ISD Noordoost

Informatiebeveiligingsbeleid
ISD Noordoost

versie 12 maart 2015

INHOUDSOPGAVE

1 INTRODUCTIE

Dit document bevat het Informatiebeveiligingsbeleid van ISD Noordoost. Dit beleid kent als uitgangspunten de bedrijfsdoelstellingen, de relevante risico's en de doelstelling van het Informatiebeveiligingsbeleid zelf.

De directie van ISD Noordoost geeft met dit beleidsdocument richting aan Informatiebeveiliging in overeenstemming met bedrijfsmatige eisen en relevante wetten en voorschriften. Zij volgt hierin, naast wet- en regelgeving, de als standaard aanvaarde norm verwoord in NEN-ISO/IEC 27002. Dit beleidsdocument is geaccordeerd door het management team en de directie van ISD Noordoost, en met geplande tussenpozen beoordeeld om doeltreffendheid te waarborgen.

1.1 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 adequate waarborgen voor de continuïteit van haar bedrijfsprocessen en dienstverlening.

Voor de realisatie van het Informatiebeveiligingsbeleid is ISD Noordoost in veel gevallen afhankelijk van partners en derden. Zij neemt daarbij haar verantwoordelijkheid door het initiatief te nemen voor overleg en samenwerking. Verder door regelmatige controles uit te voeren op de realisatie en uitvoering van maatregelen, zowel intern als extern bij derden, waar reëel en mogelijk.

1.2 Afwegingen en analyse risico's

Gezien het kader en de grootte van de organisatie zijn de inschattingen en afwegingen ten aanzien van risico's globaal gehouden. Onderstaand een overzicht van onderkende risico's.

- Onbevoegde inzage in gegevens, vooral persoonsgegevens van cliënten en medewerkers, door medewerkers bij betrokken gemeenten, GemCC, partners, derde partijen, leveranciers en bezoekers; classificatie van gegevens, adequaat beheer van toegangsrechten en juist omgaan met verwijderbare media en draagbare computers bieden ondersteuning om dit risico te verminderen.
- Onbevoegde kennisname van gegevens en informatie (afluisteren), zoals bij de balie of door bezoekers.
- Aantasten veiligheid van medewerkers, door agressie, ongewenst gedrag en fysiek geweld van cliënten.
- Fraude met geldelijke middelen door eigen medewerkers (dit wordt als relatief laag risico gekwalificeerd door de reeds aanwezige maatregelen; adequate screening, goed omgaan met toegangsrechten en autorisaties verkleint dit risico).
- Afnemende interesse voor Informatiebeveiliging door onvoldoende betrokkenheid van directie, organisatie en derde partijen.
- Tekort schietende registratie van bedrijfsmiddelen waardoor men missende of ontvreemde onderdelen niet opmerkt.
- Risico van inbraak, zowel fysiek als elektronisch.
- Negatieve meldingen in de pers door onvoldoende naleving van wet- en regelgeving.

2 TOEGEPASTE INFORMATIEBEVEILIGINGSBELEID

Onderstaand de verschillende onderdelen van het Informatiebeveiligingsbeleid, uitgaande van de indeling van NEN-IISO/IEC 27002:2007nl.

2.1 Organisatie van informatiebeveiliging

Interne organisatie

ISD Noordoost beheert en belegt de Informatiebeveiliging op de volgende manier binnen haar organisatie:

- Actieve betrokkenheid van de directie bij informatiebeveiliging, zoals het geven van goede voorbeelden en ondersteuning van de bij informatiebeveiliging betrokken functionaris(sen).
- Betrokkenheid en coördinatie vanuit alle delen van de organisatie.
- Toewijzen van verantwoordelijkheden en bevoegdheden voor Informatiebeveiliging door de aanstelling van een functionaris Informatiebeveiliging.
- Een goedkeuringsproces voor nieuwe IT-voorzieningen, informatiebeveiliging.
- De geheimhoudingsverklaring vormt een weerslag van de eisen voor vertrouwelijkheid binnen de organisatie en wordt door alle medewerkers (intern en extern) gekend en ondertekend.
- Contacten met overheidsinstanties op het gebied van (informatie)beveiliging, zoals Politie, Justitie, Brandweer en GOVCERT.
- Onafhankelijke toetsing en beoordeling van de Informatiebeveiliging op een regelmatige basis bevordert de kwaliteit en geeft een onafhankelijk advies voor mogelijke verbeteringen.

