POD Maatschappelijke Integratie
SPP Intégration Sociale

E-mail: helpdesk.security @mi-is.be
Url : www.mi-is.be

Inleiding

Deze auditlijst is gebaseerd op de kennis en ervaring van de leden van de helpdesk veiligheid van de POD MI. Deze lijst is bijgevolg niet per se volledig, maar kan beschouwd worden als een hulpmiddel voor de veiligheidsconsulenten. In de minimale normen is er voorzien dat er elke 4 jaar een audit dient te gebeuren.

Doel:voor wie en hoe?

De minimale normen preciseren dat er een audit dient te gebeuren, maar vermelden niet door wie deze audit moet uitgevoerd worden. Dus, de veiligheidconsulenten die wat ervaring hebben kunnen de bijgevoegde vragenlijst gebruiken om:

- hun eigen audit te doen om een zicht te krijgen op de veiligheidssituatie van het OCMW en dus zijn positie tov de minimale normen te kennen;
- een audit te laten uitvoeren door een veiligheidsconsulent van een ander OCMW En indien gevraagd als tegenprestatie de audit bij dit ander OCMW te gaan doen
- zich te laten inspireren om nuttige vragen te stellen over de beveiliging van het OCMW

Inhoud van de vragenlijst

De vragenlijst behandelt alle domeinen van de minimale veiligheidsnormen voor het OCMW. De vragen met een **grijze font** zijn direct gelinkt aan de minimale normen. De andere vragen zijn eerder “best practice”: ze zijn niet wettelijk verplicht, maar helpen wel om de omgeving beter te beveiligen. Indien de grijze vragen geen antwoord krijgen, kan dit aangeven dat er aan deze norm niet bevredigend werd beantwoord (of dat een beslissing die genomen werd door de veiligheidsconsulent en de OCMW-raad deze norm als een verwaarloosbaar risico heeft geklasseerd).

Het geheel der vragen geeft aan of de beveiliging goed werd toegepast. Waartoe dient het regenbanden te plaatsen als men niet regelmatig het slijtageniveau nakijkt? Waartoe dient het plaatsen van een antivirus die zelden geupdate wordt?
Bepaalde OCMW's zijn geen betrokken partij voor sommige vragen. Het merendeel der OCMW's dient dus niet te beantwoorden aan de vragen over de ontwikkeling en het onderhoud van toepassingen, maar de enkele OCMW's die hier wel voor in aanmerking komen, dienen hier dus wel aan te beantwoorden. Dus als bepaalde vragen niet geldig zijn voor uw omgeving, kan u hierop antwoorden met: nvt: niet van toepassing.
Bij het lezen van de vragenlijst, zal u vaststellen dat verschillende vragen terugkomen in verschillende domeinen van de veiligheid. Zo zal gevraagd worden of de toegang tot het OCMW gecontroleerd wordt, of de toegang tot het serverlokaal beschermd wordt, of de toegang tot de pc's, het netwerk en de toepassingen beschermd is.
Ondanks de herhaling van deze vragen, zijn deze noodzakelijk want het heeft geen zin om de ene toegang af te sluiten en de andere elders open te laten.

En daarna?

Deze vragenlijst moet gezien worden als louter een hulpmiddel en niet als een bewijsstuk van de onkunde van de veiligheidsconsulent om de minimale veiligheidsnormen te concretiseren binnen zijn OCMW. De lijst kan ook dienen als een gids voor de prioriteiten.
Indien er zware fouten in de staat van de veiligheid worden geconstateerd, dan moet er overleg gepleegd worden met één of meerdere interne verantwoordelijken, eventueel met een ervaren collega of met een externe consulent (de helpdesk van de POD, uw leverancier van sociale software, een bestaande informatica-vereniging, andere) die u kan helpen met het relativeren van de vaststellingen en bij het toepassen van de juiste maatregelen.
Wanneer het audit-domein u te technisch lijkt, twijfel dan niet om er specialisten bij te roepen (systeembeheerder, leverancier) die u kunnen uitleggen met eenvoudig woorden waar het over gaat en of aan de veiligheidsnorm werd voldaan.
Indien de resultaten van de audit u positief lijken: des te beter, maar blijf toch aandachtig.

