NOTULEN VAN DE RAAD VOOR MAATSCHAPPELIJK WELZIJN VAN 21 FEBRUARI 2022

Aanwezig:	Marco Goossens, voorzitter; René Leyssen, Ilse Wevers, Kurt Plessers, Lieve Dierickx, Jo Seutens, Raf Vliegen, Hanne Schrooten, Rob Haex, Katy Craeghs, Renaud Hamal, Jan Schonkeren, Frieda Gijbels, An Knoops, Sara Nies, Michel Creemers, Lotte Janssen, Ivan Roosen, Vanita Mertens, Petra Vandewinkel, Lut Witters, Jorn Neyens, Carine Neyens, Joris Evens en Ilse Hindrikx, raadsleden; en Guy Bodeux, algemeen directeur
Verontschuldigd:	Bart Beelen en Kristel Schrooten, raadsleden
Afwezig:	

OPENBARE VERGADERING

01. Goedkeuring van de notulen en het zittingsverslag van de vorige zitting

contactpersoon	functie	e-mail	dossier
Marina Caymax	administratief medewerkster	marina.caymax@oudsbergen.be	

Voorgeschiedenis en verwijzingsdocumenten

De vorige raad voor maatschappelijk welzijn vond digitaal plaats op 24 januari 2022. Hiervan stelde de algemeen directeur de notulen op. De opname die van de vergadering gemaakt werd, geldt als zittingsverslag en is te raadplegen via de website van Oudsbergen.

Argumentatie

De notulen en het zittingsverslag van de vergadering van de raad voor maatschappelijk welzijn worden onder de verantwoordelijkheid van de algemeen directeur opgesteld.

Elk raadslid heeft het recht tijdens de vergadering opmerkingen te maken over de redactie van de notulen en het zittingsverslag van de vorige vergadering. Als die opmerkingen door de raad voor maatschappelijk welzijn worden aangenomen, worden de notulen en het zittingsverslag in die zin aangepast.

Als er geen opmerkingen worden gemaakt over de notulen en het zittingsverslag van de vorige vergadering worden de notulen en het zittingsverslag als goedgekeurd beschouwd.

Juridische context

Bevoegdheid:

Artikels 77 en 78 van het decreet lokaal bestuur van 22 december 2017 bepalen dat de raad voor maatschappelijk welzijn bevoegd is voor deze materie.

Grond:

Artikels 74, 277 en 278 van het decreet lokaal bestuur van 22 december 2017.

Adviezen en inspraak

Er werd geen voorafgaand advies ingewonnen, noch vond er inspraak plaats.

Plaats in het meerjarenplan en financiële gevolgen

De uitvoering van het besluit heeft geen link met het meerjarenplan en heeft ook geen financiële consequenties.

Stemming, na beraadslaging

Met unanimiteit van stemmen.

Besluit

Artikel 1

De raad voor maatschappelijk welzijn keurt de notulen en het zittingsverslag van de raad voor maatschappelijk welzijn van 24 januari 2022 goed.

Artikel 2

Tegen dit besluit kan een klacht worden ingediend bij de toezichthoudende overheid. Deze klacht moet ingediend worden binnen een periode van 30 dagen die volgt op de dag van de bekendmaking van dit besluit op de website van de gemeente Oudsbergen.

De klacht kan via een aangetekend schrijven gericht worden aan:

Agentschap Binnenlands Bestuur
VAC Herman Teirlinck Brussel
Havenlaan 88, bus 70
1000 Brussel

De klacht kan ook via een aangetekende e-mail verstuurd worden naar: binnenland@vlaanderen.be

Artikel 3

Dit besluit wordt overeenkomstig de bepalingen uit artikels 285 tot en met 287 van het decreet lokaal bestuur bekendgemaakt op de website van de gemeente Oudsbergen.

02. Kennisname van het ontslag van mevrouw Carine Neyens als lid van het Bijzonder Comité voor de Sociale Dienst en van de verkiezing van de heer Marc Truyen als nieuw lid van het Bijzonder Comité voor de Sociale Dienst

contactpersoon	functie	e-mail	dossier
Guy Bodeux	algemeen directeur	guy.bodeux@oudsbergen.be	

Voorgeschiedenis en verwijzingsdocumenten

De Raad voor Maatschappelijk Welzijn heeft op 2 januari 2019 mevrouw Carine Neyens verkozen als lid van het Bijzonder Comité voor de Sociale Dienst.

Mevrouw Carine Neyens heeft op 6 februari 2022 schriftelijk gemeld dat zij ontslag wenst te nemen als lid van het Bijzonder Comité voor de Sociale Dienst vanaf 1 maart 2022.

De voorzitter van de Raad voor Maatschappelijk Welzijn heeft op 7 februari 2022 kennis genomen van het ontslag van mevrouw Carine Neyens als lid van het Bijzonder Comité voor de Sociale Dienst, waardoor het ontslag definitief is.

Argumentatie

In de voordrachtsakte van de kandidaat-leden van het Bijzonder Comité voor de Sociale Dienst werd er voor mevrouw Carine Neyens geen opvolgers aangeduid.
In toepassing van artikel 95 van het decreet lokaal bestuur van 22 december 2017 werd door de leden van de Raad voor Maatschappelijk Welzijn die indertijd mevrouw Carine Neyens voorgedragen hebben, een voordrachtsakte ingediend waarbij de heer Marc Truyen wordt voorgedragen als nieuw lid van het Bijzonder Comité voor de Sociale Dienst. Deze voordrachtsakte werd bezorgd aan de algemeen directeur op 7 februari 2022 en bezorgd aan de voorzitter van de raad voor maatschappelijk welzijn op 7 februari 2022.
Uit onderzoek van de geloofsbrieven blijkt dat de heer Marc Truyen voldoet aan de verkiesbaarheidsvoorwaarden en dat er zich geen onverenigbaarheden stellen.

Juridische context

Bevoegdheid:

Artikels 77 en 78 van het decreet lokaal bestuur van 22 december 2017 bepalen dat de raad voor maatschappelijk welzijn bevoegd is voor deze materie.

Grond:

Het besluit van de Raad voor Maatschappelijk Welzijn van 2 januari 2019 in verband met de verkiezing van de leden van het Bijzonder Comité voor de Sociale Dienst.

Hoofdstuk 6, afdeling 1 van het decreet lokaal bestuur van 22 december 2017 in verband met de organisatie van het Bijzonder Comité voor de Sociale Dienst.

Adviezen en inspraak

Er werd voorafgaand geen advies ingewonnen en er vond geen inspraak plaats.

Plaats in het meerjarenplan en financiële gevolgen

De uitvoering van het besluit heeft geen link met het meerjarenplan.

Neemt kennis van:

Artikel 1

Het ontslag van mevrouw Carine Neyens als lid van het Bijzonder Comité voor de Sociale Dienst vanaf 1 maart 2022.

Artikel 2

De geloofsbrieven van de heer Marc Truyen worden onderzocht. Hieruit blijkt dat er geen onverenigbaarheid is. De Raad voor Maatschappelijk Welzijn neemt dan ook kennis van de eedaflegging door de heer Marc Truyen, die in openbare vergadering en in handen van de voorzitter van de Raad voor Maatschappelijk Welzijn de volgende eed aflegt conform artikel 96 § 1 van het decreet lokaal bestuur van 22 december 2017:

"Ik zweer de verplichtingen van mijn mandaat trouw na te komen"

Artikel 3

De aanstelling van de heer Marc Truyen als lid van het Bijzonder Comité voor de Sociale Dienst vanaf 1 maart 2022.

Artikel 4

Tegen dit besluit kan een klacht worden ingediend bij de toezichthoudende overheid. Deze klacht moet ingediend worden binnen een periode van 30 dagen die volgt op de dag van de bekendmaking van dit besluit op de website van de gemeente Oudsbergen.

De klacht kan via een aangetekend schrijven gericht worden aan:

Agentschap Binnenlands Bestuur
VAC Herman Teirlinck Brussel
Havenlaan 88, bus 70
1000 Brussel

De klacht kan ook via een aangetekende e-mail verstuurd worden naar: binnenland@vlaanderen.be

Artikel 5

Dit besluit wordt overeenkomstig de bepalingen uit artikels 285 tot en met 287 van het decreet lokaal bestuur bekendgemaakt op de website van de gemeente Oudsbergen.