Partners en externe partijen

Partners en derde partijen kunnen toegang hebben (fysiek en/of elektronisch) tot informatie en IT-voorzieningen van ISD Noordoost. Elke toegang tot de IT-voorzieningen en het verwerken en communiceren van informatie door externe partijen wordt beheerst. Ook voorkomt ISD Noordoost dat medewerkers van derde partijen onbevoegde inzage hebben in gegevens. Communicatie en afstemming van het informatiebeveiligingsbeleid GemCC en andere partijen zijn belangrijke onderdelen van het beleid.

2.2 Beheer van bedrijfsmiddelen

ISD Noordoost maakt gebruik van middelen bij de uitvoering van haar bedrijfsprocessen. Onder bedrijfsmiddelen verstaat men in de breedste zin alle middelen die daarvoor worden gebruikt. Betreffende IT-voorzieningen vallen daaronder niet alleen apparatuur, maar ook applicaties, bijbehorende licenties en de informatie. Van een deel van de bedrijfsmiddelen is ISD Noordoost “afnemer” van middelen beschikbaar gesteld door GemCC of Gemeente Delfzijl. Alle bedrijfsmiddelen zijn door ISD Noordoost adequaat vastgelegd.

2.3 Beveiliging van personeel

ISD Noordoost gaat op juiste en verantwoorde manier om met personeel, zowel werknemers, ingehuurd personeel, betrokken medewerkers van partners als externe gebruikers. Vanwege de gevoelige informatie waarmee ISD Noordoost omgaat, is veiligheid daarvan een belangrijk onderdeel. Deze verantwoordelijkheid beperkt zich niet tot de periode van het dienstverband, maar ook voorafgaand, bij veranderingen en de beëindiging.

Onderstaand de aandachtpunten van de verschillende stadia:

- Voorafgaand aan het dienstverband:
  - Vastleggen van rollen en verantwoordelijkheden van personeel ten aanzien van veiligheid en informatiebeveiliging, dit duidelijk communiceren.
  - Vastleggen van verplichtingen in de arbeidsovereenkomst.
  - Vaststellen en vastleggen welke sancties mogelijk zijn.
  - Laten ondertekenen dat personeel bovenstaande informatie heeft gelezen.
  - Nagaan van personalia, antecedenten en CV's, door screening in die mate als vereist voor de beoogde functie.
- Tijdens het dienstverband:
  - Verbeteren van bewustzijn aangaande informatiebeveiliging en het beleid bij personeel.
  - Participeren door directie en management door het stellen van eisen en het geven van goede voorbeelden.
  - Geven van training en voorlichting over Informatiebeveiliging en het beleid.
  - Navolgen van sancties en disciplinaire maatregelen, afhankelijk van gesteld beleid en inbreuk door personeel.
- Wijziging en beëindiging van het dienstverband:
  - Vastleggen van procedures en beleggen in de organisatie, zodat bij wijziging of beëindiging van het dienstverband dit ordelijk kan verlopen.
  - Beëindigen van verantwoordelijkheden, zorg dragen voor juiste overdracht.
  - Innemen en retourneren van bedrijfsmiddelen (registratie is noodzakelijk).
  - Blokkeren van toegangsrechten, ISD Noordoost geeft dit door aan GemCC; bij ontslag op staande voet worden toegangsrechten direct geblokkeerd.

