Veiligheidsessie II 2014

BASISOPLEIDING 2014 v1

POD Maatschappelijke Integratie
SPP Intégration Sociale

INDEX

NIEWE NORMEN

15.1 Samenwerking met de onderaannemers.

Elk OCMW moet:

zich ervan vergewissen dat de verplichtingen[15] inzake de verwerking van persoonsgegevens contractueel zijn vastgelegd. In het kader van een oplossing van het type “Cloud Computing“ beperkt de keuze zich volgens de desbetreffende policy(ISMS.0050) enkel tot de diensten van het type “gemeenschappelijke[16]" (of privé-cloud").

[15] De organisatie blijft aansprakelijk voor de veiligheid van de verwerking, met inbegrip van de verwerking bij de onderaannemer.

NIEWE NORMEN

7.2 Elk OCMW moet elke medewerker bewust maken voor de informatieveiligheid

Er kunnen verschillende middelen (affichecampagne, specifieke opleiding, ...) gebruikt worden in functie van het "profiel" van iedereen.

NIEWE NORMEN

11.4 Veilig verwijderen of hergebruiken van apparatuur.

Elk OCMW moet:

de nodige maatregelen treffen opdat alle gegevens op opslagmedia gewist of ontoegankelijk gemaakt worden vóór verwijdering of hergebruik.

NIEWE NORMEN

12.1 Scheiding van omgevingen.

Elk OCMW moet:

- **de gepaste maatregelen treffen opdat de productieomgeving gescheiden en verschillend is van de andere omgevingen zoals ontwikkeling, acceptatie, test, ...**

NIEWE NORMEN

12.1 Scheiding van omgevingen.

Elk OCMW moet:

- **zich ervan verzekeren dat er geen testen of ontwikkelingen plaatsvinden in de productieomgeving. In bepaalde uitzonderlijke gevallen kan voor testdoeleinden afgeweken worden van deze regel op voorwaarde dat gepaste maatregelen getroffen worden.**

NIEWE NORMEN

8.4. Fysieke beveiliging in transit

Elk OCMW moet de nodige maatregelen treffen om fysieke media, waaronder in het bijzonder back-ups die gevoelige gegevens bevatten, tijdens het transport te beschermen tegen niet geautoriseerde toegang.

NIEWE NORMEN

9.4 Gebruik van de netwerkdiensten

Elk OCMW moet de aangepaste maatregelen nemen, zodat elke persoon enkel toegang heeft tot de diensten waarvoor hij specifiek een toelating heeft ontvangen.

NIEWE NORMEN

14.4. Toepassingsveiligheid

Elk OCMW moet:

- **de nodige maatregelen treffen om de veiligheid te garanderen op applicatieniveau teneinde eventuele veiligheidsinbreuken te vermijden (vertrouwelijkheid, integriteit, beschikbaarheid)[14]**

[14]: in verband met de bestaande bedreigingen, zoals SQL injection, Spoofing, Cross Site Scripting, Elevation Privilege (Top Ten OWASP: *Open Web Application Security Project*)

NIEWE NORMEN

VRAGEN ?

HERZIENE NORMEN

7.1 Elk OCMW moet een procedure invoeren die waarborgt dat alle interne en externe medewerkers zich ertoe verbinden hun verplichtingen na te leven in verband met de vertrouwelijkheid en de veiligheid van de gegevens.

13.2.1 Cartografie van de extranetfluxen

Elk OCMW moet:

een technische cartografie[13] bijhouden van de geïmplementeerde technische stromen via het Extranet van de sociale zekerheid. De veiligheidsconsulent moet hierover geïnformeerd worden.

13 Nodig voor het correct beheer van de firewalls in de verschillende zones van het Extranet. Voor de OCMW's die werken met een softwarehuis wordt deze cartografie up to date gehouden door het softwarehuis.

12.4 Backup-policy

Om onherstelbaar verlies van gegevens te voorkomen, moet elke organisatie:

- **de policy en strategie definiëren om een backupsysteem te implementeren, in overeenstemming met het continuïteitsbeheer (norm 17.).**
- **in dit verband regelmatig de genomen backups verifiëren.**

12.6 Traceerbaarheid van de identiteiten.

- Elk OCMW dat deelneemt aan het verzenden van gegevens via de Kruispuntbank moet op haar niveau de traceerbaarheid van de identiteiten waarborgen.