Een afschrift van het proces-verbaal van eedaflegging van dhr. Marc Truyen wordt aan de voorzitter van het Bijzonder Comité voor de Sociale Dienst bezorgd.

03. Kennisname van het ontslag vande heer Joris Evens als lid van het Bijzonder Comité voor de Sociale Dienst en van de verkiezing van de heer Rob Ulenaers als nieuw lid van het Bijzonder Comité voor de Sociale Dienst

contactpersoon	**functie**	**e-mail**	**dossier**
Guy Bodeux	algemeen directeur	guy.bodeux@oudsbergen.be	

Voorgeschiedenis en verwijzingsdocumenten

De Raad voor Maatschappelijk Welzijn heeft op 2 januari 2019 de heer Joris Evens verkozen als lid van het Bijzonder Comité voor de Sociale Dienst.
De heer Joris Evens heeft op 6 februari 2022 schriftelijk gemeld dat hij ontslag wenst te nemen als lid van het Bijzonder Comité voor de Sociale Dienst vanaf 1 maart 2022.
De voorzitter van de Raad voor Maatschappelijk Welzijn heeft op 7 februari 2022 kennis genomen van het ontslag van de heer Joris Evens als lid van het Bijzonder Comité voor de Sociale Dienst, waardoor het ontslag definitief is.

Argumentatie

In de voordrachtsakte van de kandidaat-leden van het Bijzonder Comité voor de Sociale Dienst werden er voor de heer Joris Evens geen opvolgers aangeduid.
In toepassing van artikel 95 van het decreet lokaal bestuur van 22 december 2017 werd door de leden van de Raad voor Maatschappelijk Welzijn die indertijd de heer Joris Evens voorgedragen hebben, een voordrachtsakte ingediend waarbij de heer Rob Ulenaers wordt voorgedragen als nieuw lid van het Bijzonder Comité voor de

Sociale Dienst. Deze voordrachtsakte werd bezorgd aan de algemeen directeur op 7 februari 2022 en bezorgd aan de voorzitter van de raad voor maatschappelijk welzijn op 7 februari 2022.
Uit onderzoek van de geloofsbrieven blijkt dat de heer Rob Ulenaers voldoet aan de verkiesbaarheidsvoorwaarden en dat er zich geen onverenigbaarheden stellen.

Juridische context

Bevoegdheid:

Artikels 77 en 78 van het decreet lokaal bestuur van 22 december 2017 bepalen dat de raad voor maatschappelijk welzijn bevoegd is voor deze materie.

Grond:

Het besluit van de Raad voor Maatschappelijk Welzijn van 2 januari 2019 in verband met de verkiezing van de leden van het Bijzonder Comité voor de Sociale Dienst.
Hoofdstuk 6, afdeling 1 van het decreet lokaal bestuur van 22 december 2017 in verband met de organisatie van het Bijzonder Comité voor de Sociale Dienst.

Adviezen en inspraak

Er werd voorafgaand geen advies ingewonnen en er vond geen inspraak plaats.

Plaats in het meerjarenplan en financiële gevolgen

De uitvoering van het besluit heeft geen link met het meerjarenplan.

Neemt kennis van:

Artikel 1

Het ontslag van de heer Joris Evens als lid van het Bijzonder Comité voor de Sociale Dienst vanaf 1 maart 2022.

Artikel 2

De geloofsbrieven van de heer Rob Ulenaers worden onderzocht. Hieruit blijkt dat er geen onverenigbaarheid is. De Raad voor Maatschappelijk Welzijn neemt dan ook kennis van de eedaflegging door de heer Rob Ulenaers, die in openbare vergadering en in handen van de voorzitter van Raad voor Maatschappelijk Welzijn de volgende eed aflegt conform artikel 96 § 1 van het decreet lokaal bestuur van 22 december 2017:

"Ik zweer de verplichtingen van mijn mandaat trouw na te komen"

Artikel 3

De aanstelling van de heer Rob Ulenaers als lid van het Bijzonder Comité voor de Sociale Dienst vanaf 1 maart 2022.

Artikel 4

Tegen dit besluit kan een klacht worden ingediend bij de toezichthoudende overheid. Deze klacht moet ingediend worden binnen een periode van 30 dagen die volgt op de dag van de bekendmaking van dit besluit op de website van de gemeente Oudsbergen.

De klacht kan via een aangetekend schrijven gericht worden aan:

Agentschap Binnenlands Bestuur
VAC Herman Teirlinck Brussel
Havenlaan 88, bus 70
1000 Brussel

De klacht kan ook via een aangetekende e-mail verstuurd worden naar: binnenland@vlaanderen.be

Artikel 5

Dit besluit wordt overeenkomstig de bepalingen uit artikels 285 tot en met 287 van het decreet lokaal bestuur bekendgemaakt op de website van de gemeente Oudsbergen.

Een afschrift van het proces-verbaal van eedaflegging van dhr. Rob Ulenaers wordt aan de voorzitter van het Bijzonder Comité voor de Sociale Dienst bezorgd.

04. Goedkeuring van het beleid voor informatieveiligheid

contactpersoon	**functie**	**e-mail**	**dossier**
Karla Louis	diensthoofd ICT	karla.louis@oudsbergen.be	AD18.000001

Voorgeschiedenis en verwijzingsdocumenten

De Vlaamse Toezichtcommissie (VTC) heeft aan de lokale besturen geadviseerd om hun beleid voor informatieveiligheid uit te breiden met een formele omschrijving van de rollen en verantwoordelijkheden voor de beveiliging van gegevens, zowel fysiek als digitaal.

Tevens dienen ook de logcontroles in het informatieveiligheidsbeleid te worden opgenomen.

Argumentatie

Elke medewerker van het OCMW werkt dagelijks met verschillende soorten informatie langs verschillende kanalen. Het is decretaal verplicht om een informatieveiligheidsbeleid op te stellen om op een verantwoorde manier om te gaan met informatie.

Om deze reden wordt in het document beleid voor informatieveiligheid een gestructureerde aanpak van de informatieveiligheid opgesteld, die gebruikt wordt als uitgangspunt voor de gehele informatievoorziening. Van belang daarbij is de aandacht voor de natuurlijke spanning die bestaat tussen enerzijds beveiligingseisen die beperkingen stellen en kosten met zich meebrengen, en anderzijds verwachtingen van gebruikers omtrent eenvoud, flexibiliteit en toegankelijkheid. Om de juiste balans te vinden, worden de risico's zorgvuldig gewogen.

Het beleid voor informatieveiligheid is opgesteld door de functionaris voor gegevensbescherming of data protection officer (DPO) van de Welzijnsregio Noord-Limburg, waarbij rekening werd gehouden met de adviezen van de Vlaamse Toezichtcommissie.

Op basis van dit beleid zijn concrete acties uitgewerkt die in het informatieveiligheidsplan zijn beschreven.

Juridische context

Bevoegdheid:

Artikels 77 en 78 van het decreet lokaal bestuur van 22 december 2017 bepalen dat de raad voor maatschappelijk welzijn bevoegd is voor deze materie.

Grond:

De Europese Algemene Verordening Gegevensbescherming (AVG) – Verordening 2016/679 van het Europees parlement en de raad van 27 april 2016 die de regels voor de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en het vrije verkeer van die gegevens door particuliere bedrijven en overheidsinstanties in de hele Europese Unie standaardiseert en tot intrekking van richtlijn 95/46/EG.

Het gewijzigde egov-decreet van 25 mei 2018

Het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer.

Adviezen en inspraak

Het beleid voor informatieveiligheid is opgesteld door de functionaris voor gegevensbescherming of data protection officer (DPO) van de Welzijnsregio Noord-Limburg.

