is ervoor verantwoordelijk dat werknemers die informatiebeveiligingstaken uitvoeren uitgebreide kennis hebben van de onderwerpen waaraan zij werken. Ze krijgen een security awareness training na het afsluiten van het contract en daarna weer minstens één keer per jaar. Medewerkers die betrokken zijn bij het ontwerpen en ontwikkelen van producten of personeel met extra beveiligingsverantwoordelijkheden zullen extra training krijgen die geschikt is voor hun rol.

# Planning

Het IB-team en management stelt doelen en KPI’s vast om de effectiviteit van het ISMS te meten. Het IB-team voert de metingen uit en zorgt dat meetresultaten worden besproken. Er is een jaarplanning waarin terugkerende overleggen en acties zijn vastgelegd.

# Prestatie evaluatie

Het managementteam 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.

# Continue verbetering

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

# Over dit template

Dit template is gemaakt door de mensen van ICT Institute.

Het template mag gratis worden gebruikt, onder een creative commons licentie

https://creativecommons.org/licenses/by/4.0/

De nieuwste versie staat op:

https://softwarezaken.nl/2022/01/gratis-27001-avg-templates/

Je mag het template uitbreiden, aanpassen en bewerken zoveel je wilt

Je mag het template en documenten gemaakt met het template doorgeven en delen zoveel je wilt

Als je het template doorgeeft, dan moet je "gemaakt door de mensen van ICT Institute" laten staan

Als je een document maakt met dit template en je bent geen opdrachtgever van ons, zet dat "gemaakt met template van ICT Institute" ergens in het document

Als je een opdrachtgever bent van ICT Institute, dan mag je alles doen met dit template wat je wilt

Let op dat je de ISO 27001 norm moet kopen bij NEN of een andere organisatie voordat je de norm gaat gebruiken. De norm is auteursrechtelijk beschermd.

Lees vooral ook deze artikelen als je aan de slag gaat:

<https://softwarezaken.nl/2017/03/samenvatting-iso-27001-informatie-beveiliging/>

<https://softwarezaken.nl/2021/12/iso-27001-certificatie-aanvraag/>

<https://softwarezaken.nl/2018/01/gdpr-avg-in-10-stappen/>

<https://softwarezaken.nl/security-verified/>