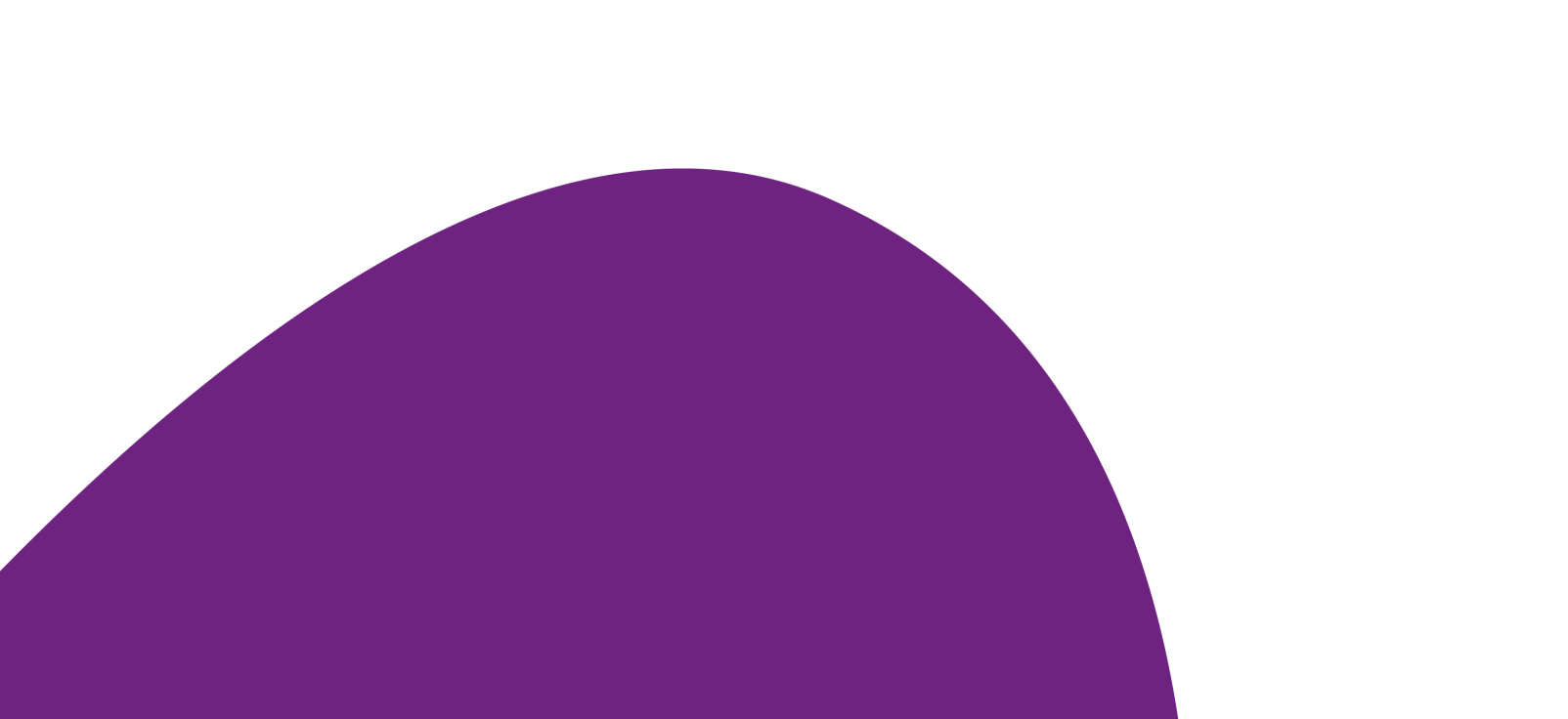
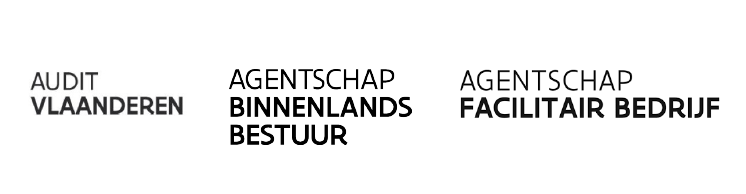
Project  
Cyberveilige gemeenten

Informatieveiligheidsplan





**Inleiding**

In het merendeel van lokale besturen gaat men actief aan de slag met persoonsgegevens en andere gevoelige informatie op IT-systemen en netwerken. Het is dan ook cruciaal om een helder en bruikbaar plan voor informatieveiligheid op te stellen en onderhouden. Om een duidelijk kader te voorzien bij het plan van aanpak, is het aanbevolen om te kijken naar bestaande normen en regelgevingen die een kader scheppen. Bij het opstellen van dit plan werd gekeken naar de internationale informatiebeveiligingsnorm ISO 27002, maar kan men ook gebruik maken van andere bestaande richtsnoeren.

**De krijtlijnen in dit plan zijn van toepassing op:**

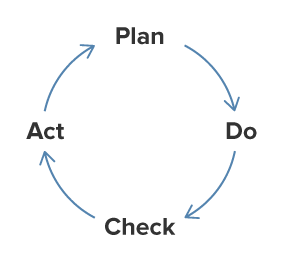
* Personen die met gevoelige informatie in aanraking komen tijdens hun werkzaamheden in het lokaal bestuur: medewerkers, bestuurders, stagiairs, vrijwilligers, externen die toegang krijgen tot gegevens, …
* Informatiesystemen: middelen die kritische informatie bevatten of toegang kunnen geven tot de informatie(systemen) van het lokaal bestuur. Hierbij gaat het om ICT-infrastructuur, toegangscontrolesystemen, IT-middelen zoals desktops, laptops, tablets, smartphones, archieven: ICT-infrastructuur, toegangscontrolesysteem, branddetectiesysteem, inbraakalarm, gebouwen, IT-middelen zoals desktop, laptop, tablet, smartphone, lokalen en kasten (sleutels), archief, ...

Bij elk van de te behandelen acties die worden ondernomen in kader van het ontwikkelen en beheren van het veiligheidsplan moet er steeds nagedacht worden over enkele factoren en processen die een invloed hierop kunnen hebben:

* Met welke risico’s, kwetsbaarheden en bedreigingen komt het lokaal bestuur in aanraking?
* Wat is de waarschijnlijkheid van de gedefinieerde risico’s?
* Werd reeds een maturiteitsmeeting ondernomen die bepaalde pijnpunten heeft blootgelegd?
* Indien er een incidentenregister wordt bijgehouden: welke noden komen er naar boven uit analyses hiervan?
* Welke tekortkomingen komen naar boven bij de evaluatie van het huidige veiligheidsplan?

Omdat de technologie, noden van inwoners en klanten, infrastructuur en breed genomen de totale omgeving van lokale besturen constant in verandering zijn, moet dit plan regelmatig onder de loep genomen worden om de status en doelen te actualiseren en te kijken of er (tussentijdse) bijsturingen nodig zijn. Een periode van maximaal drie jaar voor het bijsturen van het informatieveiligheidsplan is aangewezen.

Het is ook aangewezen dat de opmaak en bijsturing van dit plan via een vastgelegd proces gebeurt. De PDCA cyclus is hiervoor een goede inspiratiebron, omdat deze duidelijk maakt dat het hier om een proces van continue verbetering gaat. Plan, do, check, act, om deze oefening op regelmatige basis te herhalen en blijvend te optimaliseren.



**Ontwikkeling informatieveiligheidsplan**

Om tot een optimale beveiliging van informatie te komen, is het aangewezen om te vertrekken vanuit een risicoanalyse die in kaart brengt welke verbeteringen mogelijk zijn. Op basis van de risicoanalyse kan een veiligheidsbeleid uitgewerkt worden - een breder algemeen kader - om dit algemeen beleid vervolgens te vertalen naar een gedetailleerd plan van aanpak: het zogenaamde veiligheidsplan.

Voorafgaand aan de risicoanalyse kan een gespreksronde uitgevoerd worden om belangrijke problematieken te inventariseren die zeker aan bod dienen te komen in de risicoanalyse. Dit kan ook helpen om enkele concrete risico’s reeds te identificeren.De risicoanalyse neemt bij vele DPO/CISO’s de vorm aan van een workshop met het lokale managementteam, waarbij voor elk geïdentificeerd risico uit de voorafgaande inventarisatie of eigenlijke risicoanalyse geformuleerd wordt:

1. Hoe groot de waarschijnlijkheid van optreden is
2. Wat de impact voor de organisatie zou zijn
3. Welke kost vereist is om het risico te vermijden.

De thema’s die aan bod komen tijdens dit proces kunnen geïntegreerd worden in het bredere veiligheidsplan en het uitgewerkte veiligheidsplan.

Het veiligheidsplan kan beschouwd worden als een advies zoals opgenomen in het Besluit van de Vlaamse Regering van 15 mei 2009 betreffende de veiligheidsconsulenten, artikel 10 en 3. Het plan dient dan ook binnen een termijn van maximum drie maanden goedgekeurd te worden door het ultieme beslissingsorgaan van het lokaal bestuur.

Samengevat ziet het aanbevolen proces er als volgt uit:

1. **Fase 1:** Inventarisatie van de problematiek
2. **Fase 2:** Uitvoeren van een risicoanalyse
3. **Fase 3:** Opmaak veiligheidsbeleid en veiligheidsplanplan

Het opstellen van een informatieveiligheidsplan is een belangrijke eerste stap, maar het is ook belangrijk dat dit vertaald wordt naar concrete acties en dat de stand van zaken hiervan optimaal kan opgevolgd worden. Daarom werd een bijkomend opvolgingsplan toegevoegd aan dit plan (Excel-formaat), die de aanbevelingen uit het informatieveiligheidsplan omzet in stappen die ondernomen worden, met de nodige informatie om de stand van zaken op te vragen.

De functionaris gegevensbescherming dient bovendien jaarlijks naar het lokaal bestuur te rapporteren over de stand van zaken inzake de informatieveiligheid door middel van een bondig jaarverslag. Dit verslag geeft inzage in de algemene veiligheidstoestand, alsook welke geplande acties concreet uitgevoerd werden en welke vertraging hebben opgelopen of bijkomende stappen vereisen.

**Contactinfo**

|  |  |  |
| --- | --- | --- |
| Lokaal bestuur | Gemeente | Contactgegevens |
|  | adres |  |
|  |  |  |
| Algemeen directeur | naam | [emailadres](mailto:jeroen.peeters@olen.be) |
|  |  |  |
| Eerste aanspreekpunt bij bestuur | naam | [emailadres](mailto:jeroen.peeters@olen.be) |
|  |  |  |
| Functionaris gegevensbescherming | naam | [emailadres](mailto:jeroen.peeters@olen.be) |
|  |  |  |
| Samenstelling informatieveiligheidscel | naam | [emailadres](mailto:jeroen.peeters@olen.be) |
|  | naam | [emailadres](mailto:jeroen.peeters@olen.be) |
|  | naam | [emailadres](mailto:jeroen.peeters@olen.be) |
|  | naam | [emailadres](mailto:jeroen.peeters@olen.be) |
|  | naam | [emailadres](mailto:jeroen.peeters@olen.be) |
|  |  |  |
| Contactinfo privacyverklaring |  |  |
|  |  |  |
| Locaties | Gemeentebestuur |  |
|  | OCMW |  |
|  | Scholen |  |
|  | Bibliotheek |  |
|  | Woonzorgcentrum |  |
|  | AGB |  |
|  | … |  |

Handleiding bij het informatieveiligheidsplan

Zoals eerder vermeld werd dit sjabloon opgesteld met de ISO-27002 standaard als overkoepelend raamwerk. De 15 hoofdstukken worden gebruikt om het informatieveiligheidsplan op te delen in verschillende luiken zoals risicomanagement, beleid en leveranciersrelaties. Deze verschillende luiken in het plan dienen aangevuld te worden met informatie die voortkomt uit de actuele situatie in het lokale bestuur, recente risicoanalyses, inventarisaties en evaluaties. Het sjabloon werd ingevuld met informatie uit een fictief lokaal bestuur om zo houvast te bieden voor de verdere uitwerking. Deze informatie overschrijf je met een situatieschets en aanbevelingen die concreet op jouw lokaal bestuur betrekking hebben. Hieronder lichten we kort toe welke zaken zoal aangevuld dienen te worden.

1. Omschrijving huidige situatie

Hierin schrijf je een behapbare situatieschets neer voor het lokaal bestuur. Vermeld in krijtlijnen welke beveiligingsmaatregelen reeds aanwezig zijn, maar ook welke tot op heden ontbreken. Hiervoor kan de output uit de voorafgaande inventarisatie en risicoanalyse gebruikt worden, aangevuld waar nodig met normen uit de ISO-standaard waaraan nog niet (volledig voldaan is). Deze samenvatting geeft directie, IT-medewerkers en andere relevante actoren zicht op de baseline binnen het lokaal bestuur.

2. Omschrijving concrete aanbevelingen

De belangrijkste aanbevelingen op basis van de risicoanalyse worden bondig geformuleerd in deze rubriek. Het gaat hier over maatregelen die voldoende concreet zijn om vertaald te worden naar te nemen acties. Denk hierbij aan het opzetten van vorming rond informatieveiligheid voor gemeentepersoneel of het uitschrijven van een geformaliseerde back-up procedure. Aan de aanbevelingen voeg je een nummer toe voor verdere opvolging: \*cijfer hoofdstuk\*.\*cijfer tussentitel\*.\*nummer aanbeveling\*.

3. Omschrijving reactie schepencollege/secretaris

Werd een aanbeveling uit het plan voorgelegd aan het schepencollege of een ander intern beslissingsorgaan? Neem deze dan op in de tabel onder de concrete aanbevelingen, met het nummer van de aanbeveling waarop deze reactie of beslissing weerslag heeft. Het kan hierbij gaan over een goedkeuring om over te gaan tot de uitwerking van concrete acties om gehoor te geven aan de aanbeveling tot een verduidelijking over wie verantwoordelijk is voor de concrete aanbeveling of het prioriteren van bepaalde aanbevelingen.

4. Opvolgingsplan

In het opvolgingsplan worden de concrete acties opgenomen die voortvloeien uit de aanbevelingen binnen het informatieveiligheidsplan en de reacties van het schepencollege. Het gaat hier over specifieke werkpunten die binnen een bepaalde termijn gerealiseerd moeten of kunnen worden, gestoeld op de richtsnoeren en bijhorende aanbevelingen.

De bovenste rij uit het sjabloon opvolgingsplan (beschikbaar in Excel-formaat) werd reeds ingevuld, als voorbeeld van het type informatie dat in de verschillende kolommen dient toegevoegd te worden. Indien er voor bepaalde richtsnoeren geen aanbevelingen zijn, kunnen deze rijen verwijderd worden uit de Excelsheet.

Aan het opvolgingsplan werd ook een maturiteitsmeting toegevoegd die gebruikt kan worden om de vooruitgang op het gebied van informatieveiligheid in kaart te brengen. De berekening hiervoor verloopt als volgt:

* Indien er 5 vragen zijn voor 1 hoofdstuk (bv. Risico), telt elke vraag mee voor 20% (om zo te komen tot een totaalscore van 100%).
* Wanneer aan een vraag gedeeltelijk is tegemoet gekomen met een actie, is het mogelijk om aan deze concrete vraag een score van bv. 50% toe te kennen. Wanneer een vraag meetelt voor 20% bedraagt de behaalde score 10% (= 20\*0.5).
* Wanneer van de 5 vragen voor één hoofdstuk vier vragen volledig beantwoord werden met een actie, met één vraag die slechts gedeeltelijk werd beantwoord, bedraagt de maturiteitsscore voor dat hoofdstuk dus 90% (=20+20+20+20+10).

5. Jaarverslag

Voor de opmaak van het jaarverslag kunnen de aanbevelingen en actiepunten uit het opvolgingsplan gebruikt worden. Op basis van het veld met de datum van de laatste update kan je filteren op jaartal en zo alle relevante informatie voor een jaar oplijsten, om deze informatie dan te exporteren naar een PDF-versie die overlopen kan worden met het lokaal bestuur.

Inhoudstafel

[1. Risico 13](#_Toc72096155)

[1.1 Beoordelen van beveiligingsrisico’s 13](#_Toc72096156)

[1.2 Behandelen van beveiligingsrisico’s 14](#_Toc72096157)

[2. Beleid 16](#_Toc72096158)

[2.1 Informatiebeveiligingsbeleid 16](#_Toc72096159)

[3. Organisatie 17](#_Toc72096160)

[3.1 Interne organisatie rond informatiebeveiliging 17](#_Toc72096161)

[3.2 Mobiel werken 18](#_Toc72096162)

[4. Informatiebeveiliging 20](#_Toc72096163)

[4.1 Informatiebeveiliging voorafgaand aan het dienstverband 20](#_Toc72096164)

[4.2 Informatiebeveiliging tijdens het dienstverband 21](#_Toc72096165)

[4.3 Informatiebeveiliging bij beëindiging of wijziging van dienstverband 21](#_Toc72096166)

[5. Bedrijfsmiddelen 24](#_Toc72096167)

[5.1 Verantwoordelijkheid voor bedrijfsmiddelen 24](#_Toc72096168)

[5.2 Classificatie van informatie 25](#_Toc72096169)

[5.3 Behandelen van media 25](#_Toc72096170)

[6. Toegang tot persoonsgegevens 27](#_Toc72096171)

[6.1 Eisen voor toegangsbeveiliging 27](#_Toc72096172)

[6.2 Verantwoordelijke voor toegangsrechten van gebruikers 27](#_Toc72096173)

[6.3 Verantwoordelijkheden van gebruikers 28](#_Toc72096174)

[6.4 Toegangsbeveiliging van systemen en toepassingen 30](#_Toc72096175)

[7. Cryptografie 32](#_Toc72096176)

[7.1 Cryptografische beheersmaatregelen 32](#_Toc72096177)

[8. Fysieke beveiliging 33](#_Toc72096178)

[8.1 Beveiliging van de omgeving 33](#_Toc72096179)

[8.2 Beveiligde apparatuur 34](#_Toc72096180)

[9. Operationele beveiliging 36](#_Toc72096181)

[9.1 Operationele procedures en verantwoordelijkheden 36](#_Toc72096182)

[9.2 Bescherming tegen malware 36](#_Toc72096183)

[9.3 Back-up 38](#_Toc72096184)

[9.4 Monitoring 39](#_Toc72096185)

[9.5 Overwegingen bij audits van informatiesystemen 39](#_Toc72096186)

[10. Communicatiebeveiliging 41](#_Toc72096187)

[10.1 Netwerkbeveiliging 41](#_Toc72096188)

[10.2 Informatietransport 42](#_Toc72096189)

[11. Aanschaffen, ontwikkelen en onderhouden van informatiesystemen 44](#_Toc72096190)

[11.1 Beveiligingseisen voor informatiesystemen 44](#_Toc72096191)

[11.2 Beveiliging in ontwikkelings- en ondersteuningsprocessen 44](#_Toc72096192)

[12. Leveranciersrelaties 46](#_Toc72096193)

[12.1 Informatiebeveiliging in leveranciersrelaties 46](#_Toc72096194)

[13. Informatiebeveiligingsincidenten 48](#_Toc72096195)

[13.1 Beheer van informatiebeveiligingsincidenten en -verbeteringen 48](#_Toc72096196)

[14. Bedrijfscontinuïteit 50](#_Toc72096197)

[14.1 Informatiebeveiligingscontinuïteit 50](#_Toc72096198)

[14.2 Redundante componenten 51](#_Toc72096199)

[15. Naleving 53](#_Toc72096200)

[15.1 Naleving van wettelijke voorschriften 53](#_Toc72096201)

[15.2 Informatiebeveiligingsbeoordelingen 54](#_Toc72096202)

[16. Bijlage 1: ISO-norm 27002 (controls) 55](#_Toc72096203)

1. Risico

* 1. BEOORDELEN VAN BEVEILIGINGSRISICO’S

**Omschrijving huidige situatie**

[Bv. Er werd reeds een eerste, beperkte, globale risicoanalyse opgemaakt voor het serverlokaal en enkele interne en externe databanken waarin gevoelige informatie opgeslagen zit. Er is momenteel echter nog geen overzicht van alle aanwezige databanken en opslagplaatsen en het beheer van de toegangen hierbij.]

