ISD Noordoost

Samenvatting
Informatiebeveiligingsbeleid ISD Noordoost

Doelstelling Informatiebeveiligingsbeleid

ISD Noordoost biedt met haar Informatiebeveiligingsbeleid een juiste basis om verantwoord om te gaan met de aan haar toevertrouwde gegevens, een veilige werkplek voor haar medewerkers en het adequaat waarborgen van de continuïteit van haar bedrijfsprocessen en dienstverlening.

Afwegingen risico's

Onderstaand zijn de belangrijkste onderkende risico's voor ISD Noordoost.

- Onbevoegde inzage in, en kennisneming van gegevens en informatie.
- Aantasting veiligheid van medewerkers.
- Fraude of ontvreemding met middelen, zowel financiën als bedrijfsmiddelen.
- Negatieve meldingen in de pers.

Kernpunten Informatiebeveiligingsbeleid

Het Informatiebeveiligingsbeleid gaat uit van de norm NEN-ISO/IEC 27002:2007nl. Verder zijn belangrijke aspecten van wet- en regelgeving opgenomen.
Onderstaand zijn de kernpunten van het Informatiebeveiligingsbeleid.

1. Beveiligingsbeleid:
   - Goedgekeurd en door directie en management ondersteund beleid voor beveiliging.
   - Bekend bij, en nageleefd door de medewerkers.
   - Regelmatige beoordeling, evaluatie en (indien nodig) aanpassing.
2. Organisatie van Informatiebeveiliging:
   - Organisatie met interne functionaris en coördinatoren.
   - Samenwerken met partners uit publieke sector.
   - Betrekken van derde partijen, inclusief leveranciers.
3. Beheer van bedrijfsmiddelen:
   - Inventariseren van de bedrijfsmiddelen.
   - Vastleggen van eigendom, verantwoordelijkheden en regels over gebruik.
   - Classificeren van informatie, onder meer zoals aangegeven in WBP en SUWI.
4. Beveiliging van personeel:
   - In alle stadia van het dienstverband voldoende aandacht voor beveiliging.
5. Fysieke beveiliging en beveiliging van de omgeving:
   - Fysieke beveiliging betrekken op personeel en ruimten.
   - Fysieke beveiliging van apparatuur en informatiesystemen.
6. Beheer van communicatie- en bedieningsprocessen:
   - Procedures en verantwoordelijkheden voor bediening van informatiesystemen, inclusief toepassing van functiescheiding.
   - Dienstverlening door derde partij is in lijn met het informatiebeveiligingsbeleid.
   - Juist omgaan met herstelkopieën (back-ups) om integriteit en beschikbaarheid in geval van verstoring en calamiteit zo veel mogelijk te waarborgen.
   - Beveiliging en correct omgaan met media en bedrijfsmiddelen ter bescherming van onbevoegde openbaarmaking, modificatie, verwijdering en vernietiging.
   - Correcte en veilige manier van uitwisseling van informatie, op welke wijze dan ook.

7. Toegangsbeveiliging:
   - Elektronische toegangsbeveiliging is gebaseerd op gebruikersnaam/wachtwoord; hier gaan de medewerkers op een juiste en verantwoorde wijze mee om.
   - Registratie van bevoegde gebruikers met functie, rol en daarbij behorende toegangsrechten is van groot belang.
   - Duidelijke vastlegging en kennisgeving van verantwoordelijkheden van gebruikers.
   - Toegang alleen tot informatie en netwerkdiensten waarvoor de medewerker bevoegd is, op basis wat de medewerker voor het werk en functioneren nodig heeft.
   - Speciale aandacht voor draagbare computers, telewerkers en thuiswerkers.
8. Verwerving, ontwikkeling en onderhoud van informatiesystemen:
   - Beveiliging maakt integraal deel uit van informatiesystemen, vanaf de verwerving houdt de directie hiermee rekening.
   - Correcte validatie van gegevens in de verschillende stadia van verwerking is essentieel.
9. Beheer van informatiebeveiligingsincidenten:
   - Gebeurtenissen en zwakke plekken ten aanzien van informatiebeveiliging kent men, melding en rapportage is hierbij belangrijk.
   - Incidenten ten aanzien van informatiebeveiliging dienen speciale aandacht te verkrijgen, zowel in melding, afhandeling als bewaking; verbeteringen dienen hierop te volgen.
10. Bedrijfscontinuïteitsbeheer:
    - Storingen en calamiteiten kunnen de bedrijfsprocessen ernstig stagneren; door bedrijfscontinuïteit en plannen op dat gebied kan de directie de gevolgen minimaliseren, de impact beperken en risico's verkleinen.
11. Naleving:
    - Naleving van wet- en regelgeving is voor de directie van essentieel belang; met name correct omgaan met persoonsgegevens (WBP, SUWI).
    - Verder leven de medewerkers normen en dit beleid op een juiste manier na.

Prioriteiten voor realisatie en implementatie

Onderstaand belangrijkste hoofdpunten voor realisatie en implementatie en de prioriteit daarvan.

- Toetsen van bestaande regels en richtlijnen met het Informatiebeveiligingsbeleid, eventuele aanpassing van regels en richtlijnen.
- Inventariseren van de bedrijfsmiddelen, vastleggen eigenaars, verantwoordelijkheden en regels/procedures over gebruik en meenemen buiten gebouw.
- Registreren van gebruikers, functies, rollen en nodige toegang tot computers en informatiesystemen; opstellen procedures voor regelmatige controle en handhaving.
- Classificeren van informatie, gedragsregels en procedures die daarop betrekking hebben.
- Vaststellen procedures gerelateerd aan het dienstverband, met name uitdiensttreding en ontslag op staande voet.
- Vaststellen hoe om te gaan met draagbare computers, computers voor telewerken en verwijderbare media.
- Evalueren naleving wet- en regelgeving, toetsen of dit in voldoende mate verwoord is in het Informatiebeveiligingsbeleid.