- Deze traceerbaarheid moet identificatie toelaten van begin tot einde.

HERZIENE NORMEN

17.1. Continuïteitsbeheer.

Elk OCMW moet:

een continuïteitsplan uitwerken, testen en onderhouden op basis van een risicoanalyse om de opdracht van de organisatie in het kader van de sociale zekerheid te kunnen waarborgen.

HERZIENE NORMEN

18.1 Externe audit[19].

Elk OCMW moet:

periodiek een conformiteitsaudit uitvoeren met betrekking tot de veiligheidssituatie zoals beschreven in de minimale normen[20].

Herhaling: financiele inspaningen en termijn van 5 jaar.

HERZIENE NORMEN

VRAGEN ?

TOEPASSINGSGEBIED

Daarnaast zou het een goed gebruik zijn deze normen ook toe te passen op informatieveiligheid in de ruime betekenis zoals gedefinieerd in het KB van 17/03/13 betreffende de veiligheidsadviseurs ingevoerd door de wet van 15/08/12 houdende oprichting en organisatie van een federale dienstenintegrator,

CHAMPS D'APPLICATION

en zoals overgenomen in het KB van 12/08/93 houdende de organisatie van de informatieveiligheid bij de instellingen van sociale zekerheid:

"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".

HERZIENE NORMEN

VRAGEN ?

16.1 Belangrijke incidenten (1).

Elk OCMW moet:

- ervoor zorgen dat de dienst Informatieveiligheid door de verantwoordelijke dienst op de hoogte gesteld wordt van belangrijke incidenten die de informatieveiligheid in het gedrang kunnen brengen alsook van de maatregelen die genomen worden om aan deze incidenten het hoofd te bieden.

HERZIENE NORMEN

16.1 Belangrijke incidenten[17].

Elk OCMW moet:

- erop toezien dat de KSZ op de hoogte wordt gebracht van ieder veiligheidsincident dat als "major" wordt beschouwd volgens de algemene policy die binnen de sociale zekerheid werd vastgelegd met betrekking tot de mededeling van veiligheidsincidenten[18].

HERZIENE NORMEN

17 Belangrijke incidenten: het is aangewezen dat iedere organisatie het "ernstig" karakter van een incident definieert. Bijvoorbeeld, brand, waterschade, malware-aanvallen, inbraakpogingen (fysiek of logisch), diefstal of verlies van draagbare computers, loggingonderbreking kunnen beschouwd worden als ernstige incidenten.

18 Deze norm wordt pas van kracht op het ogenblik dat de veiligheidspolicy met betrekking tot de mededeling van veiligheidsincidenten binnen de sociale zekerheid goedgekeurd en beschikbaar is.

HERZIENE NORMEN

VRAGEN ?

Informatieveiligheid bij de integratie-oefening OCMW - gemeente

De veiligheidsbeheerder voert de volgende taken uit:

- de aanvragen i.v.m. de gebruikers invoeren;
- de gebruiker op het federale portaal desgevallend creëren;
- de instellingen (agentschappen) in het gebruikersbeheersysteem te definiëren in samenwerking met P&O en de KBO (om het KBO-nummer te creëren);

Informatieveiligheid bij de integratie-oefening OCMW - gemeente

De veiligheidsbeheerder voert de volgende taken uit:

- de instellingen (agentschappen) in het gebruikersbeheersysteem te definiëren in samenwerking met P&O en de KBO (om het KBO-nummer te creëren);
- de veiligheidsbeheerders en veiligheidscontactpersonen in het gebruikersbeheersysteem definiëren.

Informatieveiligheid bij de integratie-oefening OCMW - gemeente

De Commissie voor de Bescherming van de Persoonlijke Levenssfeer beveelt in haar document "Referentiemaatregelen voor de beveiliging van elke verwerking van persoonsgegevens" de aanstelling aan van een veiligheidsconsulent binnen iedere instelling.