2.4 Fysieke beveiliging en beveiliging van de omgeving

ISD Noordoost beschermt haar medewerkers, partners en bedrijfsmiddelen op de volgende wijze:

Beveiligde ruimten

Door het voorkomen van onbevoegde fysieke toegang tot, schade aan of verstoring van het gebouw en de informatie van de organisatie:

- Fysieke beveiliging van het gebouw en de ruimten, specifiek daar waar zich informatie en IT-voorzieningen bevinden.
- Bescherming door toepassing van geschikte toegangsbeveiliging voor kantoren, ruimten en faciliteiten; toegang alleen voor geautoriseerd personeel, inhoudend zowel eigen medewerkers, die van partners als ingehuurd personeel.
- Bescherming van bedreigingen van buiten, zoals schade door brand, overstroming, explosies, aanslagen en andere calamiteiten.
- ISD Noordoost geeft speciale aandacht aan de fysieke bescherming en richtlijnen voor werken in speciale ruimten, zoals spreekkamers; te denken valt aan mogelijk agressief gedrag van cliënten.

Beveiliging van apparatuur

Door het voorkomen van verlies, schade, diefstal of compromitteren van bedrijfsmiddelen en daardoor onderbreking van de bedrijfsactiviteiten. Apparatuur is beschermd tegen fysieke bedreigingen en gevaren van buitenaf. ISD Noordoost is hierbij voor een belangrijk deel afhankelijk van Gemeente Delfzijl en GemCC, samen met deze dienstverleners bereikt ze dit door onderstaande punten:

- Daar waar mogelijk wordt apparatuur zodanig geplaatst en bebeschermd dat risico's worden verminderd.
- Het schenken van speciale aandacht voor apparatuur buiten het gebouw van ISD Noordoost, zoals laptop, PDA's, USB-sticks en dergelijke.
- Zonder toestemming vooraf, mag men geen apparatuur, informatie en programmatuur van ISD Noordoost van de locatie meenemen.

2.5 Beheer van communicatie- en bedieningsprocessen

Binnen de bedrijfsprocessen zijn de informatiesystemen voor ISD Noordoost van essentieel belang. Een juist en adequaat beheer van dit onderdeel van de processen is van groot belang. Daar waar mogelijk neemt zij haar verantwoordelijkheid op de volgende wijze:

Bedieningsprocedures en verantwoordelijkheden
Door het waarborgen van een correcte en veilige bediening van IT-voorzieningen om zodoende het risico van nalatigheid of opzettelijk misbruik van het systeem te verminderen. Kernpunten:

- Het scheiden van taken en verantwoordelijkheidsgebieden om gelegenheid voor onbevoegde of onbedoelde wijziging of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.

Beheer van de dienstverlening door een derde partij
De dienstverlening door een derde partij dient in lijn te zijn met het informatiebeveiligingsbeleid van ISD Noordoost, verwoord en in overeenstemming met de overeenkomsten voor dienstverlening door die derde partij. Kernpunten:

- Beveiligingsmaatregelen, definities van dienstverlening en niveaus van dienstverlening zoals vastgelegd in de overeenkomst voor dienstverlening door een derde partij, worden geïmplementeerd, uitgevoerd en bijgehouden door die derde partij; dit inclusief geheimhoudingsverklaring.
- De diensten, rapporten en registraties die door de derde partij worden geleverd, worden regelmatig gecontroleerd.
- Toegang (fysiek en elektronisch) van medewerkers van derde partijen is tijdelijk en op afspraak, met alleen benodigde autorisaties.

Bescherming tegen virussen en "mobile code"
Voor de realisatie en toepassing van "anti-malware" is ISD Noordoost afhankelijk van GemCC. Indien apparatuur in eigen beheer is, bijvoorbeeld laptops, ligt hiervoor de verantwoordelijkheid bij ISD Noordoost.

Back-up
Voor ISD Noordoost is de handhaving van de integriteit en beschikbaarheid van informatie en IT-voorzieningen van essentieel belang. Het maken van back-ups van gegevens is hierbij belangrijk om tijdig herstel bij verstoringen en calamiteiten te realiseren. ISD Noordoost heeft de uitvoering hiervan bij GemCC belegd.

Beheer van netwerkbeveiliging
De bescherming van informatie in netwerken en bescherming van de ondersteunende infrastructuur is belegd bij GemCC en Suwinet. Vanwege het belang voor de bedrijfsprocessen controleert ISD Noordoost regelmatig of de juiste maatregelen zijn genomen voor veiligheid en beveiliging.