Veel succes

De veiligheidsdienst van de POD MI

Veiligheidsaudit

I.	Organisatie en Structuur	J	N	NVT	Commentaren
1	Werd er de afgelopen drie jaar een studie uitgevoerd naar de algemene bedreigingen voor de instelling ?				
2	Bestaat er een organigram van de instelling dat minstens éénmaal per jaar wordt bijgewerkt en verspreid onder het personeel ?				
3	Bestaat er voor elke functie een beschrijving van de verantwoordelijkheden en wordt deze ter beschikking gesteld van de betrokkenen?				
4	Wordt in deze taakbeschrijving duidelijk aangegeven welke de verantwoordelijkheden zijn op het gebied van de veiligheid en de bescherming van de gegevens en het gebruikte informaticamateriaal?				
5	Is er binnen de instelling een persoon uitdrukkelijk belast met de arbeidsveiligheid en wordt dit aangegeven op het organigram?				
6	Is er binnen de instelling een persoon uitdrukkelijk belast met de informatieveiligheid en wordt dit aangegeven op het organigram?				
7	Beschikt de veiligheidsconsulent over voldoende kennis om zijn taak waar te nemen ?				
8	Legt de verantwoordelijke voor de informatieveiligheid enkel verantwoording af aan de sociale raad ?				
9	Is de verantwoordelijke voor de informatieveiligheid zowel hiërarchisch als functioneel onafhankelijk van de informaticadienst?				

I.	Organisatie en Structuur	J	N	NVT	Commentaren
10	Oefent de veiligheidsconsulent andere functies uit die onverenigbaar zijn met zijn veiligheidstaak (bv: verantwoordelijke van informatica) ?				
11	Is de identiteit van de veiligheidsconsulent en zijn eventuele adjunct(en) meegedeeld aan de Is aan de veiligheidscel van de POD Maatschappelijke Integratie het aantal uren medegedeeld dat officieel werd toegekend aan de veiligheidsconsulent en zijn eventuele adjunct(en) voor de uitvoering van hun taak ?				
12	Beschikt de instelling over een veiligheidsplan dat goedgekeurd werd door de verantwoordelijke instantie van de betrokken instelling ?				
13	Beschikt men over de nodige werkingskredieten, goedgekeurd door de verantwoordelijke instantie van de betrokken instelling, om in de uitvoering van het veiligheidsplan te kunnen voorzien?				
14	Zijn deze werkingskredieten opgenomen in een aparte veiligheidsbegroting ?				
15	Wordt de veiligheidsconsulent op de hoogte gebracht van incidenten die de informatieveiligheid in het gedrang kunnen brengen ?				
16	Worden deze incidenten mee opgenomen in het jaarlijks verslag (zoals voorzien in art 8 van het KB op de informatieveiligheid van 12 augustus 1993)?				

I.	Organisatie en Structuur	J	N	NVT	Commentaren
17	Wordt de veiligheidsconsulent tijdig geraadpleegd indien beslissingen moeten genomen worden waarbij veiligheidsaspecten kunnen optreden ?				
18	Ontvangt de veiligheidsconsulent vanwege de secretaris een beslissing over een veiligheidsadvies binnen de opgelegde termijn (3 maanden)?				
19	Legt de veiligheidsconsulent voldoende documentatie aan met betrekking tot de informatieveiligheid?				
20	Voorziet men bij de aankoop van hardware en software in het lastenboek specifieke veiligheidsnormen die vastgelegd zijn in samenspraak met de veiligheidsconsulent?				
21	Wordt alle informatie beoordeeld in functie van haar beschikbaarheid, integriteit of vertrouwelijkheid ?				
22	Worden er in functie van bovenstaande beoordeling procedures toegepast naargelang het soort document?				
23	Worden er (geregeld) informatica-audits uitgevoerd?				
24	Is er een strategische planning van de informaticabehoeften?				
25	Wordt deze strategische planning omgezet in een jaarlijkse planning en begroting?				
26	Voor de OCMW's die over meer dan 1 informaticus beschikken: is er een taakrotatiesysteem voor de informatici?				
27	Kan een informaticus elk jaar voldoende vorming genieten?				

I	Organisatie en Structuur	J	N	NVT	Commentaren
28	Wordt daarbij specifiek aandacht besteed aan de informatieveiligheid ?				
29	Werd er een deontologische code opgesteld en heeft men het personeel in functie hiervoor gesensibiliseerd ?				
30	Wordt er bijzondere aandacht besteed aan de rekrutering van personeel voor "gevoelige" functies ?				
31	Besteedt men bij de nieuw aangeworvenen aandacht aan de algemene veiligheid ?				
II.	**Fysieke veiligheid**				
	Brand				
1	Is er een branddetectiesysteem in het gehele gebouw ?				
2	Is er een branddetectiesysteem in plaatsen (technische schachten, kokers, vloeren, ...) met veel elektrische kabels ?				
3	Is het serverlokaal uitgerust met een branddetectiesysteem dat verbonden is met een centraal systeem ?				
4	Zijn de detectoren verbonden met een synoptisch paneel dat toelaat de eventuele vuurhaard ogenblikkelijk te lokaliseren ?				
5	Worden alle alarmen (brand, beweging, ...) doorgeschakeld naar een externe bewakingsfirma buiten de werkuren ?				