Informatieveiligheid bij de integratie-oefening OCMW - gemeente

De wet van de 8/08/93 tot regeling van een Rijksregister van de natuurlijke personen voorziet de aanstelling van een consulent inzake informatieveiligheid en bescherming van de persoonlijke levenssfeer in iedere openbare overheid, openbare of private instelling die de toegang tot of de mededeling van informatiegegevens van het RR verkregen heeft. De identiteit van deze consulent moet naar het Sectoraal Comité van het Rijksregister gecommuniceerd worden. In sommige gevallen is de benaming "veiligheidconsulent voor het RR" ook in gebruik.

Informatieveiligheid bij de integratie-oefening OCMW - gemeente

De Lokale Beheerder wordt aangesteld door de Verantwoordelijke Toegangen Entiteit (of Co- Verantwoordelijke Toegangen Entiteit) om een hoedanigheid van een onderneming/organisatie te beheren (i.e. activiteitsdomein).

Informatieveiligheid bij de integratie-oefening OCMW - gemeente

De lokale beheerder voert de volgende taken uit:

- één of meer Lokale Co-Beheerders aanstellen om hem bij te staan;
- de Lokale Co-Beheerders binnen zijn hoedanigheid blokkeren, deblokkeren of verwijderen (deze functionaliteit is niet toegankelijk voor Co-Verantwoordelijken);
- de subafdelingen beheren voor zover deze hoedanigheid hem dit toelaat:
- een subafdeling toevoegen/verwijderen, vrij of onder voorwaarden in functie van de mogelijkheden die hem aangeboden worden en er bepaalde toepassingen aan koppelen;
- o een subafdeling blokkeren/deblokkeren;
- de (Co-)Subafdelingsbeheerder beheren.

Informatieveiligheid bij de integratie-oefening OCMW - gemeente

- Gebruikers beheren binnen de hoedanigheid die hij beheert:
- een nieuwe gebruiker registreren; autorisaties toewijzen aan de gebruikers die hij beheert;
- bepaalde attributen van gebruikers wijzigen (taalkeuze, e-mail en toegang tot toepassingen);
- gebruikers blokkeren, deblokkeren en verwijderen.
- gebruikers opzoeken en selecteren binnen het activiteitsdomein dat hij beheert;
- een technische gebruiker aanstellen die de contactpersoon zal zijn voor alles wat te maken heeft met de uitwisseling van gegevens via batch (gestructureerd berichten);
- bepaalde informatie wijzigen die specifiek is voor de hoedanigheid. (en een e-mail- adres definiëren voor deze hoedanigheid).
- .

Informatieveiligheid bij de integratie-oefening OCMW - gemeente

De minimale veiligheidsnormen gelden aldus voor de instellingen van sociale zekerheid.

Vermits de gemeenten verbonden zijn met het Rijksregister, gelden de veiligheidsvereisten van de privacy wet.

Informatieveiligheid bij de integratie-oefening OCMW - gemeente

De referentiemaatregelen van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer zijn hier van toepassing.

Ook gemeentebesturen moeten een veiligheidsconsulent aanstellen en beschikken over een veiligheidsbeleid. De mededeling van persoonsgegevens door gemeentes vergt tevens de voorafgaande machtiging van de bevoegde afdeling van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer.

Informatieveiligheid bij de integratie-oefening OCMW - gemeente

Elke vorm van samenwerking op gemeentelijk vlak tussen het gemeentebestuur en het OCMW dient ten volle ondersteund te worden. Dit kan leiden tot een betere en geïntegreerde dienstverlening aan de burger en tot een grotere efficiëntie en effectiviteit voor de betrokken partijen.De voorwaarde hiervoor is dat deze samenwerking geen afbreuk doet aan de principes vervat in de wet van 8/12/92 *tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens* of de andere relevante bepalingen omtrent de bescherming van (persoons)gegevens.

Informatieveiligheid bij de integratie-oefening OCMW - gemeente

Zij dragen elk hun eigen verantwoordelijkheid, en moeten elk hun eigen informatieveiligheidsbeleid ontwikkelen met de bijhorende controles.

Informatieveiligheid bij de integratie-oefening OCMW - gemeente

Het feit dat beide organisaties samenwerken, bijvoorbeeld door een beroep te doen op dezelfde personeelsleden en dezelfde infrastructuur, is toegestaan voor zover elke organisatie haar verplichtingen eigen aan haar activiteiten respecteert.