**Concrete aanbevelingen**

[Bv. Per gemeentelijke dienst moet in kaart gebracht worden tot welke databanken met persoonsgegevens medewerkers toegang hebben en op welke wijze deze toegangen beheerd worden. Via deze weg kan geëvalueerd worden of en hoe de bestaande risicoanalyse bijgestuurd moet worden.

Door een inventaris op te maken met de verschillende databanken en opslagplaatsen kan een prioritaire rangorde uitgewerkt worden naar gelang de gevoeligheid van gegevens die deze bevatten. Voor de diensten die gebruik maken van databanken en opslagplaatsen met zeer gevoelige gegevens dient een duidelijk en uniform toegangsbeleid uitgewerkt worden, waarin duidelijk beschreven wordt welke medewerkers toegang kunnen krijgen en op welke wijze deze toegangen verleend en ingetrokken worden.]

**Normen van toepassing**

|  |  |  |
| --- | --- | --- |
| De aangehaalde aanbevelingen kaderen binnen onderstaande normen | | |
| A1.1.1 ISO 27005-8 |  |  |
|  |  |  |
|  |  |  |

* 1. BEHANDELEN VAN BEVEILIGINGSRISICO’S

**Huidige toestand**

[Bv. Het behandelen van beveiligingsrisico’s kan pas nadat deze duidelijk in kaart zijn gebracht. Aangezien de inventarisatie van databanken en opslagplaatsen eerder beperkt is, is er slechts een beperkte globale risicoanalyse voor handen. Het is dan ook niet mogelijk op dit moment om voor alle systemen en toepassingen na te gaan over de nodige beheersmaatregelen genomen werden.

De reeds bestaande risicoanalyse leert wel dat de kans op het voorvallen van de vastgelegde risico’s beperkt is of dat deze reeds aangepakt werden via diverse preventieve maatregelen. Desalniettemin moet gekeken worden of deze conclusie nog steeds geldt wanneer de scope van de risicoanalyse uitgebreid wordt. Daarnaast zijn nog niet alle risico’s uit de huidige risicoanalyse afgedekt.]

**Concrete aanbevelingen**

[Bv. In navolging van de aanbevelingen in sectie 1.1 dient de huidige risicoanalyse geüpdatet worden nadat de interne en externe databanken en opslagplaatsen met gevoelige gegevens in kaart gebracht worden. Op basis van de herwerkte risicoanalyse dient gekeken te worden of aanvullende beheersmaatregelen wenselijk zijn, zoals de aanschaf van een Access and Identity Management System dat het automatisch beheren van toegangen en rechten mogelijk maakt.

Het invoeren van Multi-Factor-Authenticatie (MFA) voor alle systemen en toepassingen die gebruikt worden om persoonsgegevens in te kijken of verwerken kan de veiligheid verhogen. Concreet houdt dit in dat een medewerker na het invoeren van een wachtwoord zijn/haar identiteit nogmaals dienst te bevestigen via een andere methode, zoals een code op de mobiele telefoon.

Momenteel heeft de organisatie slechts beperkt zicht op welke zaken gedekt worden door de onderhoudscontracten met externe leveranciers en welke garanties daarbij horen. Het is dan ook aanbevolen dat de huidige onderhoudscontracten op een vaste locatie te vinden zijn en dat op basis van een grondige studie weergegeven wordt welke garanties en dienstverlening van toepassing zijn.

Om te kunnen garanderen dat de organisatie haar dienstverlening kan garanderen in geval van een cyberaanval of ander IT-gerelateerd incident is het cruciaal dat de noodstroomvoorziening optimaal functioneert. Een jaarlijkse controle is aanbevolen.

In het verleden viel al voor dat de deuren van de serverlokalen niet afgesloten werden. Het is belangrijk om er op toe te zien dat dit niet gebeurt.]

**Normen van toepassing**

|  |  |  |
| --- | --- | --- |
| De aangehaalde aanbevelingen kaderen binnen onderstaande normen | | |
| A1.2.1 ISO 27005-9 |  |  |
|  |  |  |
|  |  |  |

1. Beleid
   1. INFORMATIEBEVEILIGINGSBELEID

**Huidige toestand**

[Bv. Momenteel ontbreekt een geactualiseerde versie van het informatieveiligheidsbeleid waarin de taken van de veiligheidsconsulent of functionaris gegevensbescherming en de verantwoordelijkheden van het bestuur en de personeelsleden vastgelegd worden. Een actueel informatieveiligheidsplan dat de krijtlijnen uit het informatieveiligheidsbeleid concretiseert is echter wel voor handen.

Het informatieveiligheidsplan dat elke drie jaar automatisch herzien wordt, werd afgetoetst en goedgekeurd door de organisatie. De bepalingen hierin werden en worden vertaald naar concrete acties met bijhorende timings in het opvolgingsplan (op te vragen bij **DPO XXX**). Door middel van het opvolgingsplan is men te allen tijde op de hoogte van de stappen die het lokaal bestuur neemt om tot de gewenste situatie te komen. Op basis van het opvolgingsplan wordt elk jaar ook steeds een jaarverslag opgesteld dat aangeeft welke concrete acties ondernomen werden en wat de status van geplande acties is.]

**Concrete aanbevelingen**

[Bv. Het informatieveiligheidsbeleid dient geactualiseerd te worden, met een concrete omschrijving van de taken van de veiligheidsconsulent of functionaris gegevensbescherming (DPO) en de verantwoordelijkheden van het bestuur en de personeelsleden. Bevindingen uit de geplande uitbreiding van de risicoanalyse dienen hierin ook opgenomen te worden.

Het informatieveiligheidsplan moet elke drie jaar geëvalueerd en bijgestuurd worden. Nieuwe versies dienen steeds door de gemeenteraad goedgekeurd te worden.]

**Normen van toepassing**

|  |  |  |
| --- | --- | --- |
| De aangehaalde aanbevelingen kaderen binnen onderstaande normen | | |
| A2.1.1 ISO 27002-5.1 | A2.1.2 ISO 27002-5.1 |  |
|  |  |  |
|  |  |  |

1. Organisatie
   1. INTERNE ORGANISATIE ROND INFORMATIEBEVEILIGING

**Huidige toestand**

[Bv. Het schepencollege heeft op \*datum\* \*naam\* aangesteld als veiligheidsconsulent voor het gemeentebestuur. Tevens werd in deze collegebeslissing de oprichting van een informatieveiligheidscel goedgekeurd. Deze veiligheidscel zorgt voor de uitvoering van het beveiligingsbeleid en bestaat uit sleutelactoren binnen de organisatie. Deze cel komt minstens twee keer per jaar samen en nodigt ook andere medewerkers uit indien bijkomende visies of sensibilisering wenselijk zijn.

Er bestaat reeds een samenwerkingsakkoord tussen gemeente en OCMW. Voor informatieveiligheid zou het wenselijk zijn om 1 gezamenlijk beleid uit te werken voor de gemeente en het OCMW die de bevoegdheden en verantwoordelijkheden uitklaart.

Er is een beheersovereenkomst aanwezig tussen gemeente en \*namen software- of hardware leveranciers\*. Deze overeenkomsten worden jaarlijks vernieuwd en leggen duidelijk vast welke verantwoordelijkheden bij het lokaal bestuur en de toeleverancier liggen.]

**Concrete aanbevelingen**

[Bv. De organisatie dient in regelmatige sensibilisering te voorzien via een mix van methodes zoals waarschuwingsmails, interne campagnes, posters en vormingen, de verantwoordelijkheid hiervoor ligt bij de functionaris gegevensbescherming. Jaarlijks dienst minstens één sensibiliseringsactie voorzien te worden, met bijkomende initiatieven op basis van interne vragen en incidenten.

De veiligheidsconsultent en functionaris gegevensbescherming (DPO) dienen steeds te beschikken over de nodige gegevens om hun opdracht en werkzaamheden naar behoren te kunnen uitvoeren. Dit moet gefaciliteerd worden door een goede interne doorstroom van informatie, al dan niet vastgelegd in een interne verwittigingsboom.

Naar aanleiding van het samenwerkingsakkoord tussen de gemeente en het OCMW is het wenselijk om een gezamenlijk informatieveiligheidsbeleid uit te werken.]  
**Normen van toepassing**

|  |  |  |
| --- | --- | --- |
| De aangehaalde aanbevelingen kaderen binnen onderstaande normen | | |
| A3.1.1 ISO 27005-6.1 | A3.1.2 ISO 27005-6.1 | A3.1.3 ISO 27005-6.1 |
| A3.1.4 ISO 27005-6.1 | A3.1.7 ISO 27005-6.1 | A3.1.9 ISO 27005-6.1 |
|  |  |  |

* 1. Mobiel werken

**Huidige toestand**  
[Bv. Alle personeelsleden binnen de organisatie hebben de mogelijkheid om van thuis uit te werken, op vrijblijvende basis. Ze hebben van thuis uit ook toegang tot het gemeentelijk netwerk. Personeelsleden kunnen deze toegang aanvragen bij de ICT-dienst, en kunnen rekenen op een goedkeuring van deze vraag. Een uitgewerkt beleid met voorwaarden en beperkingen is nog niet aanwezig.

De organisatie beschikt zelf niet over smartphones, maar biedt personeelsleden wel de mogelijkheid om mails te raadplegen op hun persoonlijke smartphones. De ICT-dienst verleent hierbij assistentie waar nodig. Er bestaan geen richtlijnen in verband met de beveiliging van persoonlijke smartphones en hier wordt ook geen bijkomende sensibilisering rond voorzien.]

**Concrete aanbevelingen**

[Bv. Er dient een beleid opgemaakt te worden voor telewerk en het gebruik van mobiele middelen, waarin ook courante veiligheidsbepalingen vervat zitten. Het beleid moet zowel voorwaarden als beperkingen bevatten en kan na uitwerking geïntegreerd worden in het arbeidsreglement.

Het is wenselijk om elk jaar een sensibiliserende infosessie te voorzien waarin uitgelegd wordt welke extra risico’s mobiele apparatuur met zich meebrengt en welke voorzorgen genomen dienen te worden, zoals het niet aanzetten van de voorziene VPN via een privé-PC.

Waar mogelijk dienst sterke authenticatie afgedwongen te worden voor mobiele toegangen, met wachtwoorden van 12 tekens of meer met een combinatie van kleine letters, hoofdletters, speciale tekens en cijfers en Multi-Factor-Authenticatie waar nodig.

Voorzie in data loss prevention software die schendingen van beleidslijnen rond vertrouwelijke en kritieke informatie kan detecteren - zoals een medewerker die per ongeluk of expres gevoelige gegevens tracht te verzenden - en dergelijke inbreuken beantwoord met een waarschuwing, het versleutelen van de gegevens of andere beveiligingsmaatregelen.

**Normen van toepassing**

|  |  |  |
| --- | --- | --- |
| De aangehaalde aanbevelingen kaderen binnen onderstaande normen | | |
| A3.2.1 ISO 27002-6.2 | B3.2.1 ISO 27002-6.2 | A3.2.2 ISO 27002-6.2 |
| B3.2.2 ISO 27002-6.2 |  |  |
|  |  |  |

1. Informatiebeveiliging
   1. Informatiebeveiliging voorafgaand aan het dienstverband

**Huidige toestand**

[Bv. Tijdens de rekrutering en indiensttreding wordt er momenteel weinig aandacht besteed aan het benadrukken van het belang van informatieveiligheid.

Wel is er een onthaalprocedure aanwezig waarin dit even aan bod komt, met een peter of meter voor elke medewerker die het belang mee kunnen onderstrepen. Dit wordt wel niet formeel vastgelegd in de procedure. De personeelsdienst heeft een checklist (in het stappenplan ‘Onthalen nieuwe medewerkers’) met daarop alle taken die de personeelsdienst, de IT-dienst of de communicatiedienst moeten uitvoeren.

In het arbeidsreglement worden enkele bepalingen rond informatiebeveiliging aangehaald, maar deze worden niet bijkomend geduid en het document dient niet ondertekend te worden.]

**Concrete aanbevelingen**

[Bv. Hamer reeds tijdens het rekruteringsproces op het belang van informatieveiligheid. Een eerste stap kan bestaan uit een toevoeging bij toekomstige vacatures die reeds aanhaalt dat een gezonde informatieveiligheidshygiëne prioritair is voor de organisatie.

Verwerk in de huidige onthaalprocedure een luik waarbij de peter of meter van de nieuwe medewerker wijst op de verantwoordelijkheden rond informatiebeveiliging, zoals het hanteren van een clean desk policy en de wijze waarop gevoelige informatie veilig opgeslagen kan worden.

Het arbeidsreglement dient bij de indiensttreding voorgelegd worden ter ondertekening. Vooraf aan de ondertekening dienen de clausules rond informatiebeveiliging mondeling overlopen worden, zodat de toekomstige medewerker onduidelijkheden kan aankaarten.]

**Normen van toepassing**

|  |  |  |
| --- | --- | --- |
| De aangehaalde aanbevelingen kaderen binnen onderstaande normen | | |
| A4.1.1 ISO 27002-7.1 | A4.1.2 ISO 27002-7.1 |  |
|  |  |  |
|  |  |  |

* 1. INFORMATIEBEVEILIGING TIJDENS HET DIENSTVERBAND

**Huidige toestand**

[Bv. Er bestaat zowel een goedgekeurde versie van het arbeidsreglement als een deontologische code. Het arbeidsreglement wordt in 2021 vernieuwd, wat meteen ook de mogelijkheid biedt om de bestaande deontologische code te herzien.

Sensibiliseringsacties zijn eerder schaars en beperken zich vaak tot waarschuwingsmails bij reële dreigingen of voorvallen in andere lokale besturen.

Stagiairs, jobstudenten en externe medewerkers die belast zijn met het gebruik of de verwerking van persoonsgegevens moeten het arbeidsreglement en de deontologische code niet goedkeuren of ondertekenen.]  
 **Concrete aanbevelingen**

[Bv. Analoog met de aanbevelingen onder punt 3.1 dient jaarlijks minstens één organisatiebrede sensibiliseringsactie rond informatiebeveiliging georganiseerd te worden. Waarschuwingsmails rond praktijken als phishing bieden een meerwaarde, maar ook andere formaten en kanalen dienen aan bod te komen, zoals vormingsmomenten, posters en campagnes met zelf-ontwikkeld materiaal of bestaande dragers van bv. het CCB, Safe on Web en de Cyber Security Coalition.

Het arbeidsreglement en de deontologische code worden in de toekomst best ook ter ondertekening voorgelegd aan stagiairs, jobstudenten en externe medewerkers die persoonsgegevens verwerken of gebruiken in kader van hun activiteiten, zodat ook zij zich bewust zijn van de risico’s en gepaste handelingen.

Na de herziening van het arbeidsreglement in de tweede helft van 2021 dient de bestaande deontologische code onder handen genomen worden, zodat het beleid rond informatieveiligheid sterker aan bod komt.

**Normen van toepassing**

|  |  |  |
| --- | --- | --- |
| De aangehaalde aanbevelingen kaderen binnen onderstaande normen | | |
| A4.2.1 ISO 27002-7.2 | B4.2.1 ISO 27002-7.2 | A4.2.2 ISO 27002-7.2 |
| A4.2.3 ISO 27002-7.3 |  |  |
|  |  |  |

* 1. INFORMATIEBEVEILIGING BIJ BEËINDIGING OF WIJZIGING VAN DIENSTVERBAND

**Huidige toestand**

[Bv. Momentele zijn nog geen documenten aanwezig binnen het lokaal bestuur waarin verwezen wordt naar de taken en verantwoordelijkheden rond informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband.

Wel is er reeds een stappenplan aanwezig, waarbinnen de verschillende diensten - van personeelsdienst- tot IT en communicatie - wijzigingen doorvoeren in systemen en toepassingen. De inventarisatie van databanken en opslagplaatsen is momenteel onvolledig en de kans bestaat dan ook dat bepaalde toegangen niet opgezegd werden na uitdiensttreding.

Er is momenteel ook geen formele, uitgeschreven procedure aanwezig voor het toewijzen en intrekken van toegangen en rechten waardoor dit momentele voornamelijk ad hoc gebeurt. Een belangrijk aandachtspunt hierbij is dat bepaalde toegangen en rechten toegewezen worden door toeleveranciers. Ook hiervoor is momentele geen formule procedure aanwezig.]

**Concrete aanbevelingen**

[Bv. Maak werk van een uitgeschreven en formeel vastgelegde procedure voor de het in- en uitdiensttreden van lokale medewerkers, met daarin de belangrijkste aandachtspunten, de stappen die genomen moeten worden en wie verantwoordelijk is voor welke stappen. Denk hierbij aan het verwijderen van toegangsrechten binnen alle systemen en toepassingen wanneer een medewerker vertrekt.

Zoals reeds werd aangehaald onder sectie 1 ‘Risico’ dient de organisatie een inventaris aan te leggen waarin alle databanken en opslagplaatsen met gevoelige gegevens opgenomen worden, aangezien een correct toegangs- en rechtenbeheer cruciaal is om de veiligheid van deze gevoelige informatie te garanderen.

