Informatiebeveiligingsbeleid

V1.0 – goedgekeurd door directie op 9 juli 2021

ICT Institute
Kees van Bohemenhof 24
3544 MC Utrecht
www.ictinstitute.nl
@ictinl

1 Context en doelen

ICT Institute is een adviesbureau voor objectief en onafhankelijk IT-advies. Ons doel is altijd om te zorgen dat IT op de juist manier wordt ingezet. De kennisgebieden van ICT Institute zijn IT-security, Privacy, Agile & scrum en Deskundigenonderzoek.

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. De directie 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.

2 Scope

Het toepassingsgebied (de scope) van het informatiebeveiligingsbeleid en bijbehorend ISMS van ICT Institute is als volgt gedefinieerd:

> *Het beveiligen van informatie gerelateerd aan het verlenen van advies (consultancy), uitvoeren van onderzoek, geven van trainingen en ondersteunende processen.*

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

- workshops en training;
- onderzoek en advies;
- deskundigen-onderzoek; en
- IT due diligence.

Het beleid richt zich op de eigen medewerkers, personeel niet in loondienst (freelancers) en stagiaires. Er is geen afdeling of bedrijfsactiviteit specifiek buiten de scope van dit beleid verklaard. Ons bedrijf heeft de volgende locatie die binnen het bereik van dit beleid valt:

- Kantoor: Europalaan 400, Utrecht

Binnen deze scope vallen tot slot alle IT systemen van ICT Institute waar klantinformatie in staat.

3 Stakeholder analyse

De directie 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

De directie is op de hoogte van het informatiebeveiligingsbeleid en is vastbesloten om deze inspanning op permanente basis te ondersteunen. Er is een informatiebeveiligingsteam (IB-team) dat verantwoordelijk is voor het implementeren en onderhouden van informatiebeveiliging.

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

5 Middelen, awareness en training

De directie 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.

6 Doelstellingen

Er zullen in het eerste kwartaal van elk jaar concrete doelstellingen en KPI's worden vastgelegd in een strategie-document. Bij het vaststellen van de doelstellingen en KPI's worden informatiebeveiligingsaspecten meegenomen, waaronder het voldoen aan wet- en regelgeving, minimaliseren van incidenten, voldoen aan eisen en verwachtingen stakeholders en continue verbetering.

7 Prestatie evaluatie

De directie zal de effectiviteit van het ISMS jaarlijks beoordelen in een directiebeoordeling. Indien nodig zal ondersteuning door externe partners worden gezocht, zoals aanvullend technisch advies, onafhankelijke beveiligingstests of audits door onafhankelijke partijen.

8 Continue verbetering

De directie 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.