Informatiebeveiligingsbeleid
Eerstelijnszone Noord-Oost Waasland

Opgemaakt door de functionaris voor gegevensbescherming

Inhoud

1. Algemeen

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket aan maatregelen om de kwaliteitsaspecten beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening te garanderen.

De kwaliteitsaspecten:

- **Beschikbaarheid**: de mate waarin gegevens of functionaliteit op de juiste momenten beschikbaar zijn voor gebruikers
- **Integriteit**: de mate waarin gegevens of functionaliteit juist ingevuld zijn
- **Vertrouwelijkheid**: de mate waarin de toegang tot gegevens of functionaliteit beperkt is tot degenen die daartoe bevoegd zijn

Informatiebeveiliging is een beleidsverantwoordelijkheid van het bestuur. Ook in Eerstelijnszone Noord-Oost Waasland is sprake van toenemende afhankelijkheid van informatie en computersystemen, waardoor nieuwe kwetsbaarheden en risico's kunnen optreden. Het is daarom van belang hiertegen adequate maatregelen te nemen. Onvoldoende informatiebeveiliging kan leiden tot onacceptabele risico's bij de bedrijfsvoering van de instelling of organisatie. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades en imagoverlies.

De Eerstelijnszone Noord-Oost Waasland heeft de ambitie om met het beleidsdocument informatiebeveiliging structureel naar een hoger niveau te brengen en op dit niveau te houden door de organisatie van de beveiligingsfunctie en het informatiebeveiligingsbeleid duidelijk te beschrijven en vast te stellen.

2. Reikwijdte van het beleid

In de reikwijdte van het beleid wordt beschreven wat de afbakening is van het toepassingsgebied ervan.

Bij de Eerstelijnszone Noord-Oost Waasland wordt informatiebeveiliging breed geïnterpreteerd. Het informatiebeveiligingsbeleid binnen deze Eerstelijnszone Noord-Oost Waasland heeft betrekking op alle medewerkers, de Zorgraad, burgers, bezoekers en externe relaties (inhuur/outsourcing), alsmede op alle organisatieonderdelen. Tevens vallen onder het informatiebeveiligingsbeleid alle afdelingen van waaruit geautoriseerde toegang tot het instellingsnetwerk verkregen kan worden. Het beleid beperkt zich niet tot digitale informatie, maar omvat zeker ook informatie op andere dragers (vb. dossiers, archieven).

Bij het informatiebeveiligingsbeleid ligt de nadruk op die toepassingen die vallen onder de verantwoordelijkheid van de Eerstelijnszone Noord-Oost Waasland. Dit heeft zowel betrekking op *gecontroleerde informatie*, die door de organisatie zelf is gegenereerd, opgehaald en wordt beheerd, als ook op *niet-gecontroleerde informatie*, bv. uitspraken, persoonlijke websites of zakelijke personal pages, waarop de instelling kan worden aangesproken. Betrokkenen worden hierbij geacht zich aan de geldende gedragscode of deontologische code te houden.

3. Beleidsprincipes informatiebeveiliging

Security management wordt als proces ingericht. Dat houdt in dat er een driejaarlijkse planning en controlecyclus is. Hierin worden plannen opgesteld en uitgevoerd. De resultaten ervan worden geëvalueerd en vertaald naar nieuwe driejaarlijkse plannen.

De beleidsuitgangspunten bij de Eerstelijnszone Noord-Oost Waasland zijn:

Onze filosofie is dat we een open instelling zijn, waar veel mogelijk is. De benadering van ICT en beveiliging is minder open. Er wordt van medewerkers en de Zorgraad verwacht dat ze zich qua techniek en ook qua houding 'fatsoenlijk' gedragen (eigen verantwoordelijkheid).
Niet acceptabel is dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagoverlies. Het is om deze reden dat er gedragscodes (deontologische codes) zijn geformuleerd en geïmplementeerd.

De beveiliging dient te voldoen aan de relevante wet- en regelgeving, in het bijzonder aan de Privacywet en het eGov-decreet. De beveiliging dient de volgende aspecten te waarborgen:

- Beschikbaarheid
- Integriteit
- Vertrouwelijkheid.