Informatieveiligheid bij de integratie-oefening OCMW - gemeente

Bij het gebruik van een gemeenschappelijke informatica-infrastructuur dient erover gewaakt te worden dat de nodige technische en organisatorische maatregelen voorzien worden opdat enkel gemachtigde personen toegang zouden hebben tot de persoonsgegevens nodig voor de uitoefening van hun opdrachten.

Informatieveiligheid bij de integratie-oefening OCMW - gemeente

Bij toegang tot gegevens moet er een formele identificatie plaats vinden. Er moet onderscheid kunnen gemaakt worden tussen toegang in naam van de gemeente en toegang in naam van het OCMW.

Voor elke gebruiker betekent dit dat onderscheiden toegangsrechten tot persoonsgegevens moeten gegeven worden in functie van de rol bij de organisatie waarvoor hij werkt.

Informatieveiligheid bij de integratie-oefening OCMW - gemeente

Een machtiging van het Sectoraal Comité is verplicht voor de uitwisseling van persoonsgegevens tussen de gemeente en het OCMW.

Informatieveiligheid bij de integratie-oefening OCMW - gemeente

Gebruik van een gemeenschappelijk softwarepakket is toegelaten.

Bij de toegang tot de software en tot de gegevens opgeslagen door dat softwarepakket moet echter kunnen worden onderscheiden of die toegang geschiedt in naam van de gemeente of van het OCMW.

Er dient gezorgd te worden voor een logische scheiding van de gegevens(opslag).

Informatieveiligheid bij de integratie-oefening OCMW - gemeente

Betrokkene gemeenschappelijke diensten:

-personeeldienst;

-boekhouding;

-ontvangerij;

-logistiek;

-informatica dienst (hoogste niveau van veiligheid: opspoorbaarheid geeist).

Informatieveiligheid bij de integratie-oefening OCMW - gemeente

Gezamenlijkadressenbestand

De algemene regel stelt dat er voor elke uitwisseling van sociale persoonsgegevens een machtiging vereist is van het Sectoraal Comité van de Sociale Zekerheid en van de Gezondheid en dat die gegevensuitwisseling via de Kruispuntbank van de Sociale Zekerheid moet plaatsvinden.

Informatieveiligheid bij de integratie-oefening OCMW - gemeente

Dit houdt in dat het gezamenlijk adressenbestand geen enkel sociaal persoonsgegeven mag bevatten zonder machtiging van het Sectoraal Comité.

Bovendien, is de verwerking van dergelijke bestanden onderworpen aan de "Wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens".

Informatieveiligheid bij de integratie-oefening OCMW - gemeente

"Uniekedeur"

De term "unieke deur" definieert het concept waarbij loketten van verschillende gemeentelijke diensten op één plaats voor de burgers toegankelijk zijn, zoals (niet beperkende lijst) :

- dienst bevolking;
- dienst burgerlijke stand;
- OCMW;
- plaatselijk werkgelegenheidsagentschap (PWA);
- sociaal wonen;
- dienst lokale politie; -...

..

Informatieveiligheid bij de integratie-oefening OCMW - gemeente

Dit initiatief wordt natuurlijk enkel goedgekeurd op voorwaarde dat de maatregelen[1] vastgelegd in dit document worden nageleefd door alle organisaties die over een loket zullen beschikken.

1 Cf: https://www.bcss.fgov.be/binaries/documentation/nl/securite/policies/isms_043_ocmw_cpas_gemeente_commune_nl.pdf

Informatieveiligheid bij de integratie-oefening OCMW - gemeente

Samenbrengen van informatie- en communicatie-technologie

- Een samenwerking is toegestaan. Deze samenwerking moet de naleving van alle normen en regels garanderen waaraan elke organisatie gehouden is.
- Er moet een samenwerkingsakkoord gesloten worden tussen de verschillende partnerorganisaties.
- In dat akkoord moeten de bevoegdheden van elke organisatie vermeld worden, alsook de verantwoordelijkheden .

Informatieveiligheid bij de integratie-oefening OCMW - gemeente

Ingeval een deel van dit beheer toevertrouwd wordt aan een derde (een onderaannemer), is het noodzakelijk dat deze derde een contract afgesloten heeft met de organisatie.