II	Fysieke veiligheid	J	N	NVT	Commentaren
6	Bestaat er een procedure voor de taken (uitschakelen van de stroom, sluiten van de kasten,...) die direct na een brandalarm uitgevoerd moeten worden ?				
7	Is het serverlokaal uitgerust met een regelmatig geteste en onderhouden automatische blusinstallatie?				
8	Zijn alle lokalen voorzien van manuele brandblusapparaten (met een aangepast blusmiddel) ?				
9	Wordt er een specifieke opleiding en training voor het gebruik van de brandblusmiddelen voorzien voor de leden van de interventieploeg ?				
10	Wordt deze specifieke opleiding en training voor de leden van de interventieploeg regelmatig herhaald ?				
11	Wordt een specifieke opleiding en training voor het gebruik van de brandblusapparaten voorzien voor de personeelsleden van het serverlokaal ?				
12	Wordt deze specifieke opleiding en training voor de personeelsleden van het servelokaal regelmatig herhaald ?				
13	Is het serverlokaal ingericht met onbrandbare materialen ?				
14	Worden er in de onmiddellijke omgeving van het serverlokaal brandbare producten opgeslagen ?				
15	Worden er in het serverlokaal brandbare producten opgeslagen (handleidingen, papiervoorraad, kuisproducten)?				

II	Fysieke veiligheid	J	N	NVT	Commentaren
16	Staan er in het serverlokaal toestellen die vreemd zijn aan de functie van het lokaal (kopieertoestel, faxtoestel, printer, huishoudapparatuur, papierversnipperaar ?				
17	Kan de brandweer het gebouw gemakkelijk bereiken?				
18	Kan de brandweer het serverlokaal gemakkelijk bereiken ?				
19	Heeft de brandweer het gebouw en het serverlokaal bezocht ?				
20	Geldt er een algemeen rookverbod in de gebouwen ?				
21	Geldt er een absoluut rookverbod in het serverlokaal ?				
22	Wordt dit verbod gerespecteerd?				
	Water				
23	Heeft wateroverlast in het verleden reeds problemen veroorzaakt (riolering, lekkende kranen, overstromingen, stortregens,...) ?				
24	Is het plafond van het serverlokaal waterdicht ?				
25	Zijn de waterleidingen in de nabijheid van het serverlokaal uitgerust met kranen zodat zij bij eventuele lekken gemakkelijk gesloten kunnen worden ?				
26	Bevinden er zich regelmatig geteste waterdetectoren in de nabijheid van de waterleidingen en in de valse vloer ?				
27	Is er een afvloeisysteem voor water voorzien in het serverlokaal ?				

II	Fysieke veiligheid	J	N	NVT	Commentaren
	Bliksem				
28	Is het gebouw beveiligd tegen blikseminslag ?				
29	Zijn de lokalen waarin de informatica-apparatuur is ondergebracht, beveiligd tegen blikseminslag ?				
	Bekabeling				
30	Werd er rekening gehouden met de elektromagnetische compatibiliteit?				
31	Zijn de kabels voor de elektriciteitsvoorziening en voor de telecommunicatie overal in het gebouw duidelijk gescheiden?				
32	Zijn de kabels onder de valse vloer van het serverlokaal bevestigd op rails of op andere ondersteuningsmiddelen (andere dan de echte vloer) ?				
33	Is de hoogte van de valse vloer voldoende ?				
34	Zijn alle kabels gemerkt (aan begin en uiteinde) en worden de schema's ervan permanent bijgewerkt ?				
35	Worden alle informaticakabels en stopcontacten op minstens 15 cm boven de oppervlakte van de vloer geplaatst ?				
	Toegang				
36	Worden alle onderhouds- en herstelwerkzaamheden in het serverlokaal uitgevoerd onder voortdurende controle van bevoegd intern personeel ?				
37	Is het serverlokaal gescheiden van de publieke zones in het gebouw ?				