Naast een procedure voor in- en uitdiensttreding dient ook een procedure voor het toewijzen en intrekken van toegangen en rechten opgemaakt te worden, met daarin een duidelijke definiëring van verantwoordelijkheden. Dit houdt in dat vastgelegd dient te worden wie voor de aanwezige systemen en toepassingen toegangen en rechten verleent, wie deze bijhoudt in een register of document en wie de toegangen en rechten intrekt wanneer een medewerker de organisatie verlaat. Deze procedure kan in eerste instantie uitgewerkt worden voor de databanken en opslagplaatsen met gevoelige gegevens.

Gezien de complexiteit van de organisatie en het feit dat verschillende diensten zelf toegangen en rechten beheren voor medewerkers is het wenselijk om aan te sluiten op een Acess and Identity Management System die het beheren van toegangen en rechten vereenvoudigt. Hier kan gekeken worden naar het Toegangs- en Gebruikersbeheer van de Vlaamse Overheid (ACM-IDM).

**Normen van toepassing**

|  |  |  |
| --- | --- | --- |
| De aangehaalde aanbevelingen kaderen binnen onderstaande normen | | |
| A4.3.1 ISO 27002-7.3 | B4.3.1 ISO 27002-7.3 |  |
|  |  |  |
|  |  |  |

1. Bedrijfsmiddelen
   1. VERANTWOORDELIJKHEID VOOR BEDRIJFSMIDDELEN

**Huidige toestand**

[Bv. Er bestaat een inventaris van ICT-gerelateerde objecten, maar deze is tot op heden niet volledig uitgewerkt. De verschillende objecten en systemen hebben geen toegewezen beheerder en vaak wordt hierbij uitgegaan van een gedeelde verantwoordelijkheid door de ICT-dienst.

De meeste diensten en hun medewerkers werken met thin clients. Er is een beperkt aantal laptops aanwezig voor de ICT-dienst, brede organisatie en uitleendienst. De laptops van de uitleendienst bevatten geen gevoelige data.

Toegang tot gevoelige- of persoonsgegevens via laptops in kader van telewerk is enkel mogelijk met een beveiligde verbinding. Door het ontbreken van een sluitend toegang- en rechtenbeheer bestaat wel het risico dat ex-medewerkers nog toegang kunnen krijgen tot dergelijke informatie.]

**Te nemen maatregelen**

[Bv. Maak naast een inventaris van databanken en opslagplaatsen voor gevoelige gegevens ook werk van een inventaris dat alle IT-gerelateerde objecten oplijst en in kaart brengt, zodat vermeden wordt dat bepaalde systemen of toepassingen doorheen de tijd vergeten worden en zo veiligheidsrisico’s met zich meebrengen.

Wijs aan alle IT-gerelateerde objecten in het op te maken inventaris een verantwoordelijke beheerder toe die instaat voor het up-to-date houden en controleren van deze objecten. Indien de beheerder in kwestie een externe leverancier is dient men ook daar een verantwoordelijke contactpersoon toe te wijzen.

Zoals vermeld in punt 4 ‘Informatiebeveiliging’ moeten verantwoordelijkheden ook vastgelegd worden voor het beheer van toegangen en rechten. Men kan hieraan tegemoet komen door een formele, uitgeschreven procedure op te maken voor het verlenen en intrekken van toegangen en rechten.]

**Normen van toepassing**

|  |  |  |
| --- | --- | --- |
| De aangehaalde aanbevelingen kaderen binnen onderstaande normen | | |
| B5.1.1 ISO 27002-8.1 | B5.1.2 ISO 27002-8.1 | B5.1.3 ISO 27002-8.1 |
|  |  |  |

* 1. CLASSIFICATIE VAN INFORMATIE

**Huidige toestand**

[Bv. Het lokaal bestuur is bewust van de ernst die samengaat met het verwerken van persoonsgegevens, maar voorziet geen opdeling tussen anonieme gegevens, persoonsgegevens, gevoelige persoonsgegevens en gecodeerde al dan niet gevoelige persoonsgegevens in het informatieveiligheidsbeleid.

Dit onderscheid wordt tot op heden ook niet gecommuniceerd tijdens vormingsmomenten of de indiensttredingsprocedure.]

**Concrete aanbevelingen**

[Bv. Maak binnen het informatieveiligheidsbeleid een onderscheid tussen de vier types gegevens, met waar nodig afzonderlijke stappen en richtlijnen voor de verwerking en opslag van de verschillende types gegevens.

Neem het onderscheid tussen de vier types mee in geplande vormingsmomenten rond gegevensbeheer- en uitwisseling. Dit geldt ook voor de toelichting bij de indiensttreding van medewerkers die binnen hun functie in aanraking zullen komen met gevoelige- en/of persoonsgegevens.]

**Normen van toepassing**

|  |  |  |
| --- | --- | --- |
| De aangehaalde aanbevelingen kaderen binnen onderstaande normen | | |
| A5.1.1 ISO 27002-8.2 | B5.2.1 ISO 27002-8.2 | A5.1.2 ISO 27002-8.2 |
|  |  |  |
|  |  |  |

* 1. BEHANDELEN VAN MEDIA

**Huidige toestand**

[Bv. Globaal gezien worden verwijderbare media - zoals USB-sticks of externe harde schijven - zelden gebruikt binnen het lokaal bestuur. Dit houdt echter niet in dat personeelsleden niet gebruik maken van dergelijke media tijdens de diensturen, bijvoorbeeld omdat deze van thuis uit meegebracht worden. Dit kan een probleem vormen indien deze onvoldoende beveiligd zijn (bv. met cryptografische methodes) en ook gebruikt worden voor de opslag van gevoelige of persoonsgegevens.

Op de meeste thin clients zijn de USB-toegangen geblokkeerd, het is de ICT-dienst die hierover beslist. Bovendien worden USB-sticks, indien toegang, steeds onmiddellijk gescand op virussen en malware.

Het gebruik en behandelen van media maakt geen deel uit van bestaande trainingen, vormingsmomenten en andere sensibiliseringsacties.]

**Concrete aanbevelingen**

[Bv. Zorg ervoor dat bij de indiensttreding van medewerkers reeds gecommuniceerd wordt over de vormingsmomenten rond informatiebeveiliging en goede praktijken inzake mediagebruik. Geef ook duidelijk aan dat eigen media niet gebruikt mogen worden voor de opslag van gevoelige informatie en dat deze media niet aangesloten mogen worden op apparatuur van de organisatie.

Verwerk de richtlijnen voor het gebruik van verwijderbare media in het arbeidsreglement en/of de deontologische code, zodat de gemaakte afspraken binnen de organisatie formeel vastgelegd zijn.

Voorzie binnen de uitleendienst van de organisatie in een beperkt aantal verwijderbare media waarvan medewerkers gebruik kunnen maken voor de opslag of verzending van gevoelige gegevens. Deze verwijderbare media moeten beschermd worden door encryptietools die de gegevens versleutelen.

**Normen van toepassing**

|  |  |  |
| --- | --- | --- |
| De aangehaalde aanbevelingen kaderen binnen onderstaande normen | | |
| A5.2.1 ISO 27002-8.3 | B5.3.1 ISO 27002-8.3 | A5.2.2 ISO 27002-8.3 |
| B5.3.2 ISO 27002-8.3 | A5.2.3 ISO27002-8.3 |  |
|  |  |  |

1. Toegang tot persoonsgegevens
   1. EISEN VOOR TOEGANGSBEVEILIGING

**Huidige toestand**

[Bv. Toegangsrechten tot verschillende toepassingen zitten heel verspreid binnen de organisatie, dit geldt ook voor het verstrekken van toegangen en rechten.

Enkele voorbeelden bij het toekennen van toegangsrechten tot verschillende toepassingen:

* VTE portaal Sociale Zekerheid: **xxx**
* VTE MAGDA-platform: **xxx**
* Toegang strafregister: Extern **xxx**
* Toegang rijksregister: Extern **xxx**

In de praktijk verloopt dit proces vrij efficiënt, maar er is geen overkoepelende procedure die de stappen vastlegt voor het toekennen en verwijderen. Diensten hanteren wel bepaalde principes en processen, maar deze zijn niet uitgeschreven en gelden niet voor de volledige organisatie.]

**Concrete aanbevelingen**

De aanbevelingen onder punt 4 ‘Informatiebeveiliging - meer bepaald het opmaken van een formele procedure voor toegang- en rechtenbeheer en het aansluiten op een Identity and Access Management System - komen tegemoet aan de vermelde uitdagingen.

**Normen van toepassing**

|  |  |  |
| --- | --- | --- |
| De aangehaalde aanbevelingen kaderen binnen onderstaande normen | | |
| A6.1.1 ISO 27002-9.1 | B6.1.1 ISO 27002-9.1 | A6.1.2 ISO 27002-9.1 |
| B6.1.2 ISO 27002-9.1 |  |  |
|  |  |  |

* 1. VERANTWOORDELIJKE VOOR TOEGANGSRECHTEN VAN GEBRUIKERS

**Huidige toestand**

[Bv. Tot op heden werd binnen het lokaal bestuur geen verantwoordelijke aangeduid voor het beheer van de aanvragen voor de toegang tot persoonsgegevens. Aanvragen worden in realiteit vaak door medewerkers of hun diensthoofden verstuurd naar de ICT-dienst, die dan gevolg geven aan de concrete vraag, al dan niet na bijkomende afstemming.

Aangezien het toegang- en rechtenbeheer verspreid in de organisatie zit, kan men logischerwijze moeilijk duiden welke medewerkers tot welke toepassingen hebben of nodig hebben.

Er is geen concrete contactpersoon bij \*naam toeleverancier\* voor het aanvragen, goedkeuren of intrekken van toegangsrechten in de door hen beheerde toepassingen en systemen.]

**Concrete aanbevelingen**

[Bv. Om ervoor te zorgen dat het toegang- en rechtenbeheer binnen de organisatie op gecoördineerde wijze verloopt neemt men binnen de op te maken procedure op dat aanvragen voor toegangen en rechten steeds via de diensthoofden verlopen. Van de diensthoofden wordt verwacht dat zij binnen een centraal beheerde database de toegekende toegangen en rechten bijhouden en consequent de ICT-dienst betrekken wanneer wijzigingen doorgevoerd dienen te worden, zoals het vertrek van een medewerker.

Aangezien ook externe partners en leveranciers systemen en toepassingen beheren waar medewerkers toegangen en rechten toegekend krijgen dient ook in dergelijke situaties een contactpersoon bepaald worden die instaat voor het beheer van de toegangen en rechten. Deze afspraken moeten formeel vastgelegd worden in contracten en Service Level Agreements.

**Normen van toepassing**

|  |  |  |
| --- | --- | --- |
| De aangehaalde aanbevelingen kaderen binnen onderstaande normen | | |
| A6.2.1 ISO 27002-9.2 |  |  |
|  |  |  |
|  |  |  |

* 1. VERANTWOORDELIJKHEDEN VAN GEBRUIKERS

**Huidige toestand**

[Bv. Er is een policy rond wachtwoordgebruik aanwezig, maar deze werd nog niet uitgeschreven op papier. De policy vereist een mix van kleine letters, hoofdletters, cijfers en speciale tekens en gaat uit van een minimumlengte van 6 karakters. De mix van tekens is een positieve zaak, maar een minimumlengte van 6 karakters komt niet tegemoet aan courante aanbevelingen inzake sterke wachtwoorden. Om de 180 dagen worden op serverniveau medewerkers verplicht om hun wachtwoord te wijzigen. Hierbij morgen de laatste 5 wachtwoorden niet gebruikt worden. De policy wordt echter niet consequent afgedwongen voor alle systemen en toepassingen - bepaalde toepassingen bieden deze optie ook niet - waardoor sensibilisering nog steeds nodig is.

Elk personeelslid heeft een eigen account om in te loggen op het netwerk, maar er zijn ook toepassingen binnen de organisatie waarbij een dienst gebruik maakt van een gedeelde login om zo extra kosten uit te sparen. Het gaat hierbij wel over toepassingen die een gering risico inhouden voor de informatieveiligheid.

Wanneer medewerkers hun bureau voor enkele minuten verlaten, wordt de computer niet consequent vergrendeld. De aanwezige thin clients gaan na 1 uur inactiviteit in slaapmodus, maar dit biedt voldoende tijd en ruimte om zonder autorisatie gebruik te maken van de clients.

De organisatie maakt geen gebruik van een wachtwoordkluis die ervoor kan zorgen dat alle systemen en toepassingen - ook wanneer de mogelijkheid niet bestaat om een wachtwoordpolicy af te dwingen - beveiligd worden met een sterk, complex wachtwoord.

**Concrete aanbevelingen**

[Bv. Pas het wachtwoordbeleid aan zodat wachtwoorden minimaal 12 tekens moeten bedragen. In combinatie met een mix van letters, hoofdletters, cijfers en speciale tekens kan het kraken van wachtwoorden zo bemoeilijkt worden.

Ga voor alle systemen en toepassingen binnen de organisatie na of het geldend wachtwoordbeleid automatisch afgedwongen kan worden, zodat medewerkers niet de kans hebben om het beleid niet te volgen.

Indien het wachtwoordbeleid niet voor alle systemen en toepassingen afgedwongen kan worden, dient minstens jaarlijks een sensibiliseringsactie opgezet te worden rond goede praktijken voor medewerkers, zoals het instellen van wachtwoorden en het vergrendelen van de werkcomputer wanneer men even het bureau verlaat.

Voor systemen en toepassingen waar het wachtwoordbeleid niet afgedwongen kan worden, koopt de organisatie best een wachtwoordkluis aan. Een dergelijke kluis houdt alle accounts en bijhorende wachtwoorden bij en kan geopend worden via één sterk wachtwoord - wat als voordeel heeft dat medewerkers slechts een wachtwoord dienen te onthouden - en kan in bepaalde gevallen zelfs extra beveiligd worden met Multi-Factor-Authenticatie.

**Normen van toepassing**

|  |  |  |
| --- | --- | --- |
| De aangehaalde aanbevelingen kaderen binnen onderstaande normen | | |
| A6.3.1 ISO 27002-9.3 |  |  |
|  |  |  |
|  |  |  |

* 1. TOEGANGSBEVEILIGING VAN SYSTEMEN EN TOEPASSINGEN

**Huidige toestand**

[Bv. De gepaste beveiligingsmaatregelen om toegang tot persoonsgegevens te beperken werden reeds uitvoerig besproken in dit veiligheidsplan. Daarbij dienen ook enkele maatregelen vermeld te worden die op dit ogenblik ontbreken, ondanks dat deze een belangrijk impact op de lokale informatiebeveiliging kunnen hebben.

Hierbij gaat het onder andere over:

* Het ontbreken van een sluitende procedure voor het beheer van toegangen en rechten, met aandacht voor de bijhorende rollen en verantwoordelijkheden.
* De afwezigheid van multi-factor-authenticatie, zeker voor systemen en toepassingen die gevoelige- of persoonsgegevens bevatten of essentieel zijn voor de werking en dienstverlening van het lokaal bestuur
* Het gebrek aan afspraken met toeleveranciers rond toegang- en rechtenbeer voor de systemen en toepassingen die zij beheren
* …

De personeelsleden beschikken zelf niet over administratorrechten op hun pc’s, waardoor zij niet de mogelijkheid hebben om zelf nieuwe toepassingen te installeren of netwerk- en systeemparameters te wijzigen.

Gedeelde logins zijn aanwezig, maar enkel voor toepassingen en systemen die een gering risico voor de informatieveiligheid of werking van het lokaal bestuur inhouden.

Toegangen en rechten worden aangevraagd bij de diensthoofden of personeelsdienst, die deze aanvragen op hun beurt opnemen met de ICT-dienst. De ICT-dienst zorgt er dan voor dat de gevraagde toekenningen, wijzigingen of intrekkingen gebeuren. Momenteel bestaat er echter geen overzicht van alle verleende toegangen en rechten bij de verschillende diensten.

Momenteel is er één publieke schijf aanwezig waar elke medewerker gegevens of documenten kan toevoegen of raadplegen. Normaliter gaat het hier niet over gevoelige- of persoonsgegevens.

De organisatie maakt geen gebruik van een Identity en Access Management System om het toekennen of intrekken van toegangen en rechten te faciliteren.

Uit een informatieveiligheidsaudit in 2018 bleek dat vele IT-gerelateerde objecten zoals routers, switches en printers beveiligd waren met standaardlogins die makkelijk geraden kunnen worden door hackers.

**Concrete aanbevelingen**

[Bv. Zoals eerder vermeld moet de organisatie prioritair werk maken van een sluitende procedure voor toegang- en rechtenbeheer, waarbij de verantwoordelijkheid voor het bijhouden van verleende toegangen en rechten bij diensthoofden ligt. Dit proces kan gefaciliteerd worden door een Access and Identity Management System, zoals het toegang- en rechtenbeheer van de Vlaamse Overheid.

Voorzie waar mogelijk in Multi-Factor-Authenticatie (MFA) om toegangen extra te beveiligen, zeker wanneer het gaat over databanken of opslagplaatsen voor gevoelige informatie of systemen en toepassingen die van kritiek belang zijn voor de dienstverlening van de organisatie. Binnen het toegang- en rechtenbeheer van de Vlaamse Overheid werden mogelijkheden voorzien voor MFA.

Jaarlijks dient gecontroleerd te worden of er geen standaardwachtwoorden aanwezig zijn op de IT-gerelateerde objecten binnen de organisatie, zoals routers, switches, printers en andere apparaten. Bij installatie wordt vaak een eenvoudig standaardwachtwoord voorzien, dat zo snel mogelijk aangepast dient te worden door de organisatie. In realiteit wordt dit echter al eens vergeten, wat het werk van hackers vergemakkelijkt. Het controleren van standaardwachtwoorden kan gelegd worden bij de verantwoordelijken voor de verschillende IT-gerelateerde objecten, zoals vastgelegd in het op te maken inventaris (Cfr. De aanbevelingen onder punt 5.1 ‘Verantwoordelijkheid voor beleidsmiddelen).]

**Normen van toepassing**

|  |  |  |
| --- | --- | --- |
| De aangehaalde aanbevelingen kaderen binnen onderstaande normen | | |
| A6.4.1 ISO 27002-9.4 | B6.4.1 ISO 27002-9.4 | A6.4.2 ISO 27002-9.4 |
| B6.4.2 ISO 27002-9.4 | A6.4.3 ISO 27002-9.4 | B6.4.3 ISO 27002-9.4 |
| B6.4.4 ISO 27002-9.4 | B6.4.5 ISO 27002-9.4 | B6.4.6 ISO 27002-9.4 |
| B6.4.7 ISO 27002-9.4 | B6.4.8 ISO 27002-9.4 |  |

1. Cryptografie
   1. CRYPTOGRAFISCHE BEHEERSMAATREGELEN

**Huidige toestand**

Er wordt momenteel nog geen gebruik gemaakt van cryptografie, ook niet voor de opslag of het versturen van gevoelige- of persoonsgegevens over het internet. Dit houdt risico’s in, aangezien versleuteling een extra garantie biedt dat deze gegevens niet geraadpleegd of gemanipuleerd kunnen worden door onbevoegden.