De Eerstelijnszone Noord-Oost Waasland hanteert de volgende beleidsprincipes:

- Informatiebeveiliging is een **lijnverantwoordelijkheid**: dat betekent dat de diensthoofden de primaire verantwoordelijkheid dragen voor een goede informatiebeveiliging op hun diensten
- Informatiebeveiliging is **ieders verantwoordelijkheid**. Van medewerkers, de Zorgraad en derden wordt er verwacht dat ze actief bijdragen aan de veiligheid van geautomatiseerde en analoge systemen en de daarin opgeslagen informatie. Dat gebeurt in de aanstellingsbrief, tijdens functioneringsgesprekken, met een instelling brede gedragscode, met periodieke bewustwordingscampagnes, et cetera. Het opleggen van sancties na overtredingen maakt het geheel geloofwaardig.
- Informatiebeveiliging is een **continu proces**. Regelmatige herijking van beleid en audits: technologische en organisatorische ontwikkelingen binnen en buiten de instelling maken het noodzakelijk om periodiek te bezien of men nog op de juiste wijze bezig is de beveiliging te waarborgen. De audits maken het mogelijk het beleid en de genomen maatregelen te controleren op efficiency (**controleerbaarheid**).
- **Eigendom van informatie**: de Eerstelijnszone Noord-Oost Waasland is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd, tenzij dit voor bijvoorbeeld onderzoek anders is overeengekomen. Medewerkers dienen goed geïnformeerd te zijn over de regelgeving voor het (her)gebruik van deze informatie.
- **Waardering van informatie**: iedereen behoort de waarde van informatie te kennen en daar naar te handelen. Deze waarde wordt bepaald door de schade als gevolg van verlies van beschikbaarheid, integriteit en vertrouwelijkheid. Classificatie kan hierbij behulpzaam zijn; zie volgende hoofdstuk.
- Bij **projecten**, zoals infrastructurele wijzigingen of de aanschaf van nieuwe systemen, dient vanaf de start rekening gehouden te worden met informatiebeveiliging.

- Er wordt een **functionaris voor gegevensbescherming** aangesteld in de Eerstelijnszone Noord-Oost Waasland. De functionaris voor gegevensbescherming stelt het informatiebeveiligingsbeleid op en ziet organisatiebreed toe op de naleving ervan en de daaruit voortvloeiende maatregelen, zorgt voor onderzoek en adviseert in complexe beveiligingsvraagstukken, initieert risicoanalyses en vervult een adviserende rol naar het bestuur en zijn medewerkers.

  De functionaris voor gegevensbescherming verbindt zich ertoe de ethische gedragscode van de functionarissen voor gegevensbeschermingen in al haar aspecten na te leven.

- Er wordt een **informatieveiligheidscel** opgericht. In deze cel nemen de voorzitter van de Zorgraad, de functionaris voor gegevensbescherming, de penhouder en twee medewerkers zitting. De informatieveiligheidscel wordt voorgezeten door de functionaris voor gegevensbescherming en ziet toe op de uitvoering van het veiligheidsplan middels de behandeling van diverse aandachtspunten en voorstellen ter formalisering.

  De Zorgraad delegeert eventueel (een aantal van) haar bevoegdheden inzake informatieveiligheid naar haar medewerkers, waarmee de informatieveiligheidscel slagvaardig kan optreden.

4. Documenten informatiebeveiliging

In het kader van informatiebeveiliging worden de volgende documenten en resultaten opgeleverd.

4.1. Het informatiebeveiligingsbeleid

Het beleid ligt ten grondslag aan de aanpak van informatiebeveiliging binnen de organisatie. In het informatiebeveiligingsbeleid worden de voorwaarden en verantwoordelijkheden vastgelegd. Het informatiebeveiligingsbeleid wordt opgemaakt door de functionaris voor gegevensbescherming. Om ervoor te zorgen dat het beleid gedragen wordt binnen de organisatie en de organisatie ernaar handelt wordt het goedgekeurd en uitgedragen door de Zorgraad.

4.2. Veiligheidsplan

Het veiligheidsplan beschrijft de minimale maatregelen die nodig zijn om het gewenste niveau van informatiebeveiliging te kunnen waarborgen. Als er systemen zijn die na een risicoanalyse hogere eisen nodig hebben dan worden deze genomen. Het veiligheidsplan wordt gemaakt door de functionaris voor gegevensbescherming en goedgekeurd door de Zorgraad.