Plaats in het meerjarenplan en financiële gevolgen

De uitvoering van dit besluit kadert binnen het meerjarenplan:
- beleidsdoelstelling : 20BD08
- beleidsdoelstelling omschrijving : Organisatiebeheersing
- actieplan nummer : 20BD08AP02
- actieplan omschrijving : Informatica
- actie nummer : 20BD08AP02A01
- actie omschrijving : Het garanderen van goede IT-applicaties en software in Oudsbergen

Er zijn echter geen financiële consequenties verbonden aan de uitvoering van dit besluit.

Stemming, na beraadslaging

Met unanimiteit van stemmen.

Besluit

Artikel 1

De raad voor maatschappelijk welzijn keurt het beleid voor informatieveiligheid zoals hieronder opgenomen goed.

1. Inleiding

Het lokaal bestuur verzamelt en beheert vanuit haar wettelijke opdracht een veelheid aan informatie. Het gaat hierbij onder andere om gegevens van burgers en medewerkers van het lokaal bestuur. Het lokaal bestuur is wettelijk verplicht om deze informatie op gepaste wijze te beveiligen.
Informatieveiligheid beschermt de informatie tegen een brede waaier aan bedreigingen, zorgt voor de continuïteit van de dienstverlening en draagt bij aan een kwaliteitsvolle, transparante en toegankelijke dienstverlening.
In het lokaal bestuur is sprake van toenemende afhankelijkheid van informatie- en computersystemen, waardoor nieuwe kwetsbaarheden en risico's kunnen optreden.
Om deze reden wordt in dit document een gestructureerde aanpak van de informatieveiligheid voorgesteld, die gebruikt wordt als uitgangspunt voor de gehele informatievoorziening. Van belang daarbij is aandacht voor de

natuurlijke spanning die bestaat tussen enerzijds beveiligingseisen die beperkingen stellen en kosten met zich meebrengen, en anderzijds verwachtingen van gebruikers omtrent eenvoud, flexibiliteit en toegankelijkheid. Om de juiste balans te vinden, worden de risico's zorgvuldig gewogen.

1.1. Definitie informatieveiligheid en doelstelling

Onder informatieveiligheid verstaan we het samenhangend pakket aan maatregelen, procedures en processen die de beschikbaarheid, integriteit, vertrouwelijkheid en auditeerbaarheid van alle vormen van informatie garanderen, met als doel de continuïteit van de informatie en de informatievoorziening, inclusief de onderliggende ICT-infrastructuur, te waarborgen en de eventuele gevolgen van beveiligingsincidenten tot een acceptabel, vooraf bepaald niveau te beperken.

- **Beschikbaarheid**: het waarborgen dat de geautoriseerde gebruikers op de juiste momenten tijdig toegang hebben tot de informatie en informatiesystemen. Het betreft m.a.w. de mate waarin gegevens of functionaliteit op de juiste momenten beschikbaar zijn voor gebruikers.
- **Integriteit**: staat in het teken van het behouden en beschermen van de juistheid van data en het voorkomen dat data onbedoeld aangepast wordt.
- **Vertrouwelijkheid**: het waarborgen dat informatie alleen toegankelijk is voor diegenen die hiervoor bevoegd zijn.

Het informatieveiligheidsbeleid dient als leidraad voor de aansturing en coördinatie van de verschillende beveiligingsprocessen. Het uiteindelijke doel is het inrichten van een evenwichtig stelsel van beveiligingsmaatregelen, gericht op risicobeheersing.
Met evenwichtig bedoelen we in dit verband het vinden van een optimum tussen werkbaarheid en veiligheid. Maximale veiligheid is immers absoluut onwerkbaar, maar maximale werkbaarheid is absoluut onveilig. Het optimum is een punt waarbij ernstige informatiebeveiligingsrisico's worden beperkt, maar nog wel een zeker risico bewust wordt genomen, opdat de werkbaarheid niet in het gedrang komt.
Informatieveiligheid is geen opdracht die op zichzelf staat. Het maakt deel uit van het DNA van het lokaal bestuur. Informatieveiligheid vormt een ondeelbaar geheel met de manier waarop we iedere dag omgaan met informatie tijdens elke activiteit op de werkvloer, tijdens elk contact met de burger, bedrijven, andere overheden en organisaties. Hoe triviaal deze interacties soms lijken te zijn, telkens is er een wisselwerking aan informatiestromen en processen die de noodzakelijke beschermende maatregelen verantwoorden, op maat van de toepassing en het achterliggende proces.
Dit document bevat een strategie met voorgestelde doelstellingen en aanpak m.b.t. informatieveiligheid binnen het lokaal bestuur en binnen de dienstverlening aangeboden door het lokaal bestuur. Het wil op die manier een antwoord bieden aan de uitdagingen rond een veilige informatieverwerking binnen het lokaal bestuur.
Het informatieveiligheidsbeleid is noodzakelijkerwijs relatief abstract van aard. Nadere concretisering volgt in het informatieveiligheidsplan, waarin onder andere wordt vastgesteld welke methoden gebruikt worden, welke maatregelen worden uitgevoerd, en hoe de juiste werking daarvan wordt gecontroleerd.

1.2. Toepassingsgebied

Het informatieveiligheidsbeleid is van toepassing op alle medewerkers van het lokaal bestuur, gaande van de burgemeester, het schepencollege, de algemeen directeur, de gemeenteraadsleden, de OCWM-raadsleden en het gemeente- en OCMW-personeel, tot alle externe krachten die tijdelijk of voor onbepaalde duur werkzaam zijn binnen het lokaal bestuur en die rechtstreeks of onrechtstreeks in contact komen met het lokaal bestuur. Naleving van dit beleid vormt een voorwaarde om toegang tot de informatie en informatiesystemen te krijgen.
Daarnaast is het informatieveiligheidsbeleid van toepassing op het gehele proces van informatievoorziening en geldt dit beleid gedurende de volledige levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie.
Tot slot dient opgemerkt te worden dat er een belangrijke relatie en een gedeeltelijke overlap bestaat met aanpalende beleidsterreinen zoals onder meer fysieke beveiliging, human resources en business continuity. Op al deze terreinen zal aandacht worden geschonken aan de raakvlakken en zal er afgestemd worden.

1.3. Ambitie

We streven ernaar om de data van de burgers en medewerkers van het lokaal bestuur te waarborgen. We willen dit doen door het huidige niveau van veiligheid structureel naar een hoger informatieveiligheidsniveau te brengen en daar te houden, waar het mogelijk is, en minstens het huidige niveau van veiligheid behouden.
Dit willen we bereiken door verdere versterking van de maatregelen door te voeren, door kwaliteitsvolle, transparante en toegankelijke dienstverlening te garanderen en door ervoor te zorgen dat incidenten beperkt blijven.
Daarnaast hebben we de volgende doelstellingen:

- De instandhouding en de goede werking van de activiteiten van het lokaal bestuur garanderen.
- Het voorkomen van schade die kan worden toegebracht aan de goede werking van de informatiesystemen van de Sociale Zekerheid en het Rijksregister enerzijds, en aan de persoonlijke levenssfeer van de betrokkenen anderzijds.
- Een gezond evenwicht vinden tussen een aantal preventieve maatregelen (om beveiligingsincidenten te voorkomen) en correctieve maatregelen (om de negatieve gevolgen van incidenten te beperken).
- Het vertrouwen van de burger, onderneming en/of vereniging versterken door data te beveiligen tegen verlies, onrechtmatig gebruik, …
- De reputatie van het lokaal bestuur als betrouwbare partner versterken.
- De bedrijfscontinuïteit optimaliseren tijdens en na een ernstig incident.
- De weerbaarheid tegen cybercriminaliteit verbeteren, nl. zowel aanvallen op de toepassingen, netwerken en informatie onder vorm van ransomware als andere malware.
- De technologische evoluties met vertrouwen kunnen benutten als organisatie.