Op dit moment beschikt het lokaal bestuur nog niet over verwijderbare media, zoals USB’s of externe harde schijven - die beveiligd zijn met cryptografische methodes.

**Concrete aanbevelingen**

[Bv. Onderzoek de mogelijkheden om gevoelige informatie en persoonsgegevens te versleutelen alvorens deze opgeslagen worden, **XXX** kan een interessante tool zijn om de aanbeveling in de praktijk te brengen.

Onderzoek daarnaast ook de mogelijkheid om gevoelige informatie en gegevens te versleutelen alvorens deze worden via het internet of andere minder beveiligde verbindingen. Ook hier kan **XXX** een meerwaarde bieden.

Schaf in kader van de aanbevelingen onder punt 5.2 ‘Media’ een beperkte hoeveelheid verwijderbare media aan die gegevens versleutelen zodat deze niet misbruik of onderschept kunnen worden.

**Normen van toepassing**

|  |  |  |
| --- | --- | --- |
| De aangehaalde aanbevelingen kaderen binnen onderstaande normen | | |
| A7.1.1 ISO 27002-10.1 | B7.1.1 ISO 27002-10.1 | A7.1.2 ISO 27002-10-1 |
| B7.1.2 ISO 27002-10.1 |  |  |
|  |  |  |

1. Fysieke beveiliging  
   1. BEVEILIGING VAN DE OMGEVING

**Huidige toestand**

[Bv. Er is zowel een ingang voor het publiek als voor personeel aanwezig in het gebouw. Het personeel beschikt over een sleutel om zich toegang te verschaffen. Het gaat hierbij niet over een veiligheidssleutel, waardoor het mogelijk is om kopieën bij te maken.

De publieke ingang is enkel geopend tijdens de openingsuren en wordt geopend of gesloten door de onthaalmedewerkers. Tijdens de openingsuren is iedere voormiddag van 8:30 tot 12:00 en elke namiddag van 13:00 tot 17:00 minstens één onthaalbediende aan de balie aanwezig die alle bezoekers opvangt en doorverwijst naar de juiste medewerker.

Er is een alarm aanwezig in het gebouw, met een code voor alle personeelsleden. Deze code is al even niet meer gewijzigd, en is dus vermoedelijk nog gekend bij ex-werknemers. Het alarm wordt niet automatisch geactiveerd indien men deze vergeet aan te zetten. Er is geen formele afsluitprocedure aanwezig, al is tijdens externe vergaderingen wel steeds een personeelslid aanwezig.

Burelen worden niet op slot gedaan, maar sommige kasten wel. Gevoelige of persoonsgegevens worden standaard achter slot en grendel bewaard.

Er is een sleutelplan aanwezig dat wordt beheerd door de personeelsdienst voor de buitendeur, en bij in- en uitdiensttreding. Andere sleutels worden bewaard in een ‘kluis’ bij de dienst bevolking. Personeelsleden handtekenen een document bij ontvangst van sleutel(s) en krijgen ook een bewijs bij teruggave. Deze documenten worden bewaard in het persoonlijk dossier.

In de verschillende gebouwen zijn op de belangrijkste plaatsen brandblussers voorhanden om beginnende brandhaarden te bestrijden. Het gebouw is uitgerust met automatische branddetectoren die frequent getest worden, brandmeldknoppen, muurhaspels, snelblussers en er is een brandalarmcentrale. Dit is cruciaal om zelfs na kantooruren snel en gevat te kunnen reageren en een eventuele brand onder controle te krijgen. Er is in het gebouw zowel noodsignalisatie als noodverlichting aanwezig. Een evacuatieoefening is tot op heden echter nog niet doorgegaan. In de buurt van de serverlokalen zijn CO²-blusapparaten aanwezig. In het serverlokaal is er bovendien ook een branddetector aanwezig.]

**Concrete aanbevelingen**

[Bv. Laat personeelsleden hun bureau afsluiten wanneer zij deze verlaten. Ook afsluitbare kasten dienen elke avond op slot te zijn. Voorzie signalisatie om medewerkers hier aan te herinneren.

Documenten met vertrouwelijke gegevens mogen uitsluitend in afsluitbare kasten en lokalen bewaard worden. Daarnaast is het wenselijk om een ‘clean desk policy’ in te voeren waarbij medewerkers geen documenten laten rondslingeren op hun bureaus, aan kopieermachines en andere gekende locaties. Zorg ook dat er signalisatie aanwezig is op deze locaties om de policy onder de aandacht van medewerkers te brengen.

Het sleutelplan dient te allen tijde actueel te zijn. Waar medewerkers nu enkel een bewijs van ontvangst tekenen kan het nuttig zijn om hen ook een bewijs te laten ondertekenen bij teruggave, om de opvolging te faciliteren.

De sleutels voor de buitendeuren worden best vervangen door veiligheidssleutels die niet zomaar bijgemaakt kunnen worden. Daarnaast zou elke medewerker ook een unieke code voor het alarm moeten krijgen, om te vermijden dat ex-medewerkers zich nog toegang kunnen verschaffen.

Jaarlijks dient de organisatie een evacuatie-oefening uit te voeren zodat medewerkers de te volgen richtlijnen kennen en in de praktijk kunnen brengen. Het is ook aangeraden om in sensibilisering te voorzien via posters en/of mails.]

**Normen van toepassing**

|  |  |  |
| --- | --- | --- |
| De aangehaalde aanbevelingen kaderen binnen onderstaande normen | | |
| A8.1.1 ISO 27002-11.1 | B8.1.1 ISO 27002-11.1 | A8.1.2 ISO 27002-11.1 |
| B8.1.2 ISO 27002-11.1 |  |  |
|  |  |  |

* 1. BEVEILIGDE APPARATUUR

**Huidige toestand**

[Bv. Het serverlokaal bevindt zich in de kelder van het gebouw en kan ook afgesloten worden. In de praktijk wordt echter al eens vergeten om de deur op slot te doen. Er is ook een noodstroomvoorziening voorzien in het serverlokaal die voldoende stroom levert om een server en/of randapparatuur gedurende een uur te voeden. De noodstroomvoorziening wordt wel niet op geregeld basis getest.

In het serverlokaal is een airco-installatie aanwezig waardoor de temperatuur in het lokaal niet te hoog kan oplopen. Het risico op wateroverlast is beperkt en de elektronische apparatuur staat ook op een verhoog om de kans op schade verder te verkleinen.

Bedrijfsmiddelen worden in principe correct afgevoerd, wat inhoudt dat ze veilig geformatteerd, verwijderd en meestal ook vernietigd worden.]

**Concrete aanbevelingen**

[Bv. Signalisatie op de deuren van serverlokalen die medewerkers eraan herinnert om de deuren steeds af te sluiten is aangeraden. Zo wordt vermeden dat onbevoegden zomaar kunnen binnentreden en schade berokkenen.

Gezien het belang van een goed functionerende stroomvoorziening in geval van een cyberaanval of ander IT-gerelateerde incidenten dient jaarlijks gecontroleerd te worden of de noodstroomvoorziening naar behoren werkt.

Werk een beknopt maar helder afvoerbeleid uit dat stipuleert dat alle apparatuur met opslagmedia gecontroleerd moet worden bij verwijdering of hergebruik, om er zo op toe te zien dat gevoelige informatie en persoonsgegevens veilig overschreven of verwijderd zijn.]

**Normen van toepassing**

|  |  |  |
| --- | --- | --- |
| De aangehaalde aanbevelingen kaderen binnen onderstaande normen | | |
| A8.2.1 ISO 27002-11.2 | B8.2.1 ISO 27002-11.2 | A8.2.2 ISO 27002-11.2 |
| B8.2.2 ISO 27002-11.2 |  |  |
|  |  |  |

1. Operationele beveiliging
   1. OPERATIONELE PROCEDURES EN VERANTWOORDELIJKHEDEN

**Huidige toestand**

[Bv. De gepaste wijze met met veranderingen in organisatie, bedrijfsprocessen en informatieverwerkende faciliteiten en systemen om te gaan werd reeds aangehaald in eerdere aanbevelingen, zoals het uitwerken van een sluitende procedure voor het toekennen en intrekken van gebruikers- en toegangsrechten en het aanduiden van verantwoordelijke medewerkers.

Daarnaast is het van belang dat de personeelsleden de nodige opleidingen krijgen voor de softwaretoepassingen waar zij gebruik van maken in kader van hun werkzaamheden. Binnen het lokaal bestuur wordt hierin voorzien via on-the-job training met opleiding door softwareleveranciers waar mogelijk. De handleidingen en bedieningsprocedures staan ter beschikking van het personeel via het intranet.]

**Concrete aanbevelingen**

[Bv. Voorzie waar mogelijk in jaarlijkse opleidingen of vormingsmomenten voor personeelsleden rond onderdelen die een invloed hebben op de lokale informatiebeveiliging, zoals de organisatie-inrichting, bedrijfsprocessen en gebruikte systemen en toepassingen.

Bouw de nodige functiescheidingen in zodat één enkele persoon nooit de exclusieve controle verwerft over een verwerking van persoonsgegevens. De uitwerking van een centrale database met toegangen en rechten kan hierbij helpen.]

**Normen van toepassing**

|  |  |  |
| --- | --- | --- |
| De aangehaalde aanbevelingen kaderen binnen onderstaande normen | | |
| A9.1.1 ISO 27002-12.1 | B9.1.1 ISO 27002-12.1 | A9.1.2 ISO 27002-12.1 |
| B9.1.2 ISO 27002-12.1 |  |  |
|  |  |  |

* 1. BESCHERMING TEGEN MALWARE

**Huidige toestand**

[Het lokaal bestuur werkt op netwerkniveau met \*naam software\*. Deze wordt centraal beheerd, met een client op elk toestel. E-mails worden gescand en beveiligd via \*naam software\*.

De antivirus software wordt automatisch geactualiseerd, en kan niet worden uitgeschakeld door de gebruiker. Externe apparatuur die wordt aangesloten, zoals USB’s en externe harde schrijven, worden automatisch gescand op de aanwezigheid van malware.

Personeelsleden hebben geen administrator rechten op hun PC’s, uitgezonderd de laptops die door de ICT-dienst gebruikt worden.

Er worden nu en dan mails rondgestuurd door de ICT-dienst met richtlijnen ter bescherming tegen malware, maar dit gebeurt niet via een vaste frequentie. De automatische mailfiltering slaagt erin 80% van de spamberichten uit de inbox van medewerkers te houden.

Er zijn nog 5 computers aanwezig die draaien op het Windows 2008 besturingssysteem en dus niet langer ondersteund worden. Deze beschikken wel over een aparte internetverbinding, waardoor het gaat over een geïsoleerd veiligheidsrisico.

Een uitgewerkt patchingproces voor het actualiseren van systemen en toepassingen werd nog niet opgemaakt. Doordat er geen volledig uitgewerkt inventaris is met IT-gerelateerde objecten is het moeilijk om na te gaan welke systemen en toepassingen de nodige aandacht moeten krijgen.]

**Concrete aanbevelingen**

[Bv. Antivirus en antispyware-applicaties die voorkomen dat systemen en toepassingen het slachtoffer worden van gerichte aanvallen of uitgelezen worden moeten op regelmatige basis geüpdatet worden, zodat nieuwe(re) virusdefinities ook opgenomen zijn en deze nieuwe dreigingen ook gedetecteerd kunnen worden.

Zorg voor een uitgeschreven patchingproces voor de aanwezige systemen en toepassingen binnen de organisatie, die definieert binnen welke frequentie de systemen en toepassingen geüpdatet dienen te worden en welke medewerker of externe contactpersoon hiervoor verantwoordelijk is. Het patchingproces kan geïntegreerd worden in het op te maken inventaris van IT-gerelateerde objecten.]

**Normen van toepassing**

|  |  |  |
| --- | --- | --- |
| De aangehaalde aanbevelingen kaderen binnen onderstaande normen | | |
| A9.2.1 ISO 27002-12.2 | B9.2.1 ISO 27002-12.2 |  |
|  |  |  |
|  |  |  |
|  |  |  |

* 1. BACK-UP

**Huidige toestand**

[Bv. Backups worden bewaard in het administratief centrum op \*adres\*. Voor de toepassing \*naam software\* neemt firma \*naam leverancier\* zelf ook regelmatig back-ups.

Een uitgeschreven procedure of back-up en herstelplan werd tot op heden niet uitgewerkt. Back-ups worden gecontroleerd door de ICT-dienst, om te kijken of deze al dan niet bruikbaar zijn. In geval van afwezigheid van de ICT-dienst, volgt \*naam medewerker\* dit proces op. Om deze reden heeft \*naam medewerker\* ook toegang tot de mailbox van de ICT-dienst. Voor het lokaal bestuur worden er dagdagelijks volledige back-ups genomen.

Er zijn standaard onderhoudscontracten aanwezig met \*naam leverancier\*, die in geval van panne, herstel garanderen binnen een beperkt aantal uren.

Restores worden niet systematisch getest, wel worden nu en dan bestanden teruggezet als ad-hoc test.]

**Concrete aanbevelingen**

[Bv. Back-ups dienen jaarlijks gecontroleerd te worden op het feit of ze naar behoren functioneren en daadwerkelijk de gewenste informatie bevatten. Dit kan verrassingen voorkomen wanneer de back-ups nodig zijn om de dienstverlening deels of volledig opnieuw te starten.

Het is wenselijk om een gedragen back-up en herstelplan op te maken, aangezien back-ups essentieel zijn bij een storing, panne of aanval om zo snel mogelijk terug aan de slag te gaan met zo weinig mogelijk data- en tijdsverlies. Het plan dient de nodige maatregelen te bevatten voor de vertrouwelijkheid, integriteit en toegankelijkheid van de back-upgegevens, maar ook praktische aspecten als de bewaartijd en frequentie van testen.

Het is sterk aangeraden om back-ups redundant - op meerdere serverlocaties - op te slaan. Door de back-ups zowel lokaal als extern te bewaren kan gegevensverlies bij problemen vermeden worden.]

**Normen van toepassing**

|  |  |  |
| --- | --- | --- |
| De aangehaalde aanbevelingen kaderen binnen onderstaande normen | | |
| A9.3.1 ISO 27002-12.3 | B9.3.1 ISO 27002-12.3 | B9.3.2 ISO 27002-12.3 |
|  |  |  |
|  |  |  |

* 1. MONITORING

**Huidige toestand**

[Loggings voor het gebruik en de verwerking van persoonsgegevens zitten in principe vervat in de softwaretoepassingen die gebruikt worden om de verschillende databanken te consulteren. Zoals aangehaald werd in voorgaande aanbevelingen is het inventaris van databanken en opslagplaatsen nog niet volledig up-tot-date, wat een negatieve impact heeft op de vereiste controle en monitoring.]

**Concrete aanbevelingen**

[Bv. Zoals eerder werd vermeld is het belangrijk om het bestaande inventaris van databanken en opslagplaatsen voor gevoelige gegevens bij te werken door ontbrekende databanken en opslagplaatsen in kaart te brengen en toe te voegen, zodat deze niet over het hoofd worden gezien bij reguliere monitoring.

Voor elke databank moet in kaart gebracht worden op welke manier het gebruik en de verwerking van persoonsgegevens gelogd - een vorm van inventarisatie - en opgevraagd kan worden.

In kader van de monitoringactiviteiten is het belangrijk dat gebruikers van databanken met persoonsgegevens steeds een unieke login hebben, zodat altijd duidelijk is welke medewerker gekoppeld kan worden aan een specifiek gebruik of verwerking van persoonsgegevens.]

**Normen van toepassing**

|  |  |  |
| --- | --- | --- |
| De aangehaalde aanbevelingen kaderen binnen onderstaande normen | | |
| B9.4.1 ISO 27002-12.4 | B9.4.2 ISO 27002-12.4 | B9.4.3 ISO 27002-12.4 |
|  |  |  |
|  |  |  |

* 1. OVERWEGINGEN BIJ AUDITS VAN INFORMATIESYSTEMEN

**Huidige toestand**

[Bv. In het verleden heeft de organisatie nog geen audits gehad. Wel zijn er plannen om in te tekenen op de ICT-veiligheidsaudits met cofianciering via Audit Vlaanderen.]

**Concrete aanbevelingen**

[Bv. Maak een standaard vertrouwelijkheidsclausule op voor externe partijen, die ondertekend dient te worden bij de aanvang van een audit, pentesting door ethisch hackers of private partners of andere gerelateerde activiteiten. Deze clausule dient goedgekeurd te worden door de integrale organisatie, alvorens deze in gebruik te nemen.]

**Normen van toepassing**

|  |  |  |
| --- | --- | --- |
| De aangehaalde aanbevelingen kaderen binnen onderstaande normen | | |
| B9.5.1 ISO 27002-12.7 |  |  |
|  |  |  |
|  |  |  |

1. Communicatiebeveiliging
   1. NETWERKBEVEILIGING

**Huidige toestand**

[Bv. De ICT-dienst zorgt voor een gepaste controle en beheer van de netwerken, opdat deze beveiligd zijn tegen bedreigingen. Daarnaast wordt ook toegezien op de beveiliging van de systemen en toepassingen binnen het netwerk. tevens voor een afdoende beveiliging van de systemen en toepassingen die het netwerk gebruiken. De concrete maatregelen die hierrond genomen werden, zijn onder andere aan bod komen in het hoofdstuk rond operationele beveiliging.

Daarnaast werden ook de nodige maatregelen getroffen om de hoogst mogelijke beschikbaarheid voor de verbinding met het netwerk te waarborgen, zodat de toegankelijkheid van beschikbare en geraadpleegde gegevens niet binnen het gedrang komt. Binnen de ICT-dienst is een permanentieregeling van toepassing tijdens de openingsuren van de organisatie.

Er is een netwerkschema aanwezig waarbinnen de verschillenden verbindingen met alle buitendiensten van het lokaal bestuur in kaart worden gebracht. Dit schema is in het bezit van de gemeentelijke ICT-dienst en zij staan ook in voor het actualiseren hiervan. De verbindingen met de buitendiensten worden op gepaste wijze beveiligd.

Wifi-toegang wordt door het lokaal bestuur alleen aangeboden voor eigen personeel en schepenen, maar occasioneel ook voor externe medewerkers, met een beveiligd wachtwoord.

Er is ook een VPN verbinding aanwezig tussen de gebouwen van de politiezone op \*adres voorziening\* en het lokaal bestuur, om samenwerking mogelijk te maken via \*naam software\*.