Behandeling van media
Media als dragers van gegevens zijn fysiek beschermd om onbevoegde openbaarmaking, modificatie, verwijdering en vernietiging van bedrijfsmiddelen en onderbreking van bedrijfsactiviteiten te voorkomen.

Uitwisseling van informatie
Veel van de gegevens, waarmee ISD Noordoost werkt en die zij beheert, betreffen gevoelige informatie. Verantwoorde en veilige uitwisseling is daarom van groot belang. Voor wat betreft de uitwisseling via Suwinet zijn getroffen maatregelen onderhevig aan wet- en regelgeving. Andere uitwisseling zijn in lijn met normen, wet- en regelgeving.

Diensten voor e-commerce
Te denken valt aan aspecten van het "Digitale Klanten Dossier" (DKD) en toekomstige inzage van burgers in persoonsgegevens van de overheid. ISD Noordoost stelt zich ten doel deze aspecten en ontwikkelingen te volgen, indien nodig het beleid aan te scherpen en adequate maatregelen te nemen. Dit om frauduleuze activiteiten, onbevoegde toegang, onbevoegde openbaarmaking en onterechte modificatie van door haar beheerde informatie te voorkomen.

Controle
Om met redelijke zekerheid mogelijk inbreuken op informatiebeveiliging te kennen controleert ISD Noordoost het volgende.
- Dat alleen geautoriseerd personeel gebruik kan maken van de IT-voorzieningen.
- Verwerkingsactiviteiten en gebeurtenissen op het gebied van informatiebeveiliging, bijvoorbeeld in audit-logbestanden.
- Juiste bescherming van bovengenoemde bestanden bewerkstelligen in overleg en samenwerking met GemCC.

2.6 Toegangsbeveiliging

ISD Noordoost onderkent dat de mens bij toegangsbeveiliging een zwakke schakel in de keten is.

Bedrijfseisen ten aanzien van toegangsbeheersing
Als beleid stelt ISD Noordoost dat alleen die medewerkers toegang tot bepaalde informatie hebben als dit voor hun functie en rol noodzakelijk is. Dit geldt ook voor direct betrokken ingehuurde derden zoals b.v. ZZP'ers.

Beheer van toegangsrechten van gebruikers
ISD Noordoost wil onbevoegde toegang tot informatiesystemen voorkomen door alleen bevoegde gebruikers toegang te verlenen. Vastlegging en beheer van toegangsrechten van gebruikers tot informatie, regelmatige controle en verificatie is essentieel. Kernpunten:
- Registreren van bevoegde gebruikers met functie en rol en de daarbij behorende reguliere toegangsrechten.
- Vaststellen, documenteren en handhaven van formele procedures voor registreren en afmelden van gebruikers, en voor het verlenen en intrekken van toegangsrechten tot alle informatiesystemen en -diensten.
- Speciale bevoegdheden zijn tot een minimum te beperkt, bovendien mogen deze alleen van tijdelijke aard zijn en (indien mogelijk) automatisch komen te vervallen.

- Toewijzing van wachtwoorden gebeurt gecontroleerd, alleen tijdelijke wachtwoorden kunnen worden verstrekt, de gebruiker dient zelf het uiteindelijke wachtwoord te bepalen en in te geven. Dit is ook verwoord in de “10 gouden regels”.
- De toegangsrechten van gebruikers worden regelmatig beoordeeld in een formeel proces.

Verantwoordelijkheden van gebruikers

Gebruikers van de informatiesystemen bij ISD Noordoost werken mee aan een doeltreffende beveiliging, om daarmee onbevoegde toegang door gebruikers, en beschadiging of diefstal van informatie en IT-voorzieningen te voorkomen.
Gebruikers worden op de hoogte gebracht van hun verantwoordelijkheid voor het handhaven van doeltreffende toegangsbeveiliging, vooral met betrekking tot het gebruik van wachtwoorden en beveiliging van gebruikersapparatuur. Dit is verwoord in de “10 gouden regels”.
Kernpunten:

- Gebruikers nemen goede beveiligingsgewoontes in acht bij het kiezen en gebruiken van wachtwoorden.
- Gebruikers bewerkstelligen dat onbeheerde apparatuur passend is beschermd om onbevoegde inzage van gegevens te voorkomen.
- Waar mogelijk streeft ISD Noordoost een “clear desk”-beleid voor papier en verwijderbare opslagmedia na en een “clear screen”-beleid voor IT-voorzieningen.

