

**Veiligheidsbeleid**

**Inleiding**

De goede werking van het OCMW hangt grotendeels af van de informatie die wordt behandeld, aangemaakt en meegedeeld. Deze informatie is zeer uitgebreid en kan al dan niet op meerdere dragers staan: papier en digitaal.

Op deze dragers is informatie terug te vinden over het personeel van het OCMW en over alle gerechtigden van de wettelijke rechten. Deze informatie is vertrouwelijk en dat moet zo blijven.

Net zoals elke andere federale en regionale instelling met het OCMW's een aantal risico's en bedreigingen het hoofd bieden die de vertrouwelijkheid, de integriteit en de beschikbaarheid van de informatie schade zouden kunnen toebrengen. Deze voortdurend evolueerde bedreigingen omvatten, onder andere, diefstand van identiteit en van vertrouwelijke informatie, fraude met, diefstal van intellectuele eigendom, het gebruik, de verspreiding en de vernietiging van informatie, technische storingen, natuurlijke voorvallen en menselijke fouten.

Het OCMW wordt trouwens onderworpen aan verschillende wettelijke, federale en regionale verplichtingen die voortvloeien uit haar taken en die verband houden met de informatieveiligheid. De naleving van deze verplichtingen en de vertrouwensband die er bestaat tegenover de personeelsleden en de begunstigden zijn essentieel voor het behoud van haar reputatie en van haar goede werking.

Enkel onder deze voorwaarde zal het OCMW haar taken correct en binnen de naleving van de normen en wetten kunnen uitvoeren.

Op het vlak van de sociale zekerheid wordt de informatieveiligheid gedefinieerd als de strategie, regels, procedures en middelen voor het beschermen van alle soorten informatie zowel in de transmissiesystemen als in de verwerkingssystemen om de vertrouwelijkheid, de beschikbaarheid, de integriteit, de betrouwbaarheid, de authenticiteit en de onweerlegbaarheid ervan te garanderen. Cf. Koninklijk besluit van 17 maart 2013 betreffende de veiligheidsadviseurs ingevoerd door de wet van 15 augustus 2012 houdende oprichting en organisatie van een federale dienstenintegrator.

**Doelstellingen**

Dit beleid vormt één van de sleutelelementen die het mogelijk maakt om de missie en de doelstellingen van het OCMW uit te voeren om haar reputatie te behouden en zich te schikken naar de wettelijke, reglementaire en contractuele verplichtingen die van toepassing zijn.

Het belangrijkste doel van dit beleid is de vastberadenheid en het engagement meedelen van de Raad voor Maatschappelijk Welzijn / van het vast Bureau om het risicobeheer in verband met de informatieveiligheid te beheren en te ondersteunen. De aangeraden benadering heeft de identificatie van de betrokkenen en de definitie van hun rollen tot doel, de sensibilisering van de gebruikers voor de risico's en het ontwerp en de toepassing van maatregelen die de veiligheid van de informatiemiddelen doeltreffend verzekeren.

De volgende doelstellingen worden eveneens beoogd:

1. het respect van het privéleven en van de wettelijke verplichtingen in verband met de behandeling van persoonlijke en sociale gegevens,

2. de overeenstemming met de minimale normen vastgelegd door het sectoraal comité van de sociale zekerheid en van de gezondheid in het kader van de behandeling van voornoemde gegevens,

3. de inventaris van de middelen en het veilig stellen ervan in overeenstemming met de classificatie van de gegevens,

4. de invoering van een proces inzake risicobeheer volgens een gedocumenteerde methode voor alle kritieke processen,

5. de beschikbaarheid, de integriteit en de vertrouwelijkheid van de informatie,

6. een voortdurende verbetering van de informatieveiligheid,

7. de integratie van de vereiste veiligheidsnoden in een overeenkomst wanneer men een beroep doet op onderaannemers of leveranciers.

**Draagwijdte**

De informatieveiligheid belangt iedereen aan. Dit beleid is van toepassing op alle gebruikers van de informatiebronnen van het OCMW waartoe, onder andere, de Voorzit(st)er, de leden van de Raad voor maatschappelijk welzijn, de directeur-generaal, de veiligheidsconsulent en de personeelsleden behoren.

De onderaannemers, leveranciers en partners van het OCMW zijn aan het OCMW gebonden door een vertrouwelijkheidsclausule.

Dit beleid is van toepassing op alle informatie waarover het OCMW beschikt en waartoe het OCMW toegang heeft, ongeacht of deze informatie bewaard wordt op eender welke drager.

