Belangrijke informatiebeveiligingsspeerpunten voor CINOP

Het CINOP-informatiebeveiligingssysteem, dat is opgezet vanuit ISO 27001:2017, is zodanig ontworpen dat de bedrijfsvoering met al haar processen continu kan worden beheerst en verbeterd. De PDCA-cyclus (Plan Do Check Act) passen we hierop toe. Dit sluit aan op het doel van CINOP om continu kwaliteit te verbeteren en te voldoen aan de eisen van ISO 9001.

Directie en bestuur stellen zich tot doel om dit beleid te concretiseren en bewustwording van het belang van kwaliteit van dienstverlening én informatiebeveiliging te ontwikkelen. Dit doen we binnen de organisatie en in contact met samenwerkingspartners en opdrachtgevers.

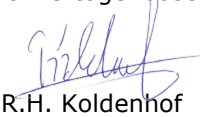
Wij hanteren de volgende uitgangspunten:

- CINOP verankert informatiebeveiliging en privacybescherming in processen en in het denken en doen.
- CINOP geeft het informatiebeveiligingsbeleid vorm aan de hand van de volgende waarden: beschikbaarheid, integriteit en vertrouwelijkheid.
- CINOP vindt het belangrijk dat maatregelen op de mogelijke risico's gebaseerd worden; wet- en regelgeving is naast de CINOP Strategiekaart en het cyberdreigingsbeeld, de basis voor het identificeren van risico's.
- CINOP vindt het belangrijk dat bij medewerkers op het gebied van informatiebeveiliging in kennis en bewustzijn geïnvesteerd wordt.
- CINOP vindt het belangrijk dat medewerkers zich verantwoordelijk voelen voor het omgaan met het beleid en werken volgens de richtlijnen en alle aspecten van informatiebeveiliging en privacy binnen de eigen invloedssfeer.
- CINOP vindt het belangrijk dat wanneer er sprake is van een detacheringsconstruct bij een externe opdrachtgever dat de medewerker zich houdt aan de informatiebeveiligingsprocedures en -protocollen van de externe opdrachtgever en hier opvolging aan geeft.
- CINOP vindt het belangrijk dat informatie die zich in onze organisatie bevindt beveiligd is tegen datalekken en andere dreigingen.
- CINOP vindt het belangrijk dat informatie afgeschermd is en alleen specifiek voor gebruikers opengezet wordt op basis van het 'need to know'-principe.
- CINOP vindt het belangrijk dat informatie geclassificeerd en versleuteld is.
- CINOP vindt het belangrijk dat informatie door een reservekopie is veiliggesteld.

Het IB-beleid volgt de kaders van het meerjarenbeleid van CINOP, het wordt jaarlijks geëvalueerd en bijgesteld en maakt daarmee onderdeel uit van de PDCA-cyclus. Ook belangrijke ontwikkelingen op cyber-beveiligingsgebied kunnen aanleiding zijn om het beleid te worden herzien.

Door verbeteren van maatregelen voor risico's en leven lang ontwikkelen zorgt CINOP voor een veilige samenwerkingsomgeving.

's-Hertogenbosch, 12 juni 2023



R.H. Koldenhof
Bestuurder Stichting CINOP-ecbo