Momenteel wordt werk gemaakt van een samenwerking met het OCWM, waardoor het belangrijk wordt om met VLAN’s te werken die een logische scheiding binnen het netwerk creëren. Gezien de eerder beperkte netwerksegmentatie en segregatie van het lokaal bestuur kan dit moment aangegrepen worden om de opdeling verder uit te breiden en monitoren, wat de informatieveiligheid ten goede komt.]

**Concrete aanbevelingen**

[Bv. Onderzoek de mogelijkheden om penetratietesten te laten uitvoeren op het netwerk waar een private organisatie of ethische hackers op zoek gaan naar zwakke plekken in het netwerk. De aankoop van een netwerk scanner software kan een waardevol alternatief of een nuttige combinatie vormen. De ICT-veiligheidsaudits met cofinanciering via Audit Vlaanderen kunnen hierin een eerste stap zijn.

Zorg dat het reeds aanwezig netwerkschema te allen tijde up-to-date is. Zorg ervoor dat hiervoor ook een duidelijke eindverantwoordelijke is aangewezen is binnen de bevoegde ICT-dienst.

Voor de geplande samenwerking tussen het lokaal bestuur en OCMW is het van belang om op netwerkniveau een fysieke of logische scheiding te voorzien tussen beide organisaties, zodat elke gebruiker enkel toegang heeft tot de middelen uit dienst organisatie. Onderzoek voorafgaand aan de integratie hoe deze evolutie kan aangegrepen worden om het netwerk verder te segmenteren en segregeren, ten voordele van de veiligheid.

Zorg ervoor dat de verbindingen met de buitendiensten op een gepaste manier beveiligd zijn. Dit kan door te voorzien in een virtuele directe lijn tussen de verschillende plaatsen, een draadloze verbinding te installeren die voldoet aan de geldende richtlijnen of een VPN-verbinding aan te leggen tussen de verschillende sites via het internet.]

**Normen van toepassing**

|  |  |  |
| --- | --- | --- |
| De aangehaalde aanbevelingen kaderen binnen onderstaande normen | | |
| A10.1.1 ISO 27002-13.1 | B10.1.1 ISO 27002-13.1 | B10.1.2 ISO 27002-13.1 |
| B10.1.3 ISO 27002-13.1 | B10.1.4 ISO 27002-13.1 | B10.1.5 ISO 27002-13.1 |
|  |  |  |

* 1. INFORMATIETRANSPORT

**Huidige toestand**

[Bv. Er is nog geen arbeidsreglement aanwezig met een passage omtrent het gebruik van elektronische informatie- en communicatiemiddelen. Alle vaste personeelsleden die nu in dienst zijn hebben een deontologische code voor akkoord ondertekend, maar dit geldt niet voor het arbeidsreglement.

Er worden geen dossiers of systemen met persoonsgegevens gedeeld tussen het lokaal bestuur en OCMW. Het OCMW heeft eigen virtuele servers, een aparte \*naam\* server en een aparte applicatieserver. Wel wordt gebruik gemaakt van dezelfde mailserver, maar ook hiervoor worden back-ups gescheiden.

**Concrete aanbevelingen**

[Bv. Voeg aan het arbeidsreglement een clausule toe voor het gebruik van elektronische informatie- en communicatiemiddelen. Zoals aangehaald onder punt 4.2 ‘informatiebeveiliging tijdens het dienstverband’ is het ook wenselijk om het arbeidsreglement ook ter ondertekening voor te leggen, zoals nu reeds het geval is voor de deontologische code.

Voorzie in een tweejaarlijkse evaluatie en bijsturing van het arbeidsreglement en de deontologische code.

Vraag machtiging aan bij de Vlaamse Toezichtcommissie voor het elektronisch meedelen van persoonsgegevens met het Autonoom Gemeentebedrijf.]

**Normen van toepassing**

|  |  |  |
| --- | --- | --- |
| De aangehaalde aanbevelingen kaderen binnen onderstaande normen | | |
| A10.2.1 ISO 27002-13.2 | A10.2.2 ISO 27002-13.2 | A10.2.3 ISO 27002-13.2 |
| B10.2.3 ISO 27002-13.2 |  |  |
|  |  |  |

1. Aanschaffen, ontwikkelen en onderhouden van informatiesystemen
   1. BEVEILIGINGSEISEN VOOR INFORMATIESYSTEMEN

**Huidige toestand**

[Momenteel worden geen informatiesystemen ontwikkeld door het lokaal bestuur. Hiervoor wordt samengewerkt met externe partners. Er is geen vaste, uitgeschreven procedure aanwezig voor de beveiligingsvereisten bij de ontwikkeling van of wijzigingen aan informatiesystemen.]

**Concrete aanbevelingen**

[Bv. Wanneer de organisatie besluit om over te gaan tot de ontwikkeling, aanschaf of wijziging van eigen systemen dienen steeds maatregelen genomen te worden om de veiligheid te garanderen op applicatieniveau en eventuele veiligheidsinbreuken te vermijden.

De veiligheidsconsulent moet steeds geraadpleegd worden bij de aanschaf, ontwikkeling of wijziging van nieuwe informatiesystemen, zodat voorafgaand een advies geformuleerd kan worden dat mee richting geeft aan de beslissingen.

Voer steeds een risicoanalyse uit wanneer een soort verwerking, in bijzonder een verwerking waarbij nieuwe technologieën gebruikt worden, een hoog risico kan hebben voor de rechten en vrijheden van natuurlijke personen.]

**Normen van toepassing**

|  |  |  |
| --- | --- | --- |
| De aangehaalde aanbevelingen kaderen binnen onderstaande normen | | |
| A11.1.1 ISO 27002-14.1 | B11.1.1 ISO 27002-14.1 |  |
|  |  |  |
|  |  |  |

* 1. BEVEILIGING IN ONTWIKKELINGS- EN ONDERSTEUNINGSPROCESSEN

**Huidige toestand**

[Bv. Momenteel is het niet zo dat vooraleer nieuwe of belangrijke evoluties van bestaande systemen in productie worden genomen, de projectverantwoordelijke consequent nagaat of aan de veiligheidsvereisten voldaan werd die aan het begin van de ontwikkelingsfase of aankoop procedure vastgesteld werden. Dit gebeurt in bepaalde gevallen ad hoc, maar het is geen standaardprocedure.]

**Concrete aanbevelingen**

[Bv. Wanneer eigen systemen ontwikkeld, aangeschaft of gewijzigd worden, moeten steeds de nodige maatregelen getroffen worden om de veiligheid te garanderen op applicatieniveau, om op deze wijze toekomstige veiligheidsinbreuken te vermijden. Een ‘security by design aanpak’ waarbij informatiebeveiliging vanaf het begin wordt ingebouwd in plaats van na de feiten te testen op veiligheid kan helpen.

Vooraleer nieuwe evoluties van bestaande systemen en toepassingen in productie worden genomen, moet eerst nagegaan worden of aan de beveiligingsvereisten voldaan is die reeds bij de ontwikkelingsfase werden vastgelegd. Deze praktijk dient consequent toegepast te worden en niet in willekeurige gevallen.]

**Normen van toepassing**

|  |  |  |
| --- | --- | --- |
| De aangehaalde aanbevelingen kaderen binnen onderstaande normen | | |
| A11.2.1 ISO 27002-14.2 | B11.2.1 ISO 27002-14.2 | A11.2.2 ISO 27002-14.2 |
|  |  |  |
|  |  |  |

1. Leveranciersrelaties
   1. INFORMATIEBEVEILIGING IN LEVERANCIERSRELATIES

**Huidige toestand**

[Het lokaal bestuur werkt samen met diverse hardware en software leveranciers, concreet gaat het hier over: **XXX**, **XXX** en **XXX**. Voor deze verschillende samenwerkingen werden de nodige (onderhouds)contracten afgesloten, maar het is niet duidelijk of daar ook steeds clausules in werden opgenomen met betrekking tot het gebruik en de verwerking persoonsgegevens en de verantwoordelijkheden qua onderhoud en opvolging.

Bovendien is het niet geheel duidelijk waar of bij wie al die contracten zich bevinden, vermoedelijk bevindt het merendeel zich bij de technische dienst. Verder wordt de dienstverlening niet actief gemonitord. Wel worden leveranciers erop aangesproken wanneer zij gemaakte afspraken niet nakomen.]

**Concrete aanbevelingen**

[Bv. Bewaar de bestaande onderhoudscontracten op een afgesproken locatie en breng in kaart welke zaken concreet gedekt worden binnen de contracten en welke garanties van toepassing zijn. Bundel de bevindingen in een beknopt doch helder overzicht, zodat de organisatie voor de verschillende hard- en software weet of de verantwoordelijkheid voor onderhoud en opvolging intern of bij de leverancier ligt.

Neem in toekomstige contracten met leveranciers steeds een clausule op waarin de leverancier de nodige waarborgen biedt voor de informatiebeveiliging van persoonsgegevens en de verplichten met betrekking tot het gebruik en de verwerking van persoonsgegevens. Daarnaast dienen de verantwoordelijkheden die de toeleverancier op zich neemt, denk bijvoorbeeld aan veiligheidsupdates, duidelijk omschreven te staan in deze contracten.

Spreek vaste rapporteringsmomenten af met toeleveranciers - minstens jaarlijks - waarin de dienstverlening in de afgelopen periode overlopen kan worden en gekeken kan worden of de leveranciers voldoen aan de clausules in de (onderhouds)contracten. De verantwoordelijke voor de opvolging van leveranciers kan zich hiervoor beroepen op het op te maken overzicht van bestaande contracten met bijhorende garanties.

Wanneer het lokaal bestuur overweegt om beroep te doen op een Cloud provider om diensten als software, databases, servers en netwerken via het internet te laten verlopen, moet eerst een grondige risicoanalyse uitgevoerd worden. Cloud computing heeft als voordeel dat eindgebruikers overal toegang hebben tot hun software en applicaties en dat de organisatie (vaak) veiliger en meer wendbaar kan functioneren, maar er moet ook gekeken worden of een dergelijke transitie geen nieuwe risico’s met zich meebrengt op vlak van informatieveiligheid.]

**Normen van toepassing**

|  |  |  |
| --- | --- | --- |
| De aangehaalde aanbevelingen kaderen binnen onderstaande normen | | |
| A12.1.1 ISO 27002-15.1 | B12.1.1 ISO 27002-15-1 | A12.1.2 ISO 27002-15.1 |
|  |  |  |
|  |  |  |

1. Informatiebeveiligingsincidenten
   1. BEHEER VAN INFORMATIEBEVEILIGINGSINCIDENTEN EN -VERBETERINGEN

**Huidige toestand**

[Bv. Klachten van burgers komen automatisch terecht in een klachtenregister zodat verdere opvolging mogelijk is. Daarnaast maakt de ICT-dienst gebruik van een ticketsysteem om grotere problemen te melden. Kleinere problemen worden ad-hoc opgelost zonder registratie. Een overkoepelende procedure die de verschillende fases doorloopt vanaf de detectie van een mogelijk incident werd tot op heden nog niet uitgeschreven.

Virusinfecties worden opgeslagen in het centraal beheerssysteem van \*naam toeleverancier\* en er zijn ook vastgelegde afspraken voor de melding en opvolging van mogelijke incidenten.]

**Concrete aanbevelingen**

[Bv. Maak een incidentenregister op waarin alle incidenten die een impact (kunnen) hebben op de informatieveiligheid, zoals het laten rondslingeren van persoonsgegevens nabij een printer, vastgelegd worden. Het is ook van belang dat een verantwoordelijke aangeduid wordt voor het onderhoud van dit register, zoals de functionaris gegevensbescherming, en dat een intern meldpunt aanwezig is om dergelijke incidenten te melden, zoals een [privacy@lokaalbestuur.be](mailto:privacy@lokaalbestuur.be) mailadres.

Zorg ervoor dat de functionaris gegevensbescherming en waar nodig de veiligheidscel steeds door de verantwoordelijke dienst op de hoogte gesteld wordt wanneer incidenten zich voordoen die kaderen binnen de informatieveiligheid.

Schrijf een formele interne meldingsprocedure uit voor de doorstroom van incidenten of meldingen rond informatieveiligheid door de verschillende diensten en medewerkers. Koppel hieraan een meldingsprocedure voor externe instanties die op de hoogte gebracht dienen te worden bij datalekken en andere IT-gerelateerde incidenten zoals de VTC, AVG, het CERT en de lokale politiezone. Hiervoor kan het bronmateriaal door **XXX** gebruikt worden.]

**Normen van toepassing**

|  |  |  |
| --- | --- | --- |
| De aangehaalde aanbevelingen kaderen binnen onderstaande normen | | |
| A13.1.1 ISO 27002-16.1 | B13.1.1 ISO 27002-16.1 | A13.1.2 ISO 27002-16.1 |
| B13.1.2 ISO 27002-16.1 | A13.1.3 ISO 27002-16.1 | B13.1.3 ISO 27002-16.1 |
| A13.1.4 ISO 27002-16.1 | A-13.1.5 ISO 27002-16.1 |  |

1. Bedrijfscontinuïteit
   1. INFORMATIEBEVEILIGINGSCONTINUÏTEIT

**Huidige toestand**

[Bv. Momenteel beschikt het bestuur nog niet over een volledig uitgewerkt business continuïteitsplan om de dienstverlening snel en efficiënt op te kunnen starten bij het voordoen van een incident. Wel is er reeds een risicobeoordeling die gebruikt kan worden om het plan concreet vorm te geven.

Wel zijn er reeds diverse (losstaande) preventieve maatregelen getroffen en aanbevelingen geformuleerd om mogelijke schade op te vangen, al worden deze niet regulier getest.]

**Concrete aanbevelingen**

[Bv. Maak werk van een volledig uitgewerkt business continuïteitsplan om de dienstverlening zo snel en efficiënt mogelijk op te starten na een cyberaanval of ander IT-gerelateerd incident. Hiervoor kan de reeds aanwezige risicoanalyse gebruikt worden, aangevuld met publiek beschikbaar bronmateriaal van **XXX** en **XXX**.

Bij het uitwerken van het business continuïteitsplan worden best alle relevante diensten en medewerkers - denk aan noodplanning, communicatie, faciliteiten, MAT – betrokken, aangezien het hier niet gaat over een puur IT-plan, maar een totaalaanpak die gedragen moet worden door de volledige organisatie.

Voorzie een business continuïteitsoefening zodra een eerste versie van het business continuïteitsplan aanwezig is. Op deze manier kan gekeken worden of het plan in de praktijk werkbaar is en er al dan niet bijsturingen nodig zijn. Het is aangeraden om deze oefening minstens tweejaarlijks te herhalen, zodat de organisatie het plan vlot kan inzetten wanneer nodig.]

**Normen van toepassing**

|  |  |  |
| --- | --- | --- |
| De aangehaalde aanbevelingen kaderen binnen onderstaande normen | | |
| A14.1.1 ISO 27002-17.1 | B14.1.1 ISO 27002-17.1 | B14.1.2 ISO 27002-17.1 |
|  |  |  |
|  |  |  |

* 1. REDUNDANTE COMPONENTEN

**Huidige toestand**

[Bv. De noodstroomvoorziening voorziet het lokaal bestuur, in combinatie met het back-upsysteem, van voldoende redundantie om de beschikbaarheid van persoonsgegevens te waarborgen.

Bovendien beschikt het bestuur over een servicecontract met verschillende firma’s, die voorzien in bijstand binnen een aantal uren in geval van panne. Daarbij dient wel aangehaald te worden dat een globaal servicecontract op dit moment nog niet aanwezig is.]

**Concrete aanbevelingen**

[Bv. Zorg ervoor dat de servicecontracten bij schade of panne op een locatie centraal beheerd worden, zodat deze snel opgevraagd en ingekeken kunnen worden in noodsituaties.

Bestudeer de bewaarde servicecontracten om na te gaan welke zaken allemaal concreet gedekt worden en welke garanties van toepassing zijn.

Giet de verschillende servicecontracten in een beknopt maar praktisch bruikbaar overzicht, zodat de organisatie in een oogopslag weet wanneer men beroep kan doen op externe firma’s en onder welke voorwaarden. Voeg ook de contactgegevens toe aan dit overzicht, zodat het opzoekwerk in tijden van hoge nood tot een minimum beperkt wordt.]

**Normen van toepassing**

|  |  |  |
| --- | --- | --- |
| De aangehaalde aanbevelingen kaderen binnen onderstaande normen | | |
| A-14.2.1 ISO 27002-17.1 |  |  |
|  |  |  |
|  |  |  |

1. Naleving
   1. NALEVING VAN WETTELIJKE VOORSCHRIFTEN

**Huidige toestand**

[Bv. De dienst informatieveiligheid houdt haar kennis op het vlak van informatieveiligheid courant door deel te nemen aan bijscholingen, seminaries en vakgroepsvergaderingen. Het gaat hierbij onder andere over de Werkgroep Informatieveiligheid onder de coördinatie van de VVSG en opleidingen uitgaande van de Vlaamse ICT organisatie.

Het behoort verder ook tot de taken van de veiligheidsconsulent om na te gaan of het gemeentebestuur voldoet aan alle vereisten, formaliteiten en voorschriften inzake informatieveiligheid. Ook voor samenwerking tussen gemeente en OCMW waakt de veiligheidsconsulent erover dat beide organisaties aan de nodige voorschriften voldoen, zeker nu een integratie van de gemeente ne het OCMW gepland staat.]

**Concrete aanbevelingen**

[Bv. Men dient op systematische wijze na te gaan of een machtiging vereist is voor de aanschaf of ontwikkeling van een systeem dat persoonsgegevens gebruikt of verwerkt. Een mogelijke werkwijze is de inzet van het [privacy@lokaalbestuur.be](mailto:privacy@lokaalbestuur.be) meldpunt voor dergelijke aanvragen, zodat de functionaris gegevensbescherming of andere relevante actoren advies kunnen verlenen.

Ga op systematische wijze na of een machtiging van de Vlaamse Toezichtcommissie (VTC vereist is voor de aanschaf of ontwikkeling van een systeem dat persoonsgegevens gebruikt of verwerkt.

Evalueer en update minstens tweejaarlijks de procedures voor de uitwerking en het onderhoud van documentatie die betrekking heeft op verleende machtigingen.

Zorg voor een centraal goedgekeurde aanpak om na te gaan of een verleende machtiging gerespecteerd blijft bij iedere wijziging aan een toepassing of applicatie die persoonsgegevens gebruikt of verwerkt.

Breng het Sectoraal Comité van het Rijksregister (Cfr. Artikel 10 van de Rijksregisterwet) op de hoogte van de identiteit van de veiligheidsconsulent en zijn/haar eventuele adjuncten.