**Verantwoordelijkheden**

Elke persoon of dienst is verantwoordelijk voor het beheer van de risico's bij de informatieveiligheid in zijn hoedanigheid van eigenaar van de informatie. Deze verantwoordelijkheid is van toepassing op de informatiemiddelen, op de processen en op de systemen die onder hun verantwoordelijkheid en controle vallen, ook diegenen die gedelegeerd zijn aan een derde.

**Naleving**

Het risicobeheer van de informatieveiligheid gebeurt in overeenstemming met de wettelijke,

reglementaire en contractuele verplichtingen die van toepassing zijn, evenals met het federale en regionale beleid en

**Sensibilisering**

Er worden aangepaste maatregelen ingevoerd om alle gebruikers en betrokkenen te sensibiliseren en actief te laten deelnemen aan de bescherming van de informatiemiddelen van het OCMW en een verantwoord gebruik van de middelen te bevorderen.

Rollen en verantwoordelijkheden

Dit beleid en de toepassing ervan valt onder de bevoegdheid van verschillende betrokkenen die de volgende mandaten kregen toegewezen:

**Raad voor maatschappelijk welzijn**

- keurt het beleid en de bijwerkingen ervan goed;

- superviseert het proces van het risicobeheer bij de informatieveiligheid, via de veiligheidsconsulent en de verantwoordelijke voor het dagelijks beheer.

**Vast bureau**

- beveelt de Raad voor Maatschappelijk Welzijn de goedkeuring van het beleid aan, evenals de bijwerkingen ervan;

- superviseert het proces van het risicobeheer bij de informatieveiligheid en de toepassing van het beleid;

- legt, indien nodig, verantwoording af aan ...

**Directie**

- stelt het veiligheidsbeleid en de bijwerkingen ervan voor en beveelt de goedkeuring ervan aan het Vast Bureau aan via …

- waarborgt de toepassing van het beleid door de informatieveiligheidsconsulent;

- zorgt ervoor dat de informatieveiligheidsconsulent over de gepaste financiële en logistieke middelen beschikt.

**Informatieveiligheidsconsulent**

Overeenkomstig het KB van 12/08/93 heeft de informatieveiligheidsconsulent de volgende verantwoordelijkheden:

* de informatieveiligheidsconsulent heeft een adviserende, stimulerende, documenterende en controlerende opdracht;
* De informatieveiligheidsconsulent adviseert de verantwoordelijke voor het dagelijks bestuur van zijn instelling, op diens verzoek of op eigen initiatief, omtrent alle aspecten van de informatieveiligheid. De adviezen worden schriftelijk en gemotiveerd uitgebracht, tenzij de risico’s niet voldoende ernstig zijn. Binnen de tijdspanne vereist door de omstandigheden, maar met een maximum van drie maanden, beslist de verantwoordelijke voor het dagelijks bestuur het advies al dan niet op te volgen en deelt hij de veiligheidsdienst de genomen beslissing mee. In geval de beslissing van een schriftelijk advies afwijkt, dient de mededeling ervan op een schriftelijk advies afwijkt, dient de mededeling ervan op een schriftelijke en gemotiveerde wijze te geschieden.
* De informatieveiligheidsconsulent bevordert de naleving van de veiligheidsvoorschriften opgelegd door of krachtens een wets- of reglementsbepaling, evenals het aannemen, door de personen tewerkgesteld in een OCMW, van een veiligheidsgedrag bij de personen tewerkgesteld in de instelling.
* De informatieveiligheidsconsulent legt de nodige documentatie aan met betrekking tot de informatieveiligheid;
* De informatieveiligheidsconsulent ziet toe op de naleving, binnen het OCMW, van de veiligheidsvoorschriften opgelegd door of krachtens een wets- of reglementsbepaling. Alle vastgestelde inbreuken worden schriftelijk en uitsluitend aan de verantwoordelijke voor het dagelijks bestuur van de instelling meegedeeld, vergezeld van de nodige adviezen om dergelijke inbreuken in de toekomst te vermijden.
* De informatieveiligheidsconsulent werkt onder het rechtstreeks functioneel gezag van de verantwoordelijke voor het dagelijks bestuur van het OCMW. Hij werkt nauw samen met de diensten waarin zijn tussenkomst vereist is of kan zijn, in het bijzonder met de informaticadienst en de dienst voor veiligheid, gezondheid en verfraaiing van de werkplaatsen van de instelling;
* De informatieveiligheidsdienst dient een gedegen kennis te bezitten van de informatica-omgeving van het OCMW en van de informatieveiligheid. Hij dient deze kennis permanent op peil te houden.
* De informatieveiligheidsconsulent stelt ten behoeve van de verantwoordelijke voor het dagelijks bestuur een ontwerp van veiligheidsplan op voor een termijn van drie jaar, met aanduiding van de middelen op jaarbasis die vereist zijn om het plan uit te voeren. Dit ontwerp wordt minstens eenmaal per jaar herzien en zo nodig aangepast. Het ontwerp van veiligheidsplan wordt beschouwd als een advies,
* De informatieveiligheidsconsulent stelt ten behoeve van de verantwoordelijke voor het dagelijks bestuur van de instelling een jaarverslag op.