Toegangsbeheersing voor netwerken

Evenals inzage van informatie voorkomt ISD Noordoost de onbevoegde toegang tot netwerkdiensten waarvan ze gebruik maakt, zowel intern als extern. Voor ISD Noordoost heeft dat in het bijzonder betrekking op Internet en Suwinet. Kernpunten:

- Gebruikers hebben alleen toegang tot diensten waarvoor ze specifiek bevoegd zijn; dit geldt met name voor toegang tot Suwinet en daaraan gerelateerde onderzoekssystemen.
- Bescherming van netwerkpoorten is afdoende.

Toegangsbeveiliging voor besturingssystemen

De primaire toegangsbeveiliging bij ISD Noordoost vindt plaats vanuit het besturingssysteem of direct daaraan gelieerde programmatuur. Beheer hiervan berust bij GemCC. Het huidige systeem gaat uit van een gebruikersnaam en een wachtwoord.

Draagbare computers en telewerken

Draagbare computers (notebooks, laptops, PDA’s en smart phones) en computers die medewerkers gebruiken voor thuiswerken vormen speciale risicogroepen. Draagbare computers zijn gevoelig voor diefstal, in die situaties mag informatie binnen redelijke termen niet raadpleegbaar zijn. Kernpunten:

- Draagbare computers:
  - Opgeslagen informatie, ook van tijdelijke aard, is niet leesbaar voor onbevoegden; toepassing van encryptie is een vereiste.
  - Waar mogelijk en reëel is adequate anti-malware te worden toegepast en regelmatig vernieuwd.
- Telewerken:
  - ISD Noordoost controleert of beveiliging van computers door telewerkers voldoende is; en gaat na of technische maatregelen gewenst en mogelijk zijn.

2.7 Verwerving, ontwikkeling en onderhoud van informatiesystemen

GemCC voert het technische beheer uit voor ISD Noordoost, daar berust voor een belangrijk deel de uitvoering van verwerving en onderhoud van informatiesystemen. ISD Noordoost ontwikkelt zelf geen informatiesystemen, behalve toepassing van bepaalde hulpmiddelen ter ondersteuning van bedrijfsprocessen.

Beveiligingseisen voor informatiesystemen
Beveiliging maakt integraal deel uit van informatiesystemen. ISD Noordoost oefent in dit kader alleen invloed uit bij de keuze van haar informatiesystemen en bij uitbreiding daarvan.

Correcte verwerking in toepassingen
Zowel de de invoer, verwerking, uitvoer als het berichtenverkeer zijn voldoende gewaarborgd om de juistheid, volledigheid en integriteit van de gegevens voldoende te waarborgen. Hiermee fouten, verlies, onbevoegde modificatie of misbruik van informatie in toepassingen voorkomen.

- Valideren van invoergegevens voor informatiesystemen om zeker te stellen dat ze juist, geschikt en compleet zijn.
- De verwerking van gegevens bevat voldoende waarborgen en controles om corrumperen door fouten of opzettelijke handelingen te ontdekken, indien mogelijk te voorkomen.

Beveiliging bij ontwikkelings- en ondersteuningsprocessen
Processen voor ontwikkeling en ondersteuning zijn voldoende beveiligd. ISD Noordoost werkt samen met GemCC om de beveiliging van toepassingsprogrammatuur en –informatie te handhaven.

2.8 Beheer van informatiebeveiligingsincidenten

Rapportage van informatiebeveiligingsgebeurtenissen en zwakke plekken
Zwakheden aangaande informatiebeveiliging worden gemeld zodat dit kenbaar is en men daarop adequate maatregelen kan treffen.
Kernpunten:

- Rapportage van gebeurtenissen over informatiebeveiliging:
- Alle medewerkers van en bij ISD Noordoost melden zwakke plekken in de beveiliging in informatiesystemen en diensten aan de Functionaris Informatiebeveiliging.
- De Functionaris Informatiebeveiliging rapporteert aan de directie van ISD Noordoost.