Win advies in bij de Vlaamse Toezichtcommissie (VTC) voorafgaan aan de verplichte aanstelling van de veiligheidsconsulent en zijn/haar eventuele adjuncten.

**Normen van toepassing**

|  |  |  |
| --- | --- | --- |
| De aangehaalde aanbevelingen kaderen binnen onderstaande normen | | |
| A15.1.1 ISO 27002-18.1 | B15.1.1 ISO 27002-18.1 | A15.1.2 ISO 27002-17.1 |
| B15.1.2 ISO 27002-17.1 | A15.1.3 ISO 27002-17.1 | A15.1.4 ISO 27002-17.1 |
| A15.1.5 ISO 27002-17.1 | A15.1.6 ISO 27002-17.1 | A15.1.10 ISO-27002-17.1 |
| A15.1.11 ISO 27002-17.1 | A15.1.12 ISO 27002-17.1 | A15.1.13 ISO 27002-17.1 |
| A15.1.14 ISO 27002-17.1 | A15.1.15 ISO 27002-17.1 | A15.1.16 ISO 27002-17.1 |

* 1. INFORMATIEBEVEILIGINGSBEOORDELINGEN

**Huidige toestand**

[Bv. Tot op heden werden nog geen informatiebeveiligings- of ICT-veiligheidsaudits uitgevoerd. Dit zou een belangrijke meerwaarde voor de organisatie kunnen betekenen omdat zo gekeken kan worden of de risicobeoordeling aangevuld moet worden en bijkomende maatregelen genomen moeten worden.]

**Concrete aanbevelingen**

[Bv. Het is aangeraden om een ICT-veiligheidsaudit uit te laten voeren binnen de organisatie om zo bestaande zwakke plekken in kaart te brengen die vervolgens procesmatig kunnen aangepakt worden. De ICT-veiligheidsaudits met cofinanciering via Audit Vlaanderen kunnen hiervoor aangegrepen worden.

Onderzoek de mogelijkheid om op regelmatige basis een netwerkscan uit te laten voeren via een professionele dienstverlener of via de aankoop van specifieke software zoals **XXX**. Zo kan na het doorlopen van de ICT-veiligheidsaudits periodiek gekeken worden of geen nieuwe kwetsbaarheden ontstaan zijn die om aandacht vragen.

Werk in samenspraak met de lokale ICT-dienst een jaarlijks stappenplan uit om te controleren op courante pijnpunten zoals ontbrekende veiligheidsupdates, mislukte back-ups, standaardwachtwoorden op systemen en toepassingen, te brede toegangen en rechten, onveilige instellingen bij systemen en toepassingen, … Zoals eerder vermeld kunnen reguliere netwerkscans of de aanschaf van een netwerk scanner dit proces faciliteren.]

**Normen van toepassing**

|  |  |  |
| --- | --- | --- |
| De aangehaalde aanbevelingen kaderen binnen onderstaande normen | | |
| A15.2.1 ISO 27002-18.2 |  |  |
|  |  |  |
|  |  |  |

1. Bijlage 1: ISO-norm 27002 (controls)

1.1 Beoordelen van beveiligingsrisico’s

|  |  |  |
| --- | --- | --- |
| A1.1.1 | ISO 27005-8 | De beveiligingsrisico’s en -behoeften rond uw informatie die eigen zijn aan uw organisatie en die het gebruik en de verwerking van persoonsgegevens betreffen moeten, na identificatie en analyse, regelmatig geëvalueerd worden in samenspraak met het hoogste beslissingsorgaan van uw organisatie. |
| A1.1.1 | ISO 27005-8 | Wanneer een soort verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen voert de verwerkingsverantwoordelijke vóór de verwerking een beoordeling uit van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens. In geval van hoog blijvend risico wordt de toezichthoudende autoriteit/"Gegevensbeschermingsautoriteit" (GBA)/“Controleorgaan op de politionele informatie” (COC) geraadpleegd. |

1.2 Behandelen van beveiligingsrisico’s

|  |  |  |
| --- | --- | --- |
| A1.2.1 | ISO 27005-9 | Voor elk relevant risico omtrent het gebruik en de verwerking van persoonsgegevens vastgesteld na de informatierisicobeoordeling moeten de nodige beheersmaatregelen genomen en opgevolgd worden. |

2.1 Informatiebeveiligingsbeleid

|  |  |  |
| --- | --- | --- |
| A2.1.1 | ISO 27002-5.1 | Uw organisatie moet over een formeel, geactualiseerd en door het hoogste beslissingsorgaan van uw organisatie goedgekeurd informatiebeveiligingsbeleid beschikken dat op regelmatige basis naar alle relevante partijen gecommuniceerd wordt. |
| A2.1.2 | ISO 27002-5.1 | Er moet een duidelijke ondersteuning zijn van het hoogste beslissingsorgaan van uw organisatie om de implementatie van informatiebeveiliging in uw organisatie op te starten, te beheersen, te onderhouden en waar nodig bij te sturen. Voorbeelden van documenten m.b.t. informatiebeveiliging zijn:  een jaarverslag inzake informatiebeveiliging en een meerjarenplan inzake informatiebeveiliging. |

3.1 Interne organisatie rond informatiebeveiliging

|  |  |  |
| --- | --- | --- |
| A3.1.1 | ISO 27005-6.1 | Uw organisatie moet de nodige werkkredieten en middelen ter beschikking stellen teneinde te kunnen voorzien in de correcte coördinatie en uitvoering van het informatiebeveiligingsbeleid.  De uitvoering van het beveiligingsbeleid moet opgevolgd worden door de informatiebeveiligingscel geleid door een veiligheidsconsulent. Deze taken kunnen ook aan een extern erkende gespecialiseerde dienst toevertrouwd worden.  De informatiebeveiligingscel heeft een adviserende, stimulerende, documenterende en controlerende opdracht binnen uw organisatie. Daartoe moet de veiligheidsconsulent instaan voor:   * het verstrekken van deskundige adviezen aan de persoon belast met het dagelijks bestuur en verantwoordelijk voor de gegevensverwerking; * het uitvoeren van opdrachten die hem door de persoon belast met het dagelijks bestuur en verantwoordelijk voor de gegevensverwerking worden toevertrouwd. |
| A3.1.2 | **ISO 27005-6.1** | De veiligheidsconsulent moet steeds over de nodige competenties en informatie beschikken om zijn taak correct en tijdig uit te voeren. |
| A3.1.3 | **ISO 27005-6.1** | Uw organisatie moet over een actief beslissingsplatform beschikken dat op regelmatige basis samenkomt voor de validatie en de goedkeuring van de beheersmaatregelen voor informatiebeveiliging voorgesteld door de informatiebeveiligingscel. |
| A3.1.4 | **ISO 27005-6.1** | Uw organisatie moet, ongeacht het soort project, informatiebeveiliging steeds integreren in de projectbeheermethode(n) teneinde informatiebeveiligingsrisico’s te identificeren en aan te pakken. |
| A3.1.7 | **ISO 27005-6.1** | Elke stad en gemeente moet de communicatie van informatie aan de veiligheidsconsulent zodanig organiseren dat hij over de gegevens beschikt voor de uitvoering van de hem toegewezen veiligheidsopdracht en om overleg te organiseren tussen de verschillende betrokken partijen teneinde op deze manier de veiligheidsconsulent nauwer te betrekken bij de werkzaamheden van de organisatie. |
| A3.1.9 | **ISO 27005-6.1** | Een samenwerking tussen de stad/gemeente en het OCMW inzake hardware en ICT-technologie is toegestaan. Deze samenwerking moet de naleving van alle normen en regels garanderen waaraan elke organisatie op zich en ingevolge die samenwerking gehouden is.  Voordat hardware, telecommunicatielijnen,…, alsook elk gemeenschappelijk beheer samengebracht kunnen worden, moet er een samenwerkingsakkoord gesloten worden tussen de verschillende partnerorganisaties. In dat akkoord moeten de bevoegdheden van elke organisatie vermeld worden, alsook de verantwoordelijkheden.  Ingeval een deel van dit beheer toevertrouwd wordt aan een derde (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 Privacywet, artikel 16. |

3.2 Mobiel werken

|  |  |  |
| --- | --- | --- |
| A3.2.1 | ISO 27002-6.2 | Uw organisatie moet beschikken over een formeel beleid inzake mobiel gebruik van apparatuur waarbij rekening wordt gehouden met de risico’s van het werken in onbeschermde omgevingen. Medewerkers die mobiele apparatuur gebruiken, moeten getraind worden zodat ze zich (1) bewust worden van de extra risico’s die deze manier van werken met zich meebrengt en (2) weten welke beheersmaatregelen dienen getroffen te worden. |
| B3.2.1 | ISO 27002-6.2 | De nodige beheersmaatregelen om mobiel computergebruik (inclusief andere mobiele media) en telewerken op een veilige manier toe te laten, moeten ingevoerd worden. Deze maatregelen kunnen onder meer betrekking hebben op:   * cryptografische technieken; * back-ups; * bescherming tegen malware; * toegangsbeveiliging bij de externe toegang tot persoonsgegevens; * fysieke beveiliging van draagbaar computerapparatuur (inclusief mobiele media) en van de telewerklocatie tegen diefstal. |
| A3.2.2 | ISO 27002-6.2 | Organisaties die telewerken toestaan, behoren een beleid uit te vaardigen dat de voorwaarden en beperkingen definieert voor het telewerken. |
| B3.2.2 | ISO 27002-6.2 | De enige toegestane oplossing om een gebruiker via het internet toegang te verlenen tot het interne netwerk van de organisatie is een beveiligde en gecontroleerde connectie te gebruiken. Indien men toegang heeft tot de KSZ moet het concept goedgekeurd zijn door de Kruispuntbank van de sociale zekerheid.  Deze verbinding moet aan de volgende voorwaarden voldoen:   * sterke authenticatie van zowel de gebruiker als de computer; * een controle van het veiligheidsniveau van het werkstation alvorens de verbinding mogelijk te maken; * de verbindingen moeten gelogd worden; * het mag niet mogelijk zijn om gelijktijdig verbindingen op te zetten met verschillende netwerken.   Meer gedetailleerde informatie kan verkregen worden in het veiligheidsbeleid met betrekking tot het gebruik van een VPN-verbinding gepubliceerd op de website van de Kruispuntbank van de Sociale Zekerheid. |

4.1 Informatiebeveiliging voorafgaand aan het dienstverband

|  |  |  |
| --- | --- | --- |
| A4.1.1 | ISO 27002-7.1 | Uw organisatie dient duidelijk het belang van informatiebeveiliging tijdens het rekruteringsproces aan te duiden aan de potentiële kandidaten. |
| A4.1.2 | **ISO 27002-7.1** | Alle kandidaten dienen hun arbeidsovereenkomst te ondertekenen waarin ook clausules staan omtrent hun verantwoordelijkheden voor de informatiebeveiliging van persoonsgegevens. |

4.2 Informatiebeveiliging tijdens het dienstverband

|  |  |  |
| --- | --- | --- |
| A4.2.1 | ISO 27002-7.2 | Opdat gegarandeerd zou worden dat alle interne medewerkers zich engageren om hun verplichtingen tot de vertrouwelijkheid en de veiligheid van persoonsgegevens te respecteren moet uw organisatie alle interne medewerkers die betrokken zijn bij het gebruik en de verwerking van de persoonsgegevens op de hoogte stellen van de vertrouwelijkheids- en beveiligingsverplichtingen onder de vorm van:   * een gedragscode; * en/of vermelding van deze gedragscode in het arbeidsreglement; * en/of een functiebeschrijving met vermelding van de vertrouwelijkheids- en beveiligingsverplichtingen; * en/of contractuele bepalingen; * en daarnaast onder de vorm van geschikte bewustzijnsopleiding en -training en regelmatige bijscholing. |
| B4.2.1 | ISO 27002-7.2 | Alle gepaste maatregelen moeten geïmplementeerd worden om te verhinderen dat persoonsgegevens ongecontroleerd uw organisatie verlaten en in ongeoorloofde handen vallen. Met name door:   * bedrijfsmiddelen te beschermen tegen ongeoorloofde toegang, openbaarmaking, wijziging, vernietiging of verstoring; * bepaalde beveiligingsprocessen of -activiteiten uit te voeren; * te waarborgen dat de verantwoordelijkheid van genomen handelingen steeds duidelijk wordt toegewezen aan een persoon; * beveiligingsgebeurtenissen of potentiële gebeurtenissen of andere beveiligingsrisico’s te rapporteren. |
| A4.2.2 | ISO 27002-7.2 | Uw organisatie moet alle externe medewerkers (ingehuurd personeel en externe gebruikers) belast met het gebruik en/of de verwerking van de persoonsgegevens op de hoogte stellen van de vertrouwelijkheids- en beveiligingsverplichtingen door een gedragscode en het ondertekenen van een contractueel document met duidelijke contractuele bepalingen. |
| A4.2.3 | ISO 27002-7.3 | Uw organisatie moet over een formele en gecommuniceerde disciplinaire procedure beschikken om actie te ondernemen tegen medewerkers die een inbreuk hebben gepleegd op de informatiebeveiliging. |

4.3 Informatiebeveiliging bij beëindiging of wijziging van dienstverband

|  |  |  |
| --- | --- | --- |
| A4.3.1 | ISO 27002-7.3 | Uw organisatie moet de verantwoordelijkheden en taken m.b.t. informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband definiëren, communiceren naar de interne of externe medewerker en ten uitvoer brengen. |
| B4.3.1 | ISO 27002-7.3 | Bij wijziging van verantwoordelijkheden aan deelname in de gegevensverwerking moeten de noodzakelijke aanpassingen aan de informatiebeveiligingsmaatregelen getroffen worden zoals opgenomen in de punten 5.1.3 en 6.1.2. |

5.1 Verantwoordelijkheid voor bedrijfsmiddelen

|  |  |  |
| --- | --- | --- |
| B5.1.1 | ISO 27002-8.1 | Een geactualiseerde inventaris van relevante bedrijfsmiddelen met betrekking tot persoonsgegevensverwerkingen moet in samenwerking met de betrokken operationele diensten worden opgesteld. Relevante bedrijfsmiddelen zijn onder andere:   * informatie; * software programma’s; * fysieke middelen; * diensten; * alle gebruikers (inclusief toegangsrechten). |
| B5.1.2 | ISO 27002-8.1 | In dit inventaris moet elk relevant bedrijfsmiddel met betrekking tot een persoonsgegevensverwerking gekoppeld zijn aan een welbepaalde functie/persoon binnen uw organisatie (verantwoordelijkheid). |
| B5.1.3 | ISO 27002-8.1 | Bij beëindiging van dienstverband, contract of overeenkomst moet een formele procedure toegepast worden voor het teruggeven van alle relevante verstrekte bedrijfsmiddelen (zoals programmatuur, bedrijfsdocumenten, apparatuur en toegangskaarten). In geval van gebruik van persoonlijke apparatuur moeten er gepaste maatregelen toegepast worden voor de overdracht van alle relevante informatie aan de organisatie en het correct verwijderen van de informatie van de apparatuur. |

5.2 Classificatie van informatie

|  |  |  |
| --- | --- | --- |
| A5.1.1 | ISO 27002-8.2 | Bij de persoonsgegevensverwerkingen moet uw organisatie een duidelijk onderscheid maken tussen de volgende gegevenstypes:   * 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. |
| B5.2.1 | ISO 27002-8.2 | Bij het gebruik en de verwerking van persoonsgegevens moet duidelijk rekening gehouden worden met het onderscheid tussen de volgende gegevenstypes:   * anonieme gegevens; * persoonsgegevens; * gevoelige persoonsgegevens; * gecodeerde al dan niet gevoelige persoonsgegevens. | |
| A5.1.2 | ISO 27002-8.2 | Alle gebruikers die persoonsgegevens gebruiken/verwerken moeten op de hoogte zijn van dit onderscheid. | |

5.3 Behandelen van media

|  |  |  |
| --- | --- | --- |
| A5.2.1 | ISO 27002-8.3 | Uw organisatie dient procedures te hebben voor het beheer van verwijderbare media waarop persoonsgegevens worden opgeslagen en die de beveiligingsperimeter van uw organisatie kunnen verlaten. Denk hierbij ook aan de verwijderbare media in apparatuur zoals multifunctionele printers en kopieermachines. |
| B5.3.1 | ISO 27002-8.3 | Bij gebruik van verwijderbare of andere media waarop persoonsgegevens worden opgeslagen dienen de gepaste beheersmaatregelen genomen te worden. Enkele voorbeelden zijn:   * indien de media de beveiligingsperimeter verlaten: * moeten de opgeslagen persoonsgegevens verwijderd worden indien ze niet meer nodig zijn, * met persoonsgegevens, moet vooraf goedkeuring worden verkregen en wordt een register bijgehouden; * stations voor verwijderbare media enkel vrijgeven als dit om bedrijfsredenen noodzakelijk is; * het bewaren van persoonsgegevens op verwijderbare media moet in lijn zijn met de levensduur van de media. Indien de bewaartermijn de levensduur overstijgt, moeten de gegevens ook elders opgeslagen worden. |
| A5.2.2 | ISO 27002-8.3 | Uw organisatie moet de nodige maatregelen bepalen om fysieke media (inclusief papieren documenten) die persoonsgegevens bevatten tijdens het transport te beschermen tegen onbevoegde toegang, misbruik of corruptie. |
| B5.3.2 | ISO 27002-8.3 | De gepaste maatregelen om fysieke media (inclusief papieren documenten) die persoonsgegevens bevatten tijdens het transport te beschermen tegen onbevoegde toegang, misbruik of corruptie behoren uitgevoerd te worden. Mogelijke maatregelen zijn:   * betrouwbare transport- of koerierdiensten gebruiken; * procedures ontwikkelen om de identificatie van koeriers te verifiëren; * toereikende verpakking gebruiken om de inhoud te beschermen tegen fysieke schade tijdens het transport; * registraties bijhouden omtrent het vervoer, de ontvangst en de identificatie van de inhoud en toegepaste bescherming van de media. |
| A5.2.3 | ISO27002-8.3 | Het hoogste beveiligingsniveau opgelegd aan de twee organisaties is van toepassing voor elke gedeelde informatiedrager/medium, en dit zowel voor actieve informatiedragers als deze gebruikt voor back-up en archivering.  De toegang tot deze informatiedragers moet in functie van de noden verleend worden door de bevoegde dienst. De toegangen tot deze dragers moeten kunnen nagegaan worden. |