Dit jaarverslag omvat minstens:

1° een algemeen overzicht van de veiligheidstoestand, de evolutie in het afgelopen jaar en de nog te realiseren doelstellingen;

2° een samenvatting van de schriftelijke adviezen die overgemaakt werden aan de verantwoordelijke voor het dagelijks bestuur en het gevolg dat eraan werd verleend;

3° een overzicht van de werkzaamheden verricht door de informatieveiligheidsdienst;

4° een overzicht van de resultaten van de controles uitgevoerd door de informatieveiligheidsdienst met weergave van alle vastgestelde voorvallen die van aard waren de informatieveiligheid van de instelling of het netwerk in het gedrang te brengen;

5° een overzicht van de gevoerde campagnes ter bevordering van de veiligheid;

6° een overzicht van alle gevolgde en de voorziene nog te volgen opleidingen;

7° de opdrachten van de informatieveiligheidsconsulent bepaald in dit KB hebben ook betrekking op de bewaring, de verwerking of de uitwisseling van sociale gegevens van persoonlijke aard die voor rekening van de betrokken instelling geschieden door derden.

**De gebruiker**

Hij neemt kennis van het beleid, van de reglementen, gedragscodes en andere richtlijnen van het OCMW die betrekking hebben op de informatieveiligheid die op hem betrekking hebben en stemt ermee in.

Hij wint inlichtingen in en neem actief deel aan de uitvoering van het beleid en hij gebruikt de informatiemiddelen door zich te beperken tot de doelstellingen waartoe zij bestemd zijn en tot de toegangen die hem worden toegekend.

Definities

Voor de toepassing van dit beleid.

**Informatiemiddel**

De informatie zelf, ongeacht op welke drager, en de systemen die gebruikt worden voor de behandeling, het gebruik, de opslag, de bewaring en de communicatie ervan. Verlies, diefstal of vernietiging van een dergelijk middel zou kunnen leiden tot schade bij het OCMW. Voorbeelden van informatiemiddelen zijn het fysiek en/of informaticadossier van de begunstigde, de archieven en de dossiers van de personeelsleden.

**Levenscyclus**

De levenscycli worden bepaald door de archivarissen van het rijk, maar de logs van de gebruikers worden minstens 10 jaar bewaard.

**Risico's in verband met de informatieveiligheid**

Wordt als een risico beschouwd: elke gebeurtenis, met een graad van onzekerheid, die schade zou kunnen toebrengen aan de vertrouwelijkheid, de integriteit of de beschikbaarheid van de informatie en die het OCMW schade berokkent.

**Veiligheidsprincipes, veiligheidsnormen en -vereisten**

De veiligheidsprincipes die worden gevolgd zijn de volgende:

* vertrouwelijkheid,
* integriteit,
* beschikbaarheid,
* externe toetsing.

De zeer belangrijke normen en vereisten voor de naleving van de informatieveiligheid zijn trouwens:

* het KB van 12/08/93 en de aanpassingen ervan,
* de minimale veiligheidsnormen van de KSZ,
* de richtlijnen van de Commissie voor de bescherming van het privéleven,
* de wet betreffende het respect voor het privéleven.

4. Wettelijk en reglementair kader

De gebruikte referenties zijn:

- de minimale normen 2015 van de KSZ,

- de ISO-normen ISO 27001, ISO 27002:2013 en ISO 2700.

- "Harmonisering van de functies van de informatieveiligheid" voorstel van het comité BELNIS;

- het KB van 12/08/93 (<https://www.ksz-bcss.fgov.be/fr/bcss/anchorpage/content/websites/belgium/legislation/legislation_03/legislation_03_01.html>);

- het informatieveiligheidsbeleid van de KSZ (<https://www.ksz-bcss.fgov.be/fr/bcss/page/content/websites/belgium/security/security_04/security_04_02.html>);

- de aanbevelingen van de Commissie voor de bescherming van het privéleven: <https://www.privacycommission.be/nl>

V1/01/2016 D