Beheer van informatiebeveiligingsincidenten en -verbeteringen
Naast de melding is een adequate registratie en beheer nodig van incidenten aangaande informatiebeveiliging. Hierbij draagt ISD Noordoost een (gedeelde) verantwoordelijkheid. Verzamelde bewijzen dienen aan bepaalde voorwaarden te voldoen en stellen ook eisen aan de betrokken functionarissen, sterke betrokkenheid van Justitie en Politie is dan ook essentieel.
Kernpunten:

- Adequate reactie op incidenten afhankelijk van het type incident.
- Evaluatie van maatregelen en procedures om lering te trekken van informatiebeveiligingsincidenten zodat continue verbetering kan worden gerealiseerd.
- ISD Noordoost dient mogelijk bewijzen overleggen. Het verzamelen van bewijslast is dan ook van groot belang; de betrokkenheid van justitiële en opsporingsambtenaren is sterk gewenst.

2.9 Bedrijfscontinuïteitsbeheer

Ernstige storingen en calamiteiten kunnen de bedrijfsprocessen ernstig stagneren. GemCC heeft een kader (raamwerk) opgesteld voor Bedrijfscontinuïteit van het gebied wat zij beheert. ISD Noordoost haakt daarop in en neemt zo haar verantwoordelijkheid op dit gebied.

Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer
De gevolgen van ernstige storingen en calamiteiten kunnen voor ISD Noordoost leiden tot uitval van kritische bedrijfsprocessen en verlies van informatie. Ook kunnen bij calamiteiten gegevens openbaar komen. ISD Noordoost gaat onderbreking van bedrijfsactiviteiten tegen en beschermt kritische bedrijfsprocessen tegen gevolgen van dergelijke storingen en calamiteiten.
Kernpunten zijn:

- Mogelijke risico's van de bedrijfscontinuïteit zijn bekend, ingeschat en beoordeeld, inclusief de gevolgen voor de informatiebeveiliging.

2.10 Naleving

Naleving van de wettelijke voorschriften
Als onderdeel van de overheid is schending van enige wetgeving, wettelijke of contractuele verplichtingen niet toelaatbaar. Wat betreft de Archiefwet heeft ISD Noordoost dit belegd bij Gemeente Delfzijl, en controleert regelmatig op de juiste naleving er van.
Kernpunten:

- Identificeren van toepasbare wetgeving, zoals:
  - WBP – Wet Bescherming Persoonsgegevens.
  - SUWI – Wet Structuur Uitvoeringsorganisatie Werk en Inkomen, aangevuld met richtlijnen van BKWI.
  - Archiefwet, aangevuld met richtlijnen over bewaarperiodes.
  - Wet Computercriminaliteit.
- Nagaan welke (types) bedrijfsdocumenten buiten klanten- en persoonsgegevens bescherming nodig hebben.
- Bescherming en geheimhouding van persoonsgegevens vormt een belangrijk aspect binnen de bedrijfsprocessen van ISD Noordoost.
- Voorkomen van misbruik van IT-voorzieningen door vaststellen van procedures, regels en richtlijnen, kenbaar maken en handhaven.

Naleving van beveiligingsbeleid en -normen en technische naleving
De naleving van beleid, maatregelen, regels en richtlijnen door medewerkers worden gecontroleerd, beoordeeld en gewaarborgd door:

- Het naleving van het beveiligingsbeleid en de -normen (dit beleid dus).
- Het controleren van de informatiesystemen op technische naleving van beleid en normen.

Overwegingen bij audits van informatiesystemen
ISD Noordoost wil door audits de doeltreffendheid van het informatiesysteem maximaliseren en verstoring als gevolg van audits minimaliseren. In principe laat ISD Noordoost audits uitvoeren door een ander (of andere partij) dan de uitvoerende personen of organisatie.