4.3. Risicoanalyses en audits

Periodieke evaluatie van de risico's van systemen is noodzakelijk om vast te stellen of het gekozen pakket maatregelen nog steeds voldoet aan de gewijzigde omstandigheden omdat bedreigingen in de loop der tijd kunnen veranderen, informatiesystemen en/of de organisatie inmiddels kunnen zijn aangepast en maatregelen wellicht anders uitdraaien dan oorspronkelijk bedoeld. De risicoanalyses worden besproken met de systeemeigenaren en functionaris voor gegevensbescherming en over maatregelen wordt geadviseerd aan het bestuur. Een evaluatie kan overigens ook aanleiding zijn tot het bijstellen van de minimale maatregelen. De risicoanalyses worden gemaakt onder verantwoordelijkheid van functionaris voor gegevensbescherming en in samenwerking met eventuele externe firma's.

4.4. Incidentregistratie

Een actuele en betrouwbare registratie van incidenten is een essentiële randvoorwaarde voor een goed beleid. De medewerker(s) van de Eerstelijnszone Noord-Oost Waasland en de leden van de informatieveiligheidscel dragen zorg voor het registreren van incidenten, maar ook voor de evaluatie ervan en op grond daarvan bijdragen aan aanscherping van het veiligheidsplan. Alle incidenten met betrekking tot (mogelijke) inbreuken op de informatieveiligheid (en in het bijzonder de privacy) worden gemeld aan de informatieveiligheidscel.

Voorbeelden van incidenten welke gerapporteerd dienen te worden:
- niet-verklaarbare onregelmatigheden in logfiles van systemen en applicaties;
- falen van een integriteitcontrole t.b.v. een informatiesysteem of informatiebron;
- verlies van een informatiebron;
- ongeplande uitval van informatiesystemen langer dan 1 dag waarvan de systeembeheerder oordeelt dat dit een incident is
- (vermoedelijke) inbraak op een systeem;
- (vermoeden van) misbruik van een systeem of gegevens door een legitieme gebruiker;

Incidenten worden besproken en geëvalueerd in de informatieveiligheidscel.

4.5. Classificatie

Bij de Eerstelijnszone Noord-Oost Waasland zullen alle gegevens waarop dit informatiebeveiligingsbeleid van toepassing is worden geclassificeerd. Het niveau van de beveiligingsmaatregelen is afhankelijk van de klasse.

Voor **vertrouwelijkheid en integriteit** wordt de volgende indeling gevolgd.

- **Anonieme gegevens**
  Dit zijn gegevens die niet in verband kunnen gebracht worden met een geïdentificeerde of identificeerbare persoon en zijn dus geen persoonsgegevens;
- **Persoonsgegevens**
  Een persoonsgegeven is iedere informatie over een geïdentificeerd of identificeerbaar natuurlijk persoon;
- **Gevoelige persoonsgegevens**
  Dit zijn gegevens over ras, politieke opvattingen, godsdienstige of levensbeschouwelijke overtuigingen, lidmaatschap van een vakvereniging, gezondheid, seksuele leven, verdenkingen, vervolgingen, strafrechtelijke of bestuurlijke veroordelingen. Het is in principe verboden om dergelijke gegevens te verwerken;
- **Gecodeerde al dan niet gevoelige persoonsgegevens**
  Dit zijn persoonsgegevens die slechts door middel van een code in verband kunnen gebracht worden met een geïdentificeerde of identificeerbare persoon.

Welk beveiligingsniveau geschikt is voor een bepaald informatiesysteem hangt af van de classificatie van de informatie die het systeem verwerkt.

In het kader van continuïteit en de beschikbaarheid worden de volgende klassen onderscheiden:

- **Niet vitaal**: algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan 1 week brengt geen merkbare (meetbare) schade toe aan de belangen van de instelling, haar medewerkers of haar klanten;

- **Vitaal**: algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan 1 week brengt merkbare schade toe aan de belangen van de instelling, haar medewerkers of haar klanten;
- **Zeer vitaal**: algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan 1 dag brengt merkbare schade toe aan de belangen van de instelling, haar medewerkers of haar klanten.

5. Wettelijke voorschriften

- Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van richtlijn 95/46/EG (Algemene Verordening Gegevensbescherming)
- Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens
- Wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen
- Decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer
- Besluit van de Vlaamse Regering van 23 november 2018 betreffende de functionarissen voor gegevensbescherming, vermeld in artikel 9 van het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer
- Besluit van de Vlaamse Regering van 15 mei 2009 houdende de uitvoering van het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer
- Besluit van de Vlaamse Regering van 29 november 2013 tot uitvoering van het decreet van 13 juli 2012 houdende de oprichting en organisatie van een Vlaamse dienstenintegrator
- Decreet van 26 april 2019 betreffende de organisatie van de eerstelijnszorg, de regionale zorgplatformen en de ondersteuning van de eerstelijnszorgaanbieders