1.4. Beheer van het beleidsdocument

Het informatieveiligheidsbeleid wordt periodiek, of zodra zich belangrijke wijzigingen voordoen, beoordeeld en zo nodig bijgesteld. Bij deze actualisatie worden nieuwe ontwikkelingen op het terrein van de bedrijfsvoering en op het terrein van informatieveiligheid en privacy meegenomen. De functionaris voor gegevensbescherming is verantwoordelijk voor het bijstellen en actueel houden van het informatieveiligheidsbeleid.
Het informatieveiligheidsbeleid wordt van kracht na goedkeuring door het college van burgemeester en schepenen. Bij het van kracht worden van dit document, worden vorige versies van het informatieveiligheidsbeleid ingetrokken.

2. Informatieveiligheidsorganisatie

2.1. Eindverantwoordelijkheid

De algemeen directeur is als verantwoordelijke voor het dagelijks bestuur de eindverantwoordelijke voor de naleving en toepassing van informatieveiligheid binnen het lokaal bestuur.
Hij zorgt ervoor dat het informatieveiligheidsbeleid de missie/visie van het lokaal bestuur ondersteunt en benadrukt het belang van informatieveiligheid binnen het lokaal bestuur en de verplichting om de voorwaarden van dit beleid na te leven.
De algemeen directeur:

- Vergewist zich van de nodige logistieke en financiële steun voor de implementatie en toepassing van het beleid;
- Zorgt ervoor dat de organisatorische structuur die noodzakelijk is voor een goed beheer van de informatieveiligheid wordt geïmplementeerd;
- Krijgt jaarlijks een verslag van de functionaris voor gegevensbescherming over de toepassing en de maturiteit van het informatieveiligheidsbeleid.

2.2. Rollen binnen de informatieveiligheidsorganisatie

Om de informatiebeveiliging gestructureerd en gecoördineerd in goede banen te kunnen leiden, werden aan de volgende actoren specifieke taken, bevoegdheden en verantwoordelijkheden toegewezen.

2.2.1. Het college van burgemeester en schepenen

Het college van burgemeester en schepenen is verantwoordelijk voor de volgende punten op vlak van informatiebeveiliging:

- Het vaststellen van het informatieveiligheidsbeleid

- Het vaststellen van het informatieveiligheidsplan
- Het vaststellen van het budget voor informatieveiligheid

2.2.2. Het managementteam

In het kader van informatieveiligheid, zorgt het managementteam voor:

- De naleving en toepassing van de informatieveiligheid binnen de organisatie;
- Dat de missie/visie van het lokaal bestuur wordt ondersteund door het informatieveiligheidsbeleid;
- Het benadrukken van het belang van informatieveiligheid binnen de organisatie en de verplichting om de voorwaarden van het informatieveiligheidsbeleid na te leven;
- Het intern controlesysteem van de organisatie waar informatieveiligheid deel van uitmaakt.

2.2.3. De functionaris voor gegevensbescherming

De functionaris voor gegevensbescherming heeft de adviserende, stimulerende, documenterende en controlerende opdracht in het kader van de informatieveiligheid na aanstelling door het lokaal bestuur.
Er is een nauwe samenwerking tussen de functionaris voor gegevensbescherming en beleidsmedewerkers van het lokaal bestuur voor de uitvoering van zijn taken. De functionaris voor gegevensbescherming is de expert voor het lokaal bestuur op het vlak van informatieveiligheid, maar er worden onderling afspraken gemaakt om het informatieveiligheidsbeleid in de organisatie uit te rollen.
Volgende taken dient de functionaris voor gegevensbescherming uit te voeren (in samenwerking met de beleidsmedewerkers):

- De functionaris voor gegevensbescherming adviseert de algemeen directeur en/of het managementteam, op hun verzoek of op eigen initiatief, omtrent alle aspecten van informatieveiligheid. Het advies wordt schriftelijk en gemotiveerd uitgebracht tenzij de risico's onvoldoende ernstig zijn.
- De functionaris voor gegevensbescherming bevordert de naleving van de veiligheidsvoorschriften opgelegd vanuit de regelgeving en draagt bij tot het bewustzijn van de medewerkers omtrent het belang van informatieveiligheid.
- De functionaris voor gegevensbescherming stimuleert de implementatie, opvolging en evaluatie van de informatieveiligheid binnen de organisatie.
- De functionaris voor gegevensbescherming brengt de nodige documentatie aan met betrekking tot informatieveiligheid.
- De functionaris voor gegevensbescherming ziet toe op de naleving binnen het lokaal bestuur van de veiligheidsvoorschriften opgelegd door of krachtens een wets- of reglementsbepaling.
- De functionaris voor gegevensbescherming stelt jaarlijks een verslag op over de maturiteit van het informatieveiligheidsbeleid.
- De functionaris voor gegevensbescherming organiseert adviescommissies informatieveiligheid beleid en IT om regionale onderwerpen betreffende informatieveiligheid over de aangesloten besturen heen aan te pakken.

2.2.4. De informatieveiligheidscel

De informatieveiligheidscel is bij voorkeur samengesteld uit alle actoren die invloed hebben op (een aspect van) informatieveiligheid binnen het lokaal bestuur, zoals de functionaris voor gegevensbescherming, de adjunct-DPO, de algemeen directeur, een deskundige IT, een beleidsmedewerker,…
De informatieveiligheidscel volgt de uitvoering van het beveiligingsbeleid op, voert het informatieveiligheidsplan uit en heeft een adviserende, stimulerende, documenterende en controlerende opdracht op het vlak van informatieveiligheid.
De cel wordt op de hoogte gebracht van incidenten en risico's die de informatieveiligheid in gedrang brengen en de hieromtrent genomen maatregelen.
De adjunct-DPO is het aanspreekpunt voor de functionaris voor gegevensbescherming.

2.2.5. De dienst ICT

In de praktijk zijn het ICT-beleid en het informatieveiligheidsbeleid sterk met elkaar verweven. Een ICT-deskundige is daarom in de dagelijkse werking een belangrijke actor in de realisatie in het werkveld van een afdoend informatieveiligheidsbeleid. Deze ICT-deskundige zorgt voor de effectieve praktische vertaling van de richtlijnen in de dagelijkse werking omtrent ICT.
Bij het bepalen van het beleid en de geschikte beheersmaatregelen, wordt de dienst ICT betrokken.

2.2.6. De projectleiders

De projectleiders zijn er verantwoordelijk voor dat, in geval persoonsgegevens worden verwerkt in de loop van het project, het project voldoet op het vlak van informatieveiligheid aan de toepasselijke wet- en regelgeving.
De projectleiders lichten de informatieveiligheidscel in over het toekomstige project vooraleer dit van start gaat.
Samen met de informatieveiligheidscel wordt bekeken op welke manier aan het project uitvoering kan worden gegeven.

2.2.7. De medewerkers

De diensthoofden en leidinggevenden zijn de primair verantwoordelijken voor het uitvoeren en handhaven van de maatregelen betreffende informatieveiligheid.
De medewerkers zijn geïnformeerd over hun beveiligingsplichten inzake omgang met vertrouwelijke gegevens, de na te leven procedures bij vaststelling van een veiligheidsprobleem en over de eventuele disciplinaire sancties en procedures die bij tekortkomingen worden toegepast.

2.2.8. Externe partijen

Met externe partijen moeten afspraken worden gemaakt en gedocumenteerd om de bescherming van de bedrijfsmiddelen te waarborgen. Alle relevante informatiebeveiligingseisen moeten worden vastgesteld en overeengekomen met elke partij die toegang heeft tot ICT-infrastructuur, informatie van de organisatie of de informatie verwerkt.
De dienstverlening wordt periodiek geëvalueerd en beoordeeld waardoor veranderingen in deze dienstverlening kunnen worden geremedieerd.