II	Fysieke veiligheid	J	N	NVT	Commentaren
38	Wordt er in de publieke zone verwezen naar de ligging van het serverlokaal (via bewegwijzering of op de evacuatieplannen)?				
39	Wordt de toegang tot het gebouw gecontroleerd ?				
40	Is er een lijst van wie via welk middel (sleutel, badge, code, andere) toegang heeft tot welk lokaal?				
41	Wordt deze lijst aangepast en het middel teruggevraagd indien iemand niet langer geauthoriseerd is om toegang te krijgen?				
42	Worden logfiles van een elektronisch toegangscontrolesysteem meerdere malen per jaar nagekeken teneinde misbruik op te sporen (bvb pogingen om toegang te krijgen tot een lokaal waar men geen rechten toe heeft, gebruik van een kaart door iemand anders bij afwezigheid, …) ?				
43	Wordt bij verlies van het middel ogenblikkelijk een aanpassing gedaan aan het systeem teneinde ongeoorloofd gebruik van het middel te voorkomen? (bvb badge ongeldig maken in software, slot vervangen, …) ?				
44	Zijn er schriftelijke procedures vastgelegd i.v.m. de toegangscontrole en worden deze procedures toegepast ?				
45	Is er een controlesysteem (sleutel, badge, code, andere) voor de toegang tot het serverlokaal ?				

II	Fysieke veiligheid	J	N	NVT	Commentaren
46	Bieden alle toegangswegen die leiden tot het serverlokaal eenzelfde fysieke inbraakvertraging voor een inbreker? (bvb via normale toegangswegen, via nooduitgang, via dakkoepel, via kelder, via garage, etc) ?				
47	Is het serverlokaal altijd gesloten voor onbevoegde gebruikers?				
48	**Voor de OCMW's waar men programma's ontwikkelt.** Is er een controlesysteem voor de toegang tot de lokalen waar de programmeringsdossiers worden bewaard ?				
49	Is er een controlesysteem voor de toegang tot de lokalen waar de sociale dossiers worden bewaard ?				
50	Is er een efficiënte inbraakbeveiliging (detectie en interventie) voorzien voor het gebouw ?				
51	Is er een efficiënte inbraakbeveiliging (detectie en interventie) voorzien voor de lokalen waarin informatica-apparatuur is ondergebracht ?				
52	Zijn de archiveringslokalen fysiek gescheiden van de andere informaticalokalen ?				
53	Zijn de archiveringslokalen beschermd in functie van de specifieke risico's ?				
54	Wordt het geheel van het toegangscontrolesysteem regelmatig getest?				
55	Wordt er een specifieke procedure toegepast voor de toegangscontrole bij bezoekers?				

II	Fysieke veiligheid	J	N	NVT	Commentaren
56	Worden de sleutels en tijdelijke (bezoekers-) badges op een veilige plaats bewaard?				
57	Is het toegangscontrolesysteem geïntegreerd in een automatische verwerking van de alarmen ?				
58	Is het serverlokaal volledig gewijd aan informatica-activiteiten (geen printers, plooi- en snijmachines, ...); en is ze dus fysiek gescheiden van alle lokalen waar andere activiteiten worden uitgevoerd ?				
59	Wordt de informatica-apparatuur minstens eenmaal per jaar stofvrijgemaakt ?				
60	Zijn de niet-publieke delen afgeschermd voor het publiek via een fysische barrière (deur, poort, hek,…)?				
61	Wordt het gebouw buiten de kantooruren door derden gebruikt?				
	Airconditioning				
62	Is het serverlokaal uitgerust met een airconditioning met voldoende capaciteit ?				

II		O	N	SO	Commentaires
67					
68					
III					
1					
2					
3					
4					
5					
6					
7					
8					

1 : ces questions ne s'adressent qu'aux quelques CPAS qui développent eux-mêmes leurs programmes.

III		O	N	SO	Commentaires
9					
10					
11					
12					
13					
14					
IV					
1					
2					
3					
4					

IV		O	N	SO	Commentaires
5					
6					
7					
8					
V					
1					
2					
3					
4					
5					
6					
7					

V		O	N	SO	Commentaires
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
V		**O**	**N**	**SO**	**Commentaires**
18					
19					
20					
21					
22					
23					
24					
25					
26					
27					
28					
29					

V		O	N	SO	Commentaires
30					
31					
32					
33					
34					
35					
36					
37					
38					
39					
40					
41					
42					

V		O	N	SO	Commentaires
43					
44					
45					
VI					
1					
2					
3					
4					
5					
6					
7					

VI		O	N	SO	Commentaires
8					
9					
10					
11					
12					
13					
14					
15					

VI		O	N	SO	Commentaires
16					
17					
VII					
1					
2					
3					
4					
5					
6					
7					

VII		O	N	SO	Commentaires
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					

VII		O	N	SO	Commentaires
20					
21					
22					
23					