6.1 Eisen voor toegangsbeveiliging

|  |  |  |
| --- | --- | --- |
| A6.1.1 | ISO 27002-9.1 | Uw organisatie moet een goedgekeurd en geactualiseerd toegangsbeveiligingsbeleid hebben met betrekking tot het toekennen, veranderen en verwijderen van toegangsrechten tot toepassingen en systemen die persoonsgegevens gebruiken/verwerken.  Dit beleid moet vastgesteld, gedocumenteerd en beoordeeld zijn op basis van de classificatie van de persoonsgegevens. |
| B6.1.1 | ISO 27002-9.1 | Uw netwerkbeheerders moeten de vastgestelde beveiligingsmaatregelen implementeren indien toegang wordt verleend tot persoonsgegevens via netwerken of netwerkdiensten. |
| A6.1.2 | ISO 27002-9.1 | Met betrekking tot netwerken of netwerkdiensten moet uw organisatie de gepaste beveiligingsmaatregelen bepalen opdat iedere persoon slechts toegang zou hebben tot de persoonsgegevens waarvoor hij uitdrukkelijk een autorisatie heeft verkregen. |
| B6.1.2 | ISO 27002-9.1 | De toegangsrechten van alle medewerkers en externe gebruikers tot informatie en informatieverwerkende faciliteiten moeten verwijderd of aangepast worden bij respectievelijk beëindiging of wijziging van hun dienstverband, contract of overeenkomst. |

6.2 Verantwoordelijke voor toegangsrechten van gebruikers

|  |  |  |
| --- | --- | --- |
| A6.2.1 | ISO 27002-9.2 | Uw organisatie moet een verantwoordelijke aanstellen die belast wordt met het beheer van alle aanvragen m.b.t. de toegang tot persoonsgegevens. Deze verantwoordelijke moet verschillend zijn van de persoon die de toegangsrechten op technisch niveau in de systemen toekent, aanpast of verwijdert. |

6.3 Verantwoordelijkheden van gebruikers

|  |  |  |
| --- | --- | --- |
| A6.3.1 | ISO 27002-9.3 | De gebruikers moeten worden ingelicht over hun verantwoordelijkheid in een doeltreffende toegangsbeveiliging, onder meer inzake het gebruik van wachtwoorden en beveiliging van gebruikersapparatuur waarop persoonsgegevens gebruikt/verwerkt worden. |

6.4 Toegangsbeveiliging van systemen en toepassingen

|  |  |  |
| --- | --- | --- |
| A6.4.1 | ISO 27002-9.4 | Uw organisatie moet de gepaste beveiligingsmaatregelen bepalen om de toegang tot persoonsgegevens te beperken. |
| B6.4.1 | ISO 27002-9.4 | Uw informaticadienst moet per bedrijfstoepassing op basis van de beveiligingseisen de nodige beveiligingsmaatregelen nemen om de toegang tot de persoonsgegevens te beperken.  Dit dient te gebeuren door middel van een:   * identificatiesysteem- (wie bent u?); * authenticatiesysteem- (hoe maakt u duidelijk wie u bent?); * en een autorisatiesysteem (wat mag u doen?). |
| A6.4.2 | ISO 27002-9.4 | Uw organisatie moet de toegang beperken voor informatiebeheerders (systeembeheerders, ook wel “superusers” genoemd) tot systemen en toepassingen waarop persoonsgegevens gebruikt/verwerkt worden. |
| B6.4.2 | ISO 27002-9.4 | De toegang voor uw informatiebeheerders (systeembeheerders, ook wel “superusers” genoemd) tot informaticasystemen waarop de persoonsgegevens gebruikt/verwerkt worden, moet beperkt worden door middel van:   * identificatie (wie bent u?); * authenticatie (hoe maakt u duidelijk wie u bent?); * en autorisatie (wat mag u doen als superuser?). |
| A6.4.3 | ISO 27002-9.4 | Bij het gebruik van gemeenschappelijke informatica-infrastructuur door verscheidende organisaties 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 ambt binnen of voor rekening van hun respectievelijke organisatie(s).  Bij toegang tot gegevens moet er een formele identificatie plaatsvinden. Er moet onderscheid kunnen gemaakt worden tussen toegang in naam van de gemeente of 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 een taak uitvoert. |
| B6.4.3 | ISO 27002-9.4 | Scheiding van de organisaties:   * Op niveau van het besturingssysteem moeten de organisaties logisch gescheiden worden. * Het systeem van toegangsrechten moet een onderscheid kunnen maken tussen de medewerkers van de verschillende organisaties. Indien een medewerker voor meerdere organisaties werkt, moet hij beschikken over een account binnen elke organisatie om een scheiding van zijn rechten en toegang te garanderen. |
| B6.4.4 | ISO 27002-9.4 | Gebruik van een gemeenschappelijk softwarepakket  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 (via een fijnkorrelig systeem van gebruikers- en toegangsbeheer). Er dient gezorgd te worden voor een logische scheiding |
| B6.4.5 | ISO 27002-9.4 | Gemeenschappelijk gebruik voor boekhouding  Het gebruik van één boekhoudpakket is toegelaten op voorwaarde dat aparte rekeningen en boekingen gehanteerd worden voor de twee entiteiten. Dit zal trouwens noodzakelijk zijn in het kader van externe audits en boekhoudkundige documenten. |
| B6.4.6 | ISO 27002-9.4 | Gemeenschappelijk systeem voor personeelsbeheer  Met betrekking tot informatiebeveiliging moeten, voor het goed functioneren van de organisatie, een aantal rollen en functies gedefinieerd worden binnen elke organisatie apart. Hierbij moet rekening gehouden worden met de regels, verplichtingen en beperkingen hierop van toepassing.  Pakketten voor tijdsregistratie, vakantieregeling, loopbaanregistratie, lonen e.d. kunnen worden gedeeld, opnieuw op voorwaarde dat toegang en opslag van de gegevens gescheiden worden gehouden. |
| B6.4.7 | ISO 27002-9.4 | Om een optimale beveiliging van het netwerk te garanderen, kan een gewone gebruiker ook in een samenwerkingsverband tussen een stad/gemeente en een OCMW niet beschikken over administratorrechten op zijn werkstation. Deze beperking van rechten heeft tot doel te vermijden dat het werkstation en het netwerk besmet worden door malware of dat het werkstation van de gebruiker slecht wordt geconfigureerd. Deze beperking heeft tot gevolg dat de gebruiker niet over alle functies op zijn werkstation zal beschikken. De gebruiker zal bijvoorbeeld niet gemachtigd zijn om nieuwe toepassingen te installeren of om de netwerk- of systeemparameters te wijzigen.  Deze maatregel geldt zowel voor vaste werkstations (“desktops”) als voor mobiele (“laptops”). In geval van nieuwe technologieën (smartphones, tablets…) dient een risicoanalyse uitgevoerd te worden teneinde de gepaste veiligheidsmaatregelen te kunnen toepassen. |
| B6.4.8 | ISO 27002-9.4 | De toegang tot de informatiesystemen moet granulair kunnen verleend worden. Het moet dus mogelijk zijn aan een gebruiker enkel de rechten te verlenen die nodig zijn voor de uitvoering van zijn opdracht binnen de gemeente/stad of binnen het OCMW. |

7.1 Cryptografische beheersmaatregelen

|  |  |  |
| --- | --- | --- |
| A7.1.1 | ISO 27002-10.1 | Afhankelijk van de resultaten van de risicobeoordeling moet uw organisatie een beleid ontwikkelen voor een correct en doeltreffend gebruik van cryptografie om de vertrouwelijkheid, authenticiteit en/of integriteit van persoonsgegevens te beschermen. |
| B7.1.1 | ISO 27002-10.1 | De vastgestelde cryptografische beheersmaatregelen dienen geïmplementeerd te worden om de vertrouwelijkheid, authenticiteit en/of integriteit van persoonsgegevens te beschermen. |
| A7.1.2 | ISO 27002-10-1 | Uw organisatie moet een beleid ontwikkelen voor het gebruik, de bescherming en de levensduur van cryptografische sleutels tijdens hun gehele levenscyclus. |
| B7.1.2 | ISO 27002-10.1 | Het beleid met betrekking tot het beheer van cryptografische sleutels moet over de gehele levenscyclus zorgvuldig worden toegepast. |

8.1 Beveiliging van de omgeving

|  |  |  |
| --- | --- | --- |
| A8.1.1 | ISO 27002-11.1 | Op basis van de resultaten van de risicobeoordeling moeten beveiligde zones en de gepaste toegangsbeveiligingen bepaald worden om alle ruimten te beveiligen waarin zich informatie en informatieverwerkende faciliteiten met persoonsgegevens bevinden. |
| B8.1.1 | ISO 27002-11.1 | De toegang tot beveiligde ruimtes (waarin zich persoonsgegevens bevinden of gebruikt/verwerkt worden) moet strikt beperkt worden tot de bevoegde personen door uw organisatie aangeduid door het aan brengen van de vastgestelde toegangsbeveiligingen.  Hierop moet door de aangeduide verantwoordelijke regelmatige controle uitgeoefend worden, zowel tijdens als buiten de normale werkuren (logboek of logfile). |
| A8.1.2 | ISO 27002-11.1 | Uw organisatie moet de nodige maatregelen bepalen met betrekking tot de beveiligde zones om elke vorm van schade te vermijden die de persoonsgegevens in gevaar kunnen brengen. |
| B8.1.2 | ISO 27002-11.1 | De gepaste maatregelen moeten genomen worden om schade door brand, wateroverlast, explosie, … kortom elke vorm van natuurlijke of door mensen veroorzaakte calamiteiten te vermijden. Enkele voorbeelden van maatregelen zijn:   * de brandcompartimentering laten aansluiten met de detectie van beveiligde ruimtes; * de gepaste branddetectie en brandblusapparatuur voorzien en de werking ervan op geregelde tijdstippen controleren; * opslag van media voor back-ups en reserveapparatuur scheiden van de beveiligde ruimte. |

8.2 Beveiligde apparatuur

|  |  |  |
| --- | --- | --- |
| A8.2.1 | ISO 27002-11.2 | Uw organisatie behoort op basis van de risicobeoordeling de gepaste beheersmaatregelen te bepalen betreffende de apparatuur, de bekabeling en de ondersteunende voorzieningen om verlies, schade, diefstal en het ongewenst veranderen van persoonsgegevens te voorkomen. Hierbij dient bijzondere aandacht te worden besteed aan apparatuur die zich buiten het terrein van de organisatie bevindt of wordt gebruikt. |
| B8.2.1 | ISO 27002-11.2 | Apparatuur moet beschermd worden tegen fysieke bedreigingen en gevaren van buitenaf. Hierbij dient bijzondere aandacht te worden besteed aan apparatuur die zich buiten het terrein van organisatie bevindt of wordt gebruikt. Er dient onder meer aandacht te zijn voor:   * de plaatsing en de bescherming van apparatuur zodat het beschermd is tegen risico’s van schade en storing van buitenaf en de toegang door onbevoegden wordt vermeden; * de bescherming tegen stroomuitval en andere storingen door onderbreking van nutsvoorzieningen; * het beveiligen van voedings- en telecommunicatiekabels tegen interceptie of beschadiging; * het onderhoud van de apparatuur. |
| A8.2.2 | ISO 27002-11.2 | Uw organisatie moet een specifieke procedure uitwerken voor het verwijderen of hergebruiken van alle apparatuur met opslagmedia waarop persoonsgegevens worden gebruikt/verwerkt.. |
| B8.2.2 | ISO 27002-11.2 | Alle apparatuur met opslagmedia moet voor verwijdering of hergebruik gecontroleerd worden zodat alle persoonsgegevens veilig overschreven of verwijderd zijn. Indien deze apparatuur gevoelige persoonsgegevens bevat moeten specifieke maatregelen genomen worden om deze apparatuur fysiek te vernietigen of de informatie zodanig te verwijderen met technieken die het onmogelijk maken deze terug te halen. |

9.1 Operationele procedures en verantwoordelijkheden

|  |  |  |
| --- | --- | --- |
| A9.1.1 | ISO 27002-12.1 | Uw organisatie moet de nodige procedures en verantwoordelijkheden bepalen bij veranderingen in de organisatie, bedrijfsprocessen, informatieverwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging van persoonsgegevens. |
| B9.1.1 | ISO 27002-12.1 | Om een correcte en veilige bediening van informatieverwerkende faciliteiten die persoonsgegevens gebruiken/verwerken te waarborgen moeten bedieningsprocedures gedocumenteerd en beschikbaar gesteld worden aan alle gebruikers die ze nodig hebben. |
| A9.1.2 | ISO 27002-12.1 | Uw organisatie moet voorzien in een functiescheiding om te voorkomen dat één enkele persoon de exclusieve controle zou verwerven over een verwerking van persoonsgegevens. |
| B9.1.2 | ISO 27002-12.1 | Conform aanbeveling nr 01/2013 van de Privacycommissie moet er een strikte scheiding zijn tussen de ontwikkelings-, test-, aanvaardings-/integratie- en productieomgevingen om het risico op onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen. Dit impliceert onder meer. dat er geen testen of ontwikkelingen mogen plaatsvinden in de productieomgeving. Slechts in uitzonderlijke gevallen kan voor testdoeleinden van deze regel afgeweken worden op voorwaarde dat de gepaste maatregelen getroffen worden. |

9.2 Bescherming tegen malware

|  |  |  |
| --- | --- | --- |
| A9.2.1 | ISO 27002-12.2 | Uw organisatie moet beschikken over geschikte procedures en richtlijnen ter bescherming tegen malware en om het bewustzijn van de systeem- en de eindgebruikers te vergroten.  Enkele voorbeelden van mogelijke richtlijnen en procedures zijn:   * gebruik van ongeautoriseerde programmatuur verbieden; * beleid bepalen inzake het ontvangen van bestanden en programmatuur vanuit of via externe netwerken of via enig ander medium; * vastleggen van de verantwoordelijkheden inzake de bescherming tegen malware. |
| B9.2.1 | ISO 27002-12.2 | Ter bescherming tegen malware (voorkomen, ontdekken en verwijderen/herstellen) behoort uw informaticadienst anti-malware- en herstelsoftware te installeren en regelmatig te updaten, waarbij computers en media als voorzorgsmaatregel of routematig worden gescand. De uitgevoerde scan behoort onder meer:   * alle bestanden die via netwerken of via elke vorm van opslagmedium zijn ontvangen, vóór gebruik op malware te scannen; * bijlagen en downloads vóór gebruik op malware te scannen en dit op verschillende cruciale plaatsen in uw netwerkconfiguratie (mailservers, computers, netwerktoegang…); * internetpagina’s op malware te scannen.   Nauwkeurige en informatieve waarschuwingsberichten in het geval van een reële bedreiging kunnen het bewustzijn van de gebruikers vergroten. |

9.3 Back-up

|  |  |  |
| --- | --- | --- |
| A9.3.1 | ISO 27002-12.3 | Uw organisatie dient een geschikt back-up beleid op te stellen en op te volgen om een adequaat herstel te waarborgen na verlies, schade, diefstal of het ongewenst veranderen van persoonsgegevens. |
| B9.3.1 | ISO 27002-12.3 | Uw verantwoordelijken voor het back-upbeheer moeten op regelmatige basis volledige en gecontroleerde back-ups van de persoonsgegevens nemen en moeten op regelmatige basis controleren of ze in staat zijn om deze back-ups terug te gebruiken (“*restore*”). |
| B9.3.2 | ISO 27002-12.3 | Uw verantwoordelijken voor het back-upbeheer moeten de nodige maatregelen nemen om de vertrouwelijkheid, integriteit en toegankelijkheid m.b.t. de back-up gegevens te garanderen. |

9.4 Monitoring

|  |  |  |
| --- | --- | --- |
| B9.4.1 | ISO 27002-12.4 | Voor het gebruik en de verwerking van persoonsgegevens moeten, conform de referentiemaatregelen van de Privacycommissie, duidelijke afgeschermde logbestanden aangemaakt worden. De logbestanden behoren onder meer activiteiten, uitzonderingen en gebeurtenissen te omvatten. |
| B9.4.2 | ISO 27002-12.4 | De door uw organisatie aangeduide verantwoordelijke moet over een geactualiseerde lijst beschikken met alle personen en hun respectievelijke toegangsniveaus tot de persoonsgegevens. |
| B9.4.3 | ISO 27002-12.4 | Elke toegang tot een informatiesysteem dat persoonsgegevens bevat, moet getraceerd kunnen worden zodat bovenop de vragen “wie heeft toegang, wanneer, tot wat en waarom?” ook op de vraag “voor welke organisatie?” kan geantwoord worden.  De integriteit en vertrouwelijkheid en afscheiding per organisatie van deze loggings moet gegarandeerd worden en ze moeten geraadpleegd kunnen worden door de bevoegde autoriteiten. |

9.5 Overwegingen bij audits van informatiesystemen

|  |  |  |
| --- | --- | --- |
| B9.5.1 | ISO 27002-12.7 | De gepaste beheers- en beveiligingsmaatregelen moet genomen worden om gegevenslekken, verlies aan persoonsgegevens, gegevensbeschadiging en verstoringen van bedrijfsprocessen te vermijden tijdens informatiesysteem-audits. |

10.1 Netwerkbeveiliging

|  |  |  |
| --- | --- | --- |
| A10.1.1 | ISO 27002-13.1 | Netwerkbeveiliging moet een onderdeel vormen van uw globaal informatiebeveiligingsplan waarbij bijzondere aandacht moet besteed worden aan de informatiestromen waarbij persoonsgegevens uw organisatie kunnen verlaten. |
| B10.1.1 | ISO 27002–13.1 | Uw netwerkbeheerders moeten beveiligingsmaatregelen nemen ter bescherming van de verschillende netwerken waarmee de apparatuur (die de persoonsgegevens verwerkt) verbonden is. |
| B10.1.2 | ISO 27002–13.1 | Uw netwerkbeheerders moeten de nodige beheersmaatregelen nemen op het niveau van de informatienetwerken om:   * de vertrouwelijkheid en de integriteit m.b.t. de persoonsgegevens te garanderen, en * ongeoorloofde toegang te voorkomen; * tegemoet te komen aan de vereisten van beschikbaarheid en capaciteit. |
| B10.1.3 | ISO 27002–13.1 | Uw netwerkbeheerders moeten een geactualiseerde cartografie bijhouden van de gegevensstromen op netwerkniveau, en deze steeds ter beschikking stellen van de veiligheidsconsulent. |
| B10.1.4 | ISO 27002–13.1 | Scheiding van de organisaties  Zelfs indien verschillende organisaties samenwerken, is het noodzakelijk een fysieke of logische scheiding te bewerkstellingen tussen die organisaties. 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 middelen. |
| B10.1.5 | ISO 27002–13.1 | Indien de organisatie(s) verspreid is/zijn over meerdere sites, dienen de nodige maatregelen getroffen te worden opdat de verbinding tussen deze sites gepast beveiligd zou zijn.  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 communiceren. Bij gebruik van draadloze technologie is de beveiligingspolicy over draadloze netwerken van toepassing (zie website van de Kruispuntbank van de Sociale Zekerheid); * een andere oplossing bestaat erin een VPN-verbinding te installeren tussen de sites via internet. De standaardoplossing die aanbevolen wordt door de Kruispuntbank van de Sociale Zekerheid is de VPN “IPSec”-verbinding LAN-to-LAN. |