3. Informatieveiligheidsbeleid

3.1. Uitgangspunten

Informatieveiligheid binnen de organisatie beoogt de instandhouding en de goede werking van de activiteiten ervan, hoofdzakelijk gericht op het voorkomen van schade. Dat houdt onder meer 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 filosofie is dat het bestuur een open instelling is, waar veel mogelijk is. De benadering van ICT en beveiliging is minder open. Er wordt van medewerkers en mandatarissen 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 zijn geformuleerd en geïmplementeerd.
De beveiliging dient te voldoen aan de relevante wet- en regelgeving, in het bijzonder aan de Europese GDPR, de federale privacywet en alle navolgende wet- en regelgevingen.
Het lokaal bestuur hanteert de volgende beleidsprincipes:
Informatiebeveiliging is ieders verantwoordelijkheid. Van medewerkers, mandatarissen en derden wordt er verwacht dat ze actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie. Dat gebeurt in de aanstellingsbrief, tijdens functioneringsgesprekken, met een gedragscode die geldt voor de volledige organisatie, met periodieke bewustwordingscampagnes,... Het opleggen van sancties na overtredingen maakt het geheel geloofwaardig.
Informatiebeveiliging is een continu proces. Technologische en organisatorische ontwikkelingen binnen en buiten de organisatie maken het noodzakelijk om periodiek te bekijken of de beveiliging nog voldoende wordt gewaarborgd. Audits maken het mogelijk het beleid en de genomen maatregelen te controleren op efficiëntie.
Eigendom van informatie. Het lokaal bestuur is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd, tenzij dit voor bijvoorbeeld onderzoek anders is overeengekomen.
Medewerkers moeten goed geïnformeerd zijn over de regelgeving voor het (her)gebruik van deze informatie.
Waardering van informatie. Iedereen behoort de waarde van informatie te kennen en daarnaar te handelen. Deze waarde wordt bepaald door de schade als gevolg van verlies van beschikbaarheid, integriteit en vertrouwelijkheid.
Privacy by design. Bij projecten, zoals infrastructurele wijzigingen of de aanschaf van nieuwe systemen, wordt vanaf de start rekening gehouden met informatiebeveiliging en gegevensbescherming.
Functionaris voor gegevensbescherming. Er is een functionaris voor gegevensbescherming aangesteld voor het lokaal bestuur. De functionaris voor gegevensbescherming stelt het informatieveiligheidsbeleid en -plan op en

ziet binnen de organisatie toe op de naleving ervan en van de daaruit voortvloeiende maatregelen. Daarnaast zorgt de functionaris voor gegevensbescherming voor onderzoek, voert hij controles uit, adviseert hij in complexe beveiligingsvraagstukken, initieert hij risicoanalyses en vervult hij een adviserende rol naar het lokaal bestuur.
Informatieveiligheidscel. Er is een informatieveiligheidscel opgericht. In deze cel zitten de belanghebbende stakeholders en de DPO. Deze cel ziet toe op de uitvoering van het informatieveiligheidsbeleid.

3.2. Beleidsmaatregelen

3.2.1. Beleid en organisatie

§1. De organisatie doet beroep op de Dienst Informatieveiligheid en de functionaris voor gegevensbescherming van Welzijnsregio Noord-Limburg. Deze is middels raadsbeslissing aangesteld voor een tijdsequivalent van 6 uur/week.
§2. De functionaris voor gegevensbescherming van Welzijnsregio Noord-Limburg zorgt voor de sturing van het informatieveiligheidsbeleid: opstelling en herziening van het beleid, bijstelling van de beleidsmaatregelen, opstelling van het plan voor informatieveiligheid, opstelling van de vereiste policy's en procedures, de vaststelling van verantwoordelijkheden en het toezicht op veranderende bedreigingen en incidenten.
§3. De organisatie duidt een adjunct-DPO aan die de rechtstreekse contactpersoon zal zijn van de functionaris voor gegevensbescherming van Welzijnsregio Noord-Limburg en de nodige informatie met de functionaris voor gegevensbescherming zal uitwisselen.
De adjunct-DPO neemt deel aan de Adviescommissies Informatieveiligheid van Welzijnsregio Noord-Limburg.
De adjunct-DPO kan optreden voor zowel OCMW als gemeentebestuur, of de organisatie kan hiervoor twee verschillende adjuncten aanstellen.
§4. De organisatie verbindt er zich toe de functionaris voor gegevensbescherming te voorzien van de noodzakelijke informatie, zodanig dat hij/zij over de nodige gegevens kan beschikken die nodig zijn voor het uitvoeren van zijn/haar opdracht.
§5. In dit kader worden de verantwoordelijken voor informatiebeveiliging aangeduid.
§6. Bijzondere aandacht wordt besteed aan de organisatorische aspecten van de samenwerking met derden (bv. uitbestedingstaken). De veiligheidsaspecten van de samenwerking worden contractueel vastgelegd.
§7. In het kader van de fysieke beveiliging en de beveiliging van de omgeving dienen de informatieveiligheidsdienst en de preventieadviseur nauw met elkaar samen te werken.
§8. In het kader van het operationeel beheer, de logische toegangsbeveiliging en de ontwikkeling en onderhoud van systemen, dienen de informatieveiligheidsdienst en systeembeheerders (informatici,...) nauw met elkaar samen te werken.

3.2.2. Classificatie en beheer van bedrijfsmiddelen

§1. Er wordt rekening mee gehouden dat er omgegaan wordt met vertrouwelijke gegevens. De behandeling van deze gegevens is onderworpen aan de wetgeving i.v.m. de persoonlijke levenssfeer met inbegrip van de wetgeving in verband met medische gegevens.
§2. Vertrouwelijke of persoonlijke gesprekken worden steeds gevoerd met aandacht voor de omgeving. Wanneer met cliënten/burgers in deze context ontvangt, gebeurt dit in de daarvoor voorziene ruimtes en doet men de deur dicht om de privacy te garanderen. (Team)overleg wordt zo gepleegd dat enkel de betrokken personeelsleden het gesprek kunnen meevolgen.
§3. Er wordt een clean-screen mentaliteit toegepast op alle werkstations. Wanneer men het werkstation verlaat, vergrendelt men de computer met behulp van de toetsencombinatie windows-toets + L. Ter aanvulling wordt op elk werkstation een screensaver met vergrendeling ingevoerd die actief wordt na 15 minuten inactiviteit. Er moet voor gezorgd worden dat derden niet onbedoeld kunnen meekijken op het scherm.
§4. Er wordt een clear-desk mentaliteit toegepast in alle bureaus. Gegevensdragers waarop persoonsgegevens aanwezig zijn, worden niet onbeheerd achtergelaten of worden afgeschermd van derden. Hieronder wordt verstaan: papieren dossiers, notities, USB-sticks, smartphone,...
§5. Vertrouwelijke of persoonlijke telefoongesprekken worden steeds gevoerd met aandacht voor de omgeving. Wanneer een vertrouwelijk telefoongesprek gevoerd moet worden, sluit men best de deur. Indien er onverwachts toch andere personen in de buurt zijn, probeert men het gesprek zo discreet mogelijk te voeren (bv. geen namen noemen, ...).
§6. Papier dat persoonlijke informatie bevat, wordt versnipperd alvorens het weg te gooien. Men laat geen persoonlijke informatie rondslingeren in een prullenmand/papierbak.

§7. Alle medewerkers zijn zich bewust van de verschillende klassen waarin informatie kan ingedeeld worden en de bijbehorende risico's, en handelen hier ook naar:

- 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: het gaat om 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.