In dit contract moeten alle verplichtingen van de onderaannemer vermeld worden inzake vertrouwelijkheid, maar ook diens verplichtingen inzake de bescherming van persoonsgegevens, zoals bepaald in de wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens

Informatieveiligheid bij de integratie-oefening OCMW - gemeente

Back ups

Indien de back ups het OCMW verlaten moeten ze vercijferd worden.

Indien de back ups de gegevens van de 2 organisaties bevatten moeten de encryptiemaatregelen doorgevoerd worden zodat elke organisatie enkel gemachtigd is om haar eigen gegevens te lezen.

Informatieveiligheid bij de integratie-oefening OCMW - gemeente

De toegang tot deze back-updragers moet verleend worden aan de bevoegde personen, volgens de noodzaak. Elke toegang moet getraceerd kunnen worden door elke organisatie.

Informatieveiligheid bij de integratie-oefening OCMW - gemeente

Internettoegangen gebruik van emails

Medewerkers in dienst van meerdere organisaties moeten beschikken over een e-mailadres binnen elke organisatie.

Administratorrechten voor gewone gebruikers

Om een optimale beveiliging van het netwerk te garanderen, kan een gewone gebruiker niet beschikken over administratorrechten op zijn werkstation.

Informatieveiligheid bij de integratie-oefening OCMW - gemeente

Deze maatregel geldt zowel voor vaste werkstations ("desktops") als voor mobiele werkstations ("laptops"). In geval van nieuwe technologieën (smartphones, tablet, ...) dient een risicoanalyse uitgevoerd te worden teneinde de gepaste veiligheidsmaatregelen te kunnen toepassen.

Informatieveiligheid bij de integratie-oefening OCMW - gemeente

Elke toegang tot een informatiesysteem dat persoonsgegevens bevat, moet getraceerd kunnen worden zodat er op de vragen "Wie, wanneer, wat en hoe?" geantwoord kan worden.

Informatieveiligheid bij de integratie-oefening OCMW - gemeente

Het moet dus mogelijk zijn aan een gebruiker enkel de rechten te verlenen die nodig zijn voor de uitvoering van zijn opdracht.

Veiligheidslogs

De integriteit en vertrouwelijkheid van deze loggings moeten gegarandeerd worden, en ze moeten geraadpleegd kunnen worden door de bevoegde autoriteiten.

Scheiding van de organisaties

Zelfs indien verschillende organisaties samenwerken, is het noodzakelijk een fysieke of logische scheiding te bewerkstelligen tussen die organisaties.

Scheidingvandeorganisaties

- Op het netwerkniveau moet een logische scheiding bewerkstelligd worden, indien een fysieke scheiding niet mogelijk is, zodat elke gebruiker enkel toegang heeft tot zijn eigen ressources/middelen.
- Op het niveau van het besturingssysteem moeten de organisaties logisch gescheiden worden.

Informatieveiligheid bij de integratie-oefening OCMW - gemeente

Verbinding tussen verschillende plaatsen

Indien de organisatie(s) verspreid is(zijn) over meerdere sites, dienen de nodige maatregelen getroffen te worden opdat de verbinding tussen deze gepast beveiligd zou zijn.

Informatieveiligheid bij de integratie-oefening OCMW - gemeente

Verbinding tussen verschillende plaatsen

Indien de organisatie(s) verspreid is(zijn) over meerdere sites, dienen de nodige maatregelen getroffen te worden.

Hiervoor bestaan er meerdere mogelijkheden:

- een oplossing bestaat erin een (virtueel) directe lijn te hebben tussen de verschillende plaatsen.
- in sommige omstandigheden kan een draadloze verbinding geïnstalleerd worden. Toch dient er opgemerkt te worden dat deze draadloze voorzieningen enkel onderling kunnen communiceren.

Informatieveiligheid bij de integratie-oefening OCMW - gemeente

Een andere oplossing bestaat erin een VPN-verbinding te installeren tussen de sites via internet.

De standaardoplossing die aanbevolen wordt door de Kruispuntbank is de VPN "IPSEC"-verbinding LAN- to-LAN.

Informatieveiligheid bij de integratie-oefening OCMW - gemeente

VRAGEN ?

SESSIE 2014 II

EIND