10.2 Informatietransport

|  |  |  |
| --- | --- | --- |
| A-10.2.1 | ISO 27002-13.2 | Uw organisatie moet over een formeel, geactualiseerd en door het hoogste beslissingsorgaan van uw organisatie goedgekeurd beleid beschikken inzake communicatiemiddelen (zoals e-mail, internet, video, fax en telefoon) dat op regelmatige basis naar alle relevante partijen gecommuniceerd wordt en waarin bijzondere aandacht wordt gegeven aan het gebruik van persoonsgegevens. Wij verwijzen hierbij ook naar aanbeveling nr. 8/2012 van de Privacycommissie betreffende de controle door de werkgever op het gebruik van elektronische communicatie-instrumenten op de werkvloer. |
| A-10.2.2 | ISO 27002-13.2 | Uw organisatie moet de eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van uw organisatie betreffende het beschermen van persoonsgegevens weerspiegelen, vastleggen, regelmatig beoordelen en documenteren. |
| A-10.2.3 | ISO 27002-13.2 | Gemeenschappelijke diensten steden/gemeenten en OCMW’s:  Juridisch hebben we te maken met twee verschillende organisaties met een eigen specifieke regelgeving. Dossiers die persoonsgegevens bevatten kunnen en mogen dus niet gedeeld worden tenzij er een specifieke machtiging van het bevoegde Sectoraal comité verleend is. |
| B-10.2.3 | ISO 27002-13.2 | Medewerkers in dienst van meerdere organisaties moeten beschikken over een onderscheiden e-mailadres binnen elke organisatie. |

11.1 Beveiligingseisen voor informatiesystemen

|  |  |  |
| --- | --- | --- |
| A-11.1.1 | ISO 27002-14.1 | Uw organisatie dient erover te waken dat de beveiligingsvereisten voor de persoonsgegevens onverminderd gegarandeerd blijven bij de aanschaf of ontwikkeling van nieuwe informatiesystemen of bij uitbreidingen van bestaande informatiesystemen. Onder informatiesystemen worden toepassingen, diensten, IT-middelen of andere informatieverwerkende onderdelen verstaan. |
| B-11.1.1 | ISO 27002-14.1 | Uw beveiligingseisen moeten voorafgaand aan de aanschaf en/of de ontwikkeling en/of de verbetering van het informatiesysteem formeel en duidelijk vastgesteld, overeengekomen en gedocumenteerd worden. |

11.2 Beveiliging in ontwikkelings- en ondersteuningsprocessen

|  |  |  |
| --- | --- | --- |
| A-11.2.1 | ISO 27002-14.2 | Uw organisatie moet over procedures beschikken voor de ontwikkeling van nieuwe systemen of belangrijke evoluties van bestaande systemen zodat door de projectverantwoordelijke rekening wordt gehouden met de noodzakelijke beveiligingsvereisten met betrekking tot de bescherming van persoonsgegevens. |
| B-11.2.1 | ISO 27002-14.2 | De projectverantwoordelijke moet, vooraleer nieuwe of belangrijke evoluties van bestaande systemen in productie genomen worden, nagaan of aan de beveiligingsvereisten die aan het begin van de ontwikkelingsfase vastgesteld zijn, voldaan is. |
| A-11.2.2 | ISO 27002-14.2 | Uw organisatie moet duidelijke formele wijzigingsprocedures toepassen zodat de kans op onterechte wijzigingen of het lekken van persoonsgegevens tot een minimum beperkt wordt. |

12.1 Informatiebeveiliging in leveranciersrelaties

|  |  |  |
| --- | --- | --- |
| A12.1.1 | ISO 27002-15.1 | In geval van samenwerking met leveranciers dient uw organisatie zich ervan te vergewissen dat de leverancier voldoende waarborgen biedt m.b.t. de informatiebeveiliging van persoonsgegevens en dat de verplichtingen inzake het gebruik en de verwerking van persoonsgegevens contractueel zijn vastgelegd (cfr. Privacywet Art.16 §1). |
| B12.1.1 | ISO 27002-15-1 | De dienstverlening van leveranciers moet op regelmatige basis gemonitord, beoordeeld en geaudit worden. |
| A12.1.2 | ISO 27002-15.1 | In het geval uw organisatie voor de opslag, het gebruik en/of de verwerking van persoonsgegevens overweegt gebruik te maken van de diensten van een cloudprovider dient uw organisatie een risicobeoordeling uit te voeren met betrekking tot de overeenstemming inzake de voorgestelde informatiebeveiliging en onderhavige richtsnoeren, en de contractuele voorwaarden (inzonderheid een eventuele toegang tot de persoonsgegevens door derden en minimale contractuele garanties met betrekking tot bijvoorbeeld auditregels, de continuïteit en kwaliteit van de dienstverlening, interoperabiliteit en omkeerbaarheid/overdraagbaarheid). |

13.1 Beheer van informatiebeveiligingsincidenten en -verbeteringen

|  |  |  |
| --- | --- | --- |
| A13.1.1 | ISO 27002-16.1 | De verantwoordelijkheden en de procedures moeten vastgelegd worden inzake de detectie en de behandeling van informatiebeveiligingsincidenten en zwakke plekken rond persoonsgegevens die gerapporteerd worden. |
| B-13.1.1 | ISO 27002-16.1 | Een procedure moet geïnstalleerd worden die toelaat om informatiebeveiligingsgebeurtenissen m.b.t. de gebruikte/verwerkte persoonsgegevens:   * op te sporen; * te beoordelen, en indien van toepassing: * op te volgen; * en te herstellen. |
| A-13.1.2 | ISO 27002-16.1 | Uw organisatie moet er voor zorgen dat de informatiebeveiligingscel/verantwoordelijke voor de verwerking steeds direct op de hoogte gesteld wordt van gebeurtenissen en incidenten die de informatiebeveiliging van persoonsgegevens in het gedrang kunnen brengen of gebracht hebben. |
| B-13.1.2 | ISO 27002-16.1 | De door uw organisatie aangeduide veiligheidsconsulent treedt op als contactpunt voor het opsporen en rapporteren van beveiligingsincidenten. |
| A-13.1.3 | ISO 27002-16.1 | Uw organisatie moet er voor zorgen dat de informatiebeveiligingscel/verantwoordelijke voor de verwerking steeds direct op de hoogte gesteld wordt van de gedetecteerde of vermeende zwakke plekken in de beveiliging in de systemen of de diensten die verband houden met de persoonsgegevensverwerking. |
| B-13.1.3 | ISO 27002-16.1 | Indien een informatiebeveiligingsincident de grenzen van de organisatie overschrijdt moeten alle getroffen externe partijen op een gecoördineerde wijze tijdig en afdoende geïnformeerd worden door de veiligheidsconsulent. |
| A-13.1.4 | ISO 27002-16.1 | Uw organisatie dient te beschikken over een formele en geactualiseerde procedure voor het rapporteren van informatiebeveiligingsgebeurtenissen in combinatie met een reactie- en een escalatieprocedure voor incidenten rond persoonsgegevens. In het geval van een openbaar incident strekt het tot de aanbeveling melding te doen bij de bevoegde instanties conform aanbeveling nr 01/2013 van de Privacycommissie. Meer in het bijzonder geldt, conform de wet van 13 juni 2005 betreffende de elektronische communicatie, de meldingsplicht indien het een openbaar incident betreft in de telecomsector. |
| A-13.1.5 | ISO 27002-16.1 | De informatiebeveiligingscel/verantwoordelijke voor de verwerking moet systematisch geïnformeerd worden over alle maatregelen die genomen worden om aan informatiebeveiligingsincidenten en zwakke plekken rond persoonsgegevens het hoofd te bieden. |

14.1 Informatiebeveiligingscontinuïteit

|  |  |  |
| --- | --- | --- |
| A14.1.1 | ISO 27002-17.1 | Uw organisatie moet op basis van een risicobeoordeling de nodige maatregelen bepalen om de continuïteit van de informatiebeveiliging van persoonsgegevens te waarborgen. |
| B14.1.1 | ISO 27002-17.1 | De nodige procedures moeten geïmplementeerd worden voor het herstel van uw bedrijfsprocessen, het waarborgen van het vereiste niveau van informatiebeveiliging en het opnieuw beschikbaar stellen van de persoonsgegevens binnen een vooraf bepaalde tijdspanne. De procedures kunnen omvatten: procedures voor noodsituaties, uitwijkprocedures, herstartprocedures, …  Deze procedures moeten gedocumenteerd zijn, regelmatig getest en aangepast worden en de betrokken personen moeten opgeleid zijn. De procedures rond bedrijfscontinuïteit dienen eveneens beveiligd te worden tegen lekken en beschadiging gezien de gevoelige informatie die erin aanwezig is (met name hoe de organisatie zal reageren bij een ernstig incident of ramp). |
| B14.1.2 | ISO 27002-17.1 | Uw maatregelen voor de continuïteit van de informatiebeveiliging van persoonsgegevens moeten op regelmatige basis getest en indien nodig geüpdatet worden. |

14.2 Redundante componenten

|  |  |  |
| --- | --- | --- |
| A-14.2.1 | ISO 27002-17.1 | Naargelang de eisen van uw organisatie dienen informatieverwerkende faciliteiten met voldoende redundantie te worden voorzien om de beschikbaarheid van persoonsgegevens te waarborgen. Bijkomende informatiebeveiligingsrisico’s als gevolg van redundantie moeten hierbij in acht te worden genomen. |

15.1 Naleving van wettelijke voorschriften

|  |  |  |
| --- | --- | --- |
| A15.1.1 | ISO 27002-18.1 | Uw organisatie moet steeds alle van toepassing zijnde wetten en regels over de verwerking en de bescherming van persoonsgegevens naleven. Minimaal moeten de bepalingen opgenomen in de wet van 8 december 1992 voor de bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (Privacywet) en haar uitvoeringsbesluit (KB van 13 februari 2001) worden nageleefd. In functie van de gegevensverwerking wordt dit wettelijk kader aangevuld met specifieke wetgeving:   * [*Koninklijk Besluit van 17 december 2003 tot vaststelling van de nadere regels met betrekking tot de samenstelling en de werking van bepaalde sectorale comités opgericht binnen de Commissie voor de bescherming van de persoonlijke levenssfeer*](http://www.privacycommission.be/nl/legislation/national/#N100CE)*;* * [*Wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen*](http://www.privacycommission.be/nl/legislation/national/#N100D9)*;* * [*Wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de Sociale Zekerheid*](http://www.privacycommission.be/nl/legislation/national/#N100F6)*;* * [*Wet van 16 januari 2003 tot oprichting van een Kruispuntbank van Ondernemingen, tot modernisering van het handelsregister, tot oprichting van erkende ondernemingsloketten en houdende diverse bepalingen*](http://www.privacycommission.be/nl/legislation/national/#N10119)*;* * [*Wet van 4 juli 1962 betreffende de openbare statistiek*](http://www.privacycommission.be/nl/legislation/national/#N10144)*;* * *Wet van 13 juni 2005 betreffende de elektronische communicatie;* * *Wet van 15 augustus 2012 houdende oprichting en organisatie van een federale dienstenintegrator;* * *Wet van 5 mei 2014 houdende verankering van het principe van de unieke gegevensinzameling in de werking van de diensten en instanties die behoren tot of taken uitvoeren voor de overheid en tot vereenvoudiging en gelijkschakeling van elektronische en papieren formulieren;* * *Koninklijk besluit van 12 augustus 1993 houdende de organisatie van de informatieveiligheid bij de instellingen van sociale zekerheid;* * *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;* * [*Koninklijk besluit van 7 juni 2007 tot vaststelling van de nadere regels met betrekking tot de samenstelling en de werking van het Statistisch Toezichtscomité opgericht binnen de Commissie voor de bescherming van de persoonlijke levenssfeer*](http://www.privacycommission.be/nl/legislation/national/#N10155)*;* * *Omzendbrief van 9 januari 2002 betreffende de toegang tot de informatiegegevens die in het Rijksregister van de natuurlijke personen opgenomen zijn. Maatregelen ter beveiliging van de gegevens;* * *Omzendbrief van 24 september 2007 betreffende de verplichtingen voor de verantwoordelijken van gegevensverwerking;* * *Omzendbrief van 12 maart 2008 betreffende de bescherming van de persoonlijke levenssfeer t.o.v. de verwerking van persoonsgegevens- Toegang tot de informatiegegevens van het Rijksregister – Veiligheidsmaatregelen die ertoe strekken de vertrouwelijkheid en de integriteit van de gegevens, de authenticatie van de gebruikers en het spoor van de activiteiten die uitgevoerd werden op de informatiesystemen, te waarborgen;* * *Omzendbrief van 10 juli 2008 betreffende de bescherming van de persoonlijke levenssfeer t.o.v. de verwerking van persoonsgegevens -Toegang tot de informatiegegevens van het Rijksregister – Respect voor de doeleinden waarvoor toestemming werd gegeven om toegang te krijgen tot de informatiegegevens in het Rijksregister of om er mededeling van te bekomen.* |
| B15.1.1 | ISO 27002-18.1 | De veiligheidsconsulent communiceert tijdig aan alle personen die betrokken zijn bij het verwerken van persoonsgegevens over de relevante na te leven wet- en regelgeving. |
| A15.1.2 | ISO 27002-17.1 | Voor de Vlaamse steden en gemeenten geldt bijkomend:   * Het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer; * Het besluit van de Vlaamse Regering van 15 mei 2009 houdende uitvoering van het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer; * Het besluit van de Vlaamse regering van 15 mei 2009 betreffende de veiligheidsconsulenten, vermeld in artikel 9 van het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer. |
| B15.1.2 | ISO 27002-17.1 | Gemeenschappelijk systeem voor boekhouding  In geval van externe audit van de boekhouding, is het noodzakelijk dat de gegevens die niet behoren tot de geauditeerde organisatie geanonimiseerd zijn indien deze overgemaakt moeten worden aan de auditeur. |
| A15.1.3 | ISO 27002-17.1 | Uw organisatie moet op een systematische wijze nagaan of een machtiging (al dan niet onder de vorm van een aansluiting) vereist is voor het aanschaffen of ontwikkelen van een systeem dat persoonsgegevens gebruikt/verwerkt. Indien die vereist is moet zij maatregelen nemen om aan alle verplichten te voldoen inzonderheid de melding van de identiteit van de veiligheidsconsulent en de beschrijving van het beveiligingsbeleid ter attentie en door middel van de formulieren voorgeschreven door het instrumenterende sectoraal comité. |
| A15.1.4 | ISO 27002-17.1 | Uw organisatie moet op een systematische wijze nagaan of een machtiging van de VTC vereist is. Indien die vereist is, moet zij maatregelen nemen om aan alle verplichtingen te voldoen inzonderheid de melding van de identiteit van de veiligheidsconsulent en de beschrijving van het beveiligingsbeleid ter attentie en door middel van de formulieren voorgeschreven door de VTC. |
| A15.1.5 | ISO 27002-17.1 | Uw organisatie moet over geactualiseerde procedures beschikken voor de uitwerking en onderhoud van documentatie die betrekking heeft op de verleende machtiging(en). |
| A15.1.6 | ISO 27002-17.1 | Uw organisatie moet over een goedgekeurde aanpak beschikken om na te gaan dat de machtiging gerespecteerd blijft bij iedere wijziging aan de toepassing/applicatie die persoonsgegevens gebruikt/verwerkt waarvoor deze machtiging verleend is. |
| A15.1.10 | ISO-27002-17.1 | Elke stad of gemeente moet de van toepassing zijnde generieke en individuele machtigingen naleven. |
| A15.1.11 | ISO 27002-17.1 | Elke Vlaamse stad of gemeente moet het besluit van de Vlaamse Regering van 15 mei 2009 betreffende de veiligheidsconsulenten, vermeld in artikel 9 van het decreet 189 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer naleven. |
| A15.1.12 | ISO 27002-17.1 | Elke stad of gemeente moet de identiteit van haar veiligheidsconsulent en zijn eventuele adjuncten meedelen aan het Sectoraal Comité van het Rijksregister (zie artikel 10 van het de Rijksregisterwet). |
| A15.1.13 | ISO 27002-17.1 | Elke stad of gemeente moet voorafgaand aan de verplichte aanstelling van haar veiligheidsconsulent en zijn eventuele adjuncten advies vragen aan de VTC. |
| A15.1.14 | ISO 27002-17.1 | Boekhouding  Indien in de boekhouding sociale persoonsgegevens aanwezig zijn (vb. OCMW’s), zijn de minimale normen van het Sectoraal Comité van de Sociale Zekerheid en van de Gezondheid van toepassing. Deze regel blijft gelden in geval van een gemeenschappelijk systeem van boekhouding. |
| A15.1.15 | ISO 27002-17.1 | Gezamenlijk adressenbestand  De algemene regel stelt dat er voor elke uitwisseling van sociale persoonsgegevens een machtiging vereist is van het Sectoriaal Comité van de Sociale Zekerheid en van de Gezondheid en dat die gegevensuitwisseling via de Kruispuntbank van de Sociale Zekerheid moet plaatsvinden.  Dit houdt in dat het gezamenlijk adressenbestand geen enkel sociaal persoonsgegeven mag bevatting zonder machtiging van het Sectoriaal Comité van de Sociale Zekerheid en van de Gezondheid. |
| A15.1.16 | ISO 27002-17.1 | Een machtiging van het Sectoraal Comité van de Sociale Zekerheid en van de Gezondheid is vereist voor de uitwisseling van persoonsgegevens tussen de gemeente/stad en het OCMW. |

15.2 Informatiebeveiligingsbeoordelingen

|  |  |  |
| --- | --- | --- |
| A15.2.1 | ISO 27002-18.2 | Uw organisatie moet op regelmatige basis een degelijke audit organiseren met betrekking tot informatiebeveiliging van persoonsgegevens. Deze audit moet betrekking hebben op de volgende domeinen uit de onderhavige richtsnoeren:   * risicobeoordeling; * beleid i.v.m. informatiebeveiliging; * organisatie van de informatiebeveiliging; * beveiligingsvereisten m.b.t. personeel; * beheer van bedrijfsmiddelen; * logische toegangsbeveiliging; * cryptografische beheersmaatregelen * fysieke beveiliging; * operationeel beheer; * onderhoud en ontwikkeling van informatiesystemen; * informatiebeveiliging in leveranciersrelaties * beheersen van informatiebeveiligingsincidenten; * beheersproces bedrijfscontinuïteit; * naleving. |