3.2.3. Aan medewerkers gerelateerde veiligheid

§1. Medewerkers moeten zich bewust zijn van de bedreigingen voor en het belang van informatieveiligheid en moeten daartoe de juiste middelen, kennis en vaardigheden tot hun beschikking hebben.
§2. Er moet rekening mee gehouden worden dat de medewerkers van de organisatie op verschillende locaties werken. In elk van deze locaties kunnen specifieke veiligheidsmaatregelen van kracht zijn.
§3. Het personeelsbeleid draagt hiertoe bij, door de opname van informatieveiligheidsaspecten en de verantwoordelijkheid van de werknemer op het gebied van informatieveiligheid op te nemen in de deontologische code en/of het arbeidsreglement en/of het arbeidscontract.
§4. Elke medewerker heeft de plicht om beveiligingsrisico's en beveiligingsincidenten te melden.
§5. Medewerkers worden gewezen op hun verantwoordelijkheid voor het handhaven van een effectieve toegangsbeveiliging, met name met betrekking tot het gebruik van wachtwoorden, MFA en beveiliging van gebruikersapparatuur. Wachtwoorden zijn strikt persoonlijk en vertrouwelijk.
§6. Men moet zich steeds bewust zijn van welke informatie men aan wie kan en mag doorgeven. Controleer steeds of de aanvrager wel degelijk recht heeft op de informatie. Wanneer men gebonden is aan het beroepsgeheim, dient men zich hier steeds aan te houden.
§7. Medewerkers worden gewezen op de veiligheidsrisico's die elektronische kantoorsystemen met zich meebrengen (vb. computers, mobiele computers, telefoons, mobiele telefoons, e-mail, post, voicemail, postdiensten, …): deze systemen houden een risico in voor de vertrouwelijkheid van bedrijfsgegevens.
§8. Het gebruik van bedrijfsmiddelen voor privédoeleinden moet tot een strikt minimum beperkt blijven.
§9. Medewerkers worden gewezen op hun verantwoordelijkheid bij het gebruik van bedrijfsmiddelen.
§10. Op apparatuur die verbonden is met de infrastructuur/het netwerk van de organisatie (bv. pc's) mag alleen hardware aangesloten worden, software geïnstalleerd worden en/of configuraties ingesteld worden door de bevoegde diensten aangesteld door de organisatie.
§11. Bij het verlaten van de dienst of bij wijziging van functie-inhoud worden toegangsrechten en autorisaties zo snel mogelijk aangepast en wordt materiaal indien nodig gerecupereerd.
§12. De schending van het beveiligingsbeleid en de beveiligingsprocedures van de organisatie worden middels een formeel proces afgehandeld.

3.2.4. Fysieke beveiliging en beveiliging van de omgeving

§1. Bij integratie van andere diensten in het gebouw, wordt er rekening gehouden met het verhoogde risico op onbevoegde toegang.
§2. De ramen van alle lokalen worden na de werkdag steeds afgesloten. Ieder personeelslid is verantwoordelijk voor het correct afsluiten van zijn eigen bureel. Voor gezamenlijke ruimtes en de afsluiting van het gebouw wordt een verantwoordelijke aangeduid of worden er afspraken gemaakt.
§3. Tijdens de openingsuren bewaart het baliepersoneel het overzicht over wie het gebouw betreedt. Bezoekers moeten zich steeds aanmelden alvorens ze zich naar het spreekuur/hun afspraak kunnen begeven. Dit wordt duidelijk aangegeven.
§4. De toegang tot het gebouw wordt buiten de openingsuren beperkt tot het personeel, dat toegang heeft door middel van een persoonlijke code. De persoon die als laatste het gebouw verlaat, zorgt ervoor dat de deuren afgesloten zijn.

§5. Personen die een afspraak hebben buiten de openingsuren, worden binnengelaten door iemand van het personeel en naar hun afspraak begeleid. Men verzekert zich ervan dat alle bezoek het gebouw ook effectief verlaat.
§6. Bij het opmerken van “verdwaalde” personen, probeert men te voorkomen dat deze personen ergens terecht komen waar ze niet moeten zijn. Een simpele ‘Kan ik u helpen?’ doet wonderen.
§7. Worden er personen aangetroffen op verboden plaatsen, dan wordt hen vriendelijk maar kordaat duidelijk gemaakt dat zij zich moeten verwijderen.
§8. De toegang tot de serverruimte wordt beperkt. Enkel bevoegde personen krijgen toegang door middel van een sleutel.

3.2.5. Operationeel beheer

§1. Er moet rekening gehouden worden met het feit dat naarmate de zichtbaarheid van de elektronische toepassingen toeneemt, ook het risico op aanvallen op het systeem toeneemt.
§2. Verantwoordelijkheden worden vastgelegd voor het beheer en de bediening van alle ICT-voorzieningen.
§3. Bij uitbesteding van ICT-activiteiten naar een extern bedrijf, wordt extra aandacht besteed aan eventuele beveiligingsrisico’s. De beveiligingsmaatregelen worden contractueel vastgelegd.
§4. Door gepaste capaciteitsplanning en acceptatieprocedures voor nieuwe en gewijzigde ICT-systemen, wordt het risico van systeemstoringen tot een minimum beperkt.
§5. Er worden maatregelen genomen om virussen en kwaadaardige software te voorkomen, ontdekken en eventuele gevolgen ervan zo veel mogelijk in te perken. De anti-virussoftware wordt nauwkeurig up-to-date gehouden gecentraliseerd of lokaal. De anti-virussoftware mag nooit uitgeschakeld worden zonder toestemming van een bevoegde.
§6. Er worden dagelijks back-ups gemaakt van essentiële informatie en software om de integriteit, beschikbaarheid en continuïteit van de diensten te handhaven. Deze back-ups worden bewaard op een veilige locatie, dit zowel qua toegang als locatie.
§7. Speciale aandacht wordt besteed aan de beveiliging van informatie in netwerken en de bescherming van de ondersteunende infrastructuur. Maximale maatregelen worden genomen bij het transport van gevoelige gegevens via openbare netwerken (vb. internet).
§8. Opslagmedia worden beveiligd tegen schade, diefstal en ongeoorloofde toegang/badge.
§9. Met het oog op de naleving van de wettelijke bepalingen op de bewaring en het gebruik van gearchiveerde gegevens, moet bij elke evolutie van de informatica-infrastructuur en het informatiesysteem nagegaan worden of de gearchiveerde gegevens, de opslagmedia en de noodzakelijke applicaties nodig voor hun exploitatie, op elkaar afgestemd blijven.
§10. Maatregelen worden genomen om te voorkomen dat informatie die wordt uitgewisseld met andere organisaties, verloren gaat, gewijzigd of misbruikt wordt.
§11. Aandacht wordt besteed aan het beschermen van de integriteit van informatie op publiek toegankelijke systemen (zoals webservers) om ongeoorloofde wijzigingen te voorkomen die de instelling of één van de organisaties van de Sociale Zekerheid zouden kunnen schaden.
§12. Indien media en/of informatie vernietigd moeten worden, dient dit te gebeuren op een niet-herstelbare wijze.

3.2.6. Logische toegangsbeveiliging

§1. Rekening wordt gehouden met het feit dat binnen de organisatie omgegaan wordt met vertrouwelijke gegevens en dat de beperking van toegang tot informatie en bedrijfsprocessen van primordiaal belang is.
§2. Functionele eisen voor toegangsbeveiliging (identificatie, authenticatie en autorisatie) worden gedefinieerd en gedocumenteerd.
§3. Procedures worden vastgelegd om alle fases in de levenscyclus van een autorisatie te beheren. (vb. creatie, wijziging, controle, opheffing)
§4. Wachtwoorden worden beheerd aan de hand van een formeel proces.
§5. De toewijzing en het gebruik van speciale, kritieke bevoegdheden worden beperkt en gecontroleerd.
§6. Gebruikers worden gewezen op hun verantwoordelijkheden voor het handhaven van een effectieve toegangsbeveiliging, met name met betrekking tot het gebruik van wachtwoorden en beveiliging van gebruikersapparatuur.
§7. Toegang tot interne en externe netwerkdiensten wordt op afdoende manier beschermd. Ook wordt bijzondere aandacht besteed aan de beveiliging van de toegang op afstand.

§8. Specifieke maatregelen worden uitgewerkt voor de toegangsbeveiliging voor besturingssystemen en toepassingen.
§9. Toegang tot en gebruik van systemen kan gemonitord worden om afwijkingen van het toegangsbeleid of anomalieën te detecteren.
§10. Voor toegang op afstand worden speciale veiligheidsmaatregelen genomen in overeenstemming met de risico's verbonden aan deze manier van werken.
§11. Voor gebruik van mobiele opslagmedia die de beveiligingsperimeter van de instelling kunnen verlaten, worden gepaste veiligheidsmaatregelen genomen.

3.2.7. Ontwikkeling en onderhoud van systemen
§1. Voor nieuwe systemen of uitbreidingen van bestaande systemen, dienen de veiligheidsvereisten gespecificeerd te worden.
§2. De ontwikkeling wordt gebaseerd op een gestructureerde aanpak die de veiligheidsvereisten oplegt.
§3. Bijzondere aandacht wordt besteed aan de uitwerking van documentatie bij de ontwikkeling van nieuwe en het onderhoud van bestaande systemen.
§4. Bij de ontwikkeling van toepassingssystemen dient bijzondere aandacht besteed te worden aan de validatie van invoergegevens, de beveiliging van interne verwerking en de validatie van uitvoergegevens.
§5. Maximale maatregelen worden genomen om te vermijden dat geheime communicatiekanalen in systemen verborgen worden. Het nazicht van software door andere partijen dan de ontwikkelaars is een methode om deze risico's in te perken.
§6. Bij de ontwikkeling van toepassingssystemen moet rekening gehouden worden met gekende zwakke punten op het gebied van veiligheid, eigen aan programmeertalen. Het nazicht van software door andere partijen dan de ontwikkelaars is een methode om deze risico's in te perken.
§7. Het beschermen van de vertrouwelijkheid, de authenticiteit en de integriteit van de informatie steunt op gepaste cryptografische beveiligingsmaatregelen (versleuteling, digitale handtekening, ...). Hierbij wordt bijzondere aandacht besteed aan de bescherming van cryptografische sleutels. Waar nodig ondersteunen deze technieken ook de onweerlegbaarheid van de gegevens.
§8. De integriteit van informaticasystemen wordt gewaarborgd door een goed beheer van de software op operationele systemen en de toegangsbeveiliging voor softwarebibliotheken.
§9. Formele procedures voor het beheer van wijzigingen worden gebruikt om de kans op verminking van informatiesystemen tot een minimum te beperken. In het bijzonder worden nieuwe versies van besturingssystemen met de nodige omzichtigheid benaderd.
§10. Veiligheidsmaatregelen worden genomen bij het uitbesteden van softwareontwikkeling. De veiligheidsaspecten van de samenwerking worden contractueel vastgelegd. Wijzigingen aan softwarepakketten geleverd door derden dienen zo veel mogelijk beperkt te worden.
§11. De vertrouwelijkheid van testgegevens moet op hetzelfde niveau gegarandeerd worden als operationele gegevens.
§12. Updates van besturingssystemen en toepassingen worden op gepaste wijze uitgevoerd om de veiligheid en weerbaarheid ervan te kunnen garanderen.

3.2.8. Beheer van incidenten in verband met informatieveiligheid
§1. Medewerkers hebben de plicht om risico's en veiligheidsincidenten te melden. Alle incidenten moeten overgemaakt worden aan de functionaris voor gegevensbescherming.
§2. Om een beter zicht te krijgen op eventuele risico's en incidenten, wordt er een register bijgehouden.
§3. Het beleid, de policy's, de procedures en het veiligheidsplan worden elk jaar geëvalueerd en eventueel aangepast. Belangrijke wijzigingen worden steeds bekend gemaakt.
§4. Volgende situaties dienen gemeld en geregistreerd te worden. Deze lijst is niet-limitatief. Geregistreerde incidenten moeten op regelmatige basis besproken en geëvalueerd worden op de cel informatieveiligheid.

- Niet-verklaarbare onregelmatigheden in logfiles van systemen en applicaties;
- Verlies van een informatiebron;
- Ongeplande uitval van informatiesystemen langer dan 1 dag waarvan de systeembeheerder oordeelt dat dit een incident is;
- Inbraak op een systeem (of vermoeden van);
- Misbruik van een systeem of gegevens door een legitieme gebruiker (of vermoeden van).

3.2.9. Continuïteitsbeheer
§1. Zie procedure(s) voor back-up en continuïteitsbeheer.

3.2.10. Naleving
§1. De organisatie zal de wettelijke en contractuele beveiligingseisen naleven waaraan de gebruikte informatiesystemen onderworpen zijn.
§2. De toestand van het niveau van de beveiliging van de informatiesystemen (inclusief de herziening en de opvolging van de procedures) wordt regelmatig geëvalueerd op basis van het betreffende beleid. Dit zal gebeuren door interne begeleiding, interne controle, interne audit en/of externe audit.
§3. De controle op de toepassing van het veiligheidsbeleid zal mogelijk worden gemaakt met ICT-hulpmiddelen die ter beschikking gesteld worden van interne en externe auditeurs.
§4. Het beleid, de bijhorende policy's en procedures en eventuele andere nuttige documenten worden ter beschikking gesteld op een door iedereen toegankelijke plaats. Elke belangrijke toevoeging, aanpassing of verwijdering, wordt steeds bekend gemaakt.
§5. Sommige policy's en procedures zullen een verklaring inhouden die ondertekend moet worden door elk personeelslid. Zo verklaart hij/zij dat hij/zij het document gelezen heeft en verbindt hij/zij zich ertoe zich te houden aan de richtlijnen die beschreven staan in het document.
§6. Elke instelling die aangesloten is op het netwerk van de Kruispuntbank van de Sociale Zekerheid moet ten minste één keer om de vier jaar een audit organiseren met betrekking tot de situatie van de logische en fysieke veiligheid.
§7. De functionaris voor gegevensbescherming heeft een intern-auditerende functie. Hij/zij adviseert, motiveert en sensibiliseert waar en wanneer nodig.
§8. De eigenlijke implementatie en controle op de naleving van de informatieveiligheidsmaatregelen die beschreven worden in het beleid en de bijhorende policy(s en procedures, behoort tot de verantwoordelijkheid van de persoon die belast is met het dagelijks bestuur van de organisatie.
§9. Bij een eventuele niet-naleving van de informatieveiligheidsmaatregelen gebeurt de sanctionering conform de rechtspositieregeling en/of de wetgeving.
§10. Het advies van de functionaris voor gegevensbescherming kan en mag niet beschouwd worden als een garantie of pasklare oplossing voor een eventueel veiligheidsprobleem. Afhankelijk van de situatie moet de functionaris voor gegevensbescherming permanent evalueren en zijn/haar advies aanpassen.

Artikel 2

Tegen dit besluit kan een klacht worden ingediend bij de toezichthoudende overheid. Deze klacht moet ingediend worden binnen een periode van 30 dagen die volgt op de dag van de bekendmaking van dit besluit op de website van de gemeente Oudsbergen.

De klacht kan via een aangetekend schrijven gericht worden aan:

Agentschap Binnenlands Bestuur
VAC Herman Teirlinck Brussel
Havenlaan 88, bus 70
1000 Brussel

De klacht kan ook via een aangetekende e-mail verstuurd worden naar: binnenland@vlaanderen.be

Artikel 3

Dit besluit wordt overeenkomstig de bepalingen uit artikels 285 tot en met 287 van het decreet lokaal bestuur bekendgemaakt op de website van de gemeente Oudsbergen.

De raad voor maatschappelijk welzijn bezorgt een afschrift van dit besluit aan:

- dienst ICT
- de Welzijnsregio Noord-Limburg

05. Goedkeuring van het informatieveiligheidsplan

contactpersoon	functie	e-mail	dossier
Karla Louis	diensthoofd ICT	karla.louis@oudsbergen.be	AD18.000001

Voorgeschiedenis en verwijzingsdocumenten

Om het informatieveiligheidsplan op te maken, is er gebruik gemaakt van verschillende bronnen:

- Het informatieveiligheidsplan van de pre-fusie gemeente Meeuwen-Gruitrode
- Het informatieveiligheidsplan van de pre-fusie gemeente Opglabbeek
- Input van de functionaris voor gegevensbescherming van de Welzijnsregio Noord-Limburg
- Het verslag en het rapport opgemaakt door Deloitte naar aanleiding van de ICT-veiligheidsaudit, uitgevoerd in december 2020.
- De documenten aangeboden door het programma 'Cyberveilige gemeenten' die ook terug te vinden zijn via volgende url: https://www.vvsg.be/kennisitem/vvsg/cyberveilige-gemeenten
- De vragenlijst risicobeoordeling Ethias Cyber Protection in het kader van een verzekering cybercriminaliteit
- Naslagwerken zoals
    - Belgische gids voor cyberveiligheid
    - Cyberrisico's: een nieuwe dagelijkse realiteit voorgesteld in tien cases
    - Hoe reageren op een cyberaanval

Argumentatie

Elke medewerker van het OCMW werkt dagelijks met verschillende soorten informatie langs verschillende kanalen. Het is decretaal verplicht om een informatieveiligheidsbeleid op te stellen om op een verantwoorde manier om te gaan met informatie.

Het informatieveiligheidsplan is opgesteld in samenwerking met de functionaris voor gegevensbescherming of data protection officer (DPO) van de Welzijnsregio Noord-Limburg. Het plan bevat concrete acties die opgedeeld zijn in 3 subdomeinen:

- Beleidsacties
- Technische acties
- Acties op het vlak van sensibilisering

Elke actie is duidelijk omschreven, bevat de huidige status alsook een timing en wie verantwoordelijk is voor de actie.

Daarnaast zijn er ook recurrente acties gedefinieerd om periodiek de uitgevoerde acties te controleren en te beoordelen.

Juridische context

Bevoegdheid:

Artikels 77 en 78 van het decreet lokaal bestuur van 22 december 2017 bepalen dat de raad voor maatschappelijk welzijn bevoegd is voor deze materie.

Grond:

De Europese Algemene Verordening Gegevensbescherming (AVG) – Verordening 2016/679 van het Europees parlement en de raad van 27 april 2016 die de regels voor de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en het vrije verkeer van die gegevens door particuliere bedrijven en overheidsinstanties in de hele Europese Unie standaardiseert en tot intrekking van richtlijn 95/46/EG.

Het gewijzigde egov-decreet van 25 mei 2018

Het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer.

Adviezen en inspraak

Het informatieveiligheidsplan kwam tot stand in samenwerking met de functionaris voor gegevensbescherming of data protection officer (DPO) van de Welzijnsregio Noord-Limburg. De acties in het informatieveiligheidsplan werden in onderling overleg door de DPO en het diensthoofd ICT gedefinieerd.

Plaats in het meerjarenplan en financiële gevolgen

De uitvoering van dit besluit kadert binnen het meerjarenplan:
- beleidsdoelstelling : 20BD08
- beleidsdoelstelling omschrijving : Organisatiebeheersing
- actieplan nummer : 20BD08AP02
- actieplan omschrijving : Informatica
- actie nummer : 20BD08AP02A01
- actie omschrijving : Het garanderen van goede IT-applicaties en software in Oudsbergen

Er zijn echter geen financiële consequenties verbonden aan de uitvoering van dit besluit.

Stemming, na beraadslaging

Met unanimiteit van stemmen.

Besluit

Artikel 1

De raad voor maatschappelijk welzijn keurt het informatieveiligheidsplan goed.

Artikel 2

De raad voor maatschappelijk welzijn delegeert de opvolging van het informatieveiligheidsplan aan het vast bureau. De uitvoering van het informatieveiligheidsplan wordt eveneens 3-maandelijks opgevolgd in de cel informatieveiligheid.

De raad voor maatschappelijk welzijn wordt jaarlijks op de hoogte gebracht van de stand van zaken.

Artikel 3

Tegen dit besluit kan een klacht worden ingediend bij de toezichthoudende overheid. Deze klacht moet ingediend worden binnen een periode van 30 dagen die volgt op de dag van de bekendmaking van dit besluit op de website van de gemeente Oudsbergen.

De klacht kan via een aangetekend schrijven gericht worden aan:

Agentschap Binnenlands Bestuur
VAC Herman Teirlinck Brussel
Havenlaan 88, bus 70
1000 Brussel

De klacht kan ook via een aangetekend e-mail verstuurd worden naar: binnenland@vlaanderen.be

Artikel 4

Dit besluit wordt overeenkomstig de bepalingen uit artikels 285 tot en met 287 van het decreet lokaal bestuur bekendgemaakt op de website van de gemeente Oudsbergen.

De raad voor maatschappelijk welzijn bezorgt een afschrift van dit besluit aan:

- dienst ICT
- de Welzijnsregio Noord-Limburg

06. Kennisname van het besluit van het vast bureau van 31 januari 2022 betreffende het vaststellen van het mandaat van de vertegenwoordiger van het OCMW op de algemene vergadering van Welzijnsregio Noord-Limburg van 15 februari 2022

contactpersoon	**functie**	**e-mail**	**dossier**
Marina Caymax	administratief medewerkster	marina.caymax@oudsbergen.be	

Voorgeschiedenis en verwijzingsdocumenten

Op 14 januari 2022 ontving het OCMW van Oudsbergen per e-mail de uitnodiging voor de algemene vergadering van Welzijnsregio Noord-Limburg die plaatsvindt op 15 februari 2022.

Op de agenda van deze vergadering staan de volgende punten:
- Goedkeuring verslag van de Algemene Vergadering van 14 december 2021
- Aanstellingen van het college van commissarissen

Het vast bureau heeft in de vergadering van 31 januari 2022 het mandaat van de vertegenwoordiger van het OCMW voor de algemene vergadering van Welzijnsregio Noord-Limburg van 15 februari 2022 vastgesteld.

Op 29 januari 2019 duidde de raad voor maatschappelijk welzijn de heer Kurt Plessers aan als stemgerechtigde vertegenwoordiger op de algemene vergaderingen van Welzijnsregio Noord-Limburg.

Argumentatie

Het OCMW van Oudsbergen maakt deel uit van Welzijnsregio Noord-Limburg en wordt in de organen van de welzijnsvereniging vertegenwoordigd door leden van de raad voor maatschappelijk welzijn.

De vaststelling van het mandaat van de vertegenwoordiger van het OCMW voor de algemene vergadering van Welzijnsregio Noord-Limburg van 15 februari 2022 kon niet meer tijdig geagendeerd worden voor de vergadering van de raad voor maatschappelijk welzijn van 24 januari 2022.
Daarom stelde het vast bureau in de vergadering van 31 januari 2022 het mandaat van de vertegenwoordiger vast en wordt dit besluit nu ter kennisgeving voorgelegd aan de raad voor maatschappelijk welzijn.

Juridische context

Bevoegdheid:

Artikels 77 en 78 van het decreet lokaal bestuur van 22 december 2017 bepalen dat de raad voor maatschappelijk welzijn bevoegd is voor deze materie.

Grond:

Artikels 475 tot en met 495 van het decreet lokaal bestuur van 22 december 2017 gaan over de welzijnsverenigingen. Artikel 484 gaat specifiek over de vertegenwoordiging vanwege het OCMW in deze vereniging.

De statuten van Welzijnsregio Noord-Limburg.

Adviezen en inspraak

Er werd geen voorafgaand advies ingewonnen, noch vond er inspraak plaats.

Plaats in het meerjarenplan en financiële gevolgen

De uitvoering van het besluit heeft geen link met het meerjarenplan en heeft ook geen financiële consequenties.

Neemt kennis van

Artikel 1

Het besluit van het vast bureau van 31 januari 2022 in verband met het vaststellen van het mandaat van de vertegenwoordiger van het OCMW voor de algemene vergadering van Welzijnsregio Noord-Limburg van 15 februari 2022.

Artikel 2

Tegen dit besluit kan een klacht worden ingediend bij de toezichthoudende overheid. Deze klacht moet ingediend worden binnen een periode van 30 dagen die volgt op de dag van de bekendmaking van dit besluit op de website van de gemeente Oudsbergen.

De klacht kan via een aangetekend schrijven gericht worden aan:

Agentschap Binnenlands Bestuur
VAC Herman Teirlinck Brussel
Havenlaan 88, bus 70
1000 Brussel

De klacht kan ook via een aangetekende e-mail verstuurd worden naar: binnenland@vlaanderen.be

Artikel 3

Dit besluit wordt overeenkomstig de bepalingen uit artikels 285 tot en met 287 van het decreet lokaal bestuur bekendgemaakt op de website van de gemeente Oudsbergen.

De raad voor maatschappelijk welzijn bezorgt een afschrift van dit besluit aan:

- Welzijnsregio Noord-Limburg
- De heer Kurt Plessers

Namens de raad voor maatschappelijk welzijn

Guy Bodeux
algemeen directeur

Marco Goossens
voorzitter