Lokaal bestuur Pepingen

Informatieveiligheidsbeleid

Information Security Management System (ISMS)

Filip Haesen – Data Protection Officer - Welzijnskoepel West-Brabant
16-8-2023

Inhoud

1. Algemeen

1.1 Het belang van Informatieveiligheid

Informatie is een bedrijfsmiddel dat, zoals andere belangrijke bedrijfsmiddelen, een belangrijke waarde vertegenwoordigt en waar dus op gepaste wijze moet mee omgegaan worden. Een beleid voor Informatieveiligheid beschermt deze informatie tegen een brede waaier van bedreigingen om de continuïteit van de organisatie te verzekeren, eventuele schade te beperken en maximaal bij te dragen tot resultaten en opportuniteiten in de dienstverlening.
Informatieveiligheid wordt geschetst als het verzekeren van **vertrouwelijkheid**, **integriteit, beschikbaarheid** en **auditeerbaarheid** met betrekking tot de informatie. Dit geldt voor alle vormen van informatie, zowel in niet-tastbaar (elektronisch) als tastbaar (papier) formaat. Bijkomend zal de Informatieveiligheid middelen aanreiken om vervalste informatie te identificeren en weerlegging van legitieme informatie onmogelijk te maken.
De informatisering van de instellingen van de federale en Vlaamse overheid, alsook de sociale zekerheid en de toenemende samenwerking bieden immers enorme verbeteringen op het vlak van effectiviteit en efficiëntie, maar tegelijkertijd worden er ook nieuwe risico's gelopen. Het onderhouden en verbeteren van de Informatieveiligheid is dus van essentieel belang voor het verzekeren van de naleving van de wet, maar ook voor de continuïteit van de werking van de organisatie en het imago ervan. Informatieveiligheid moet steunen op een lagenmodel waar verschillende maatregelen complementair zijn. De beveiliging die kan bereikt worden met technische middelen is slechts één van die lagen. Ze moet ondersteund worden door een geschikt beheer en een integer gebruik van alle bedrijfsmiddelen. Cruciaal voor een goede informatiebeveiliging is dus ook de deelname van alle personeelsleden van de organisatie en de ondersteuning van het management. Ook de bijdrage van derden (bv. leveranciers, externe medewerkers, …) is belangrijk.
Gebaseerd op de ISO 2700x normen verplicht de federale overheid lokale besturen om de volgende regels m.b.t. informatieveiligheid na te leven :

Voor steden en gemeenten gelden de Richtsnoeren :
https://overheid.vlaanderen.be/digitale-overheid/documenten-vlaamse-toezichtcommissie
Voor OCMW's gelden de KSZ Minimale Normen :
https://www.ksz-bcss.fgov.be/nl/gegevensbescherming/informatieveiligheidsbeleid

1.2 Doelstelling informatieveiligheid bij een bestuur

Informatieveiligheid binnen de organisatie (lokaal bestuur) beoogt de instandhouding en de goede werking van de activiteiten ervan, primair gericht op het voorkomen van schade, met het oog op de realisatie van de doelstellingen zoals vooropgesteld in haar missie.
Meer algemeen heeft ze als doelstelling het voorkomen van schade die kan worden toegebracht aan de goede werking van de informatiesystemen van de organisatie enerzijds en aan de persoonlijke levenssfeer van de betrokkenen anderzijds.
Het streefdoel is een gezond evenwicht tussen een aantal preventieve maatregelen om beveiligingsincidenten te voorkomen en correctieve maatregelen om de negatieve gevolgen van incidenten te beperken. In dit beleid worden de basismaatregelen van de organisatie inzake informatieveiligheid beschreven.

1.3 Wettelijke verplichtingen

De wetgeving in verband met informatieveiligheid evolueert regelmatig. Een laatste stand van zaken is steeds te raadplegen op de websites van de Europese, federale en Vlaamse overheden. De normen in verband met informatieveiligheid evolueren steeds mee met de technologische evolutie en de wetgeving.

2. Reikwijdte

Het **Informatieveiligheidsbeleid** van de organisatie is van toepassing op alle ontwikkelde, operationele en toekomstige informatiesystemen van de organisatie alsook alle daartoe behorende entiteiten (scholen, bibliotheken, academies, culturele centra, woonzorgcentra, sociaal woningverhuur, kinderopvang, dienstencentra,…). Het is ook van toepassing op alle personeelsleden, medewerkers en bestuursleden van de organisatie. Het is tevens van toepassing op alle externe krachten die tijdelijk of voor onbepaalde duur werkzaam zijn binnen of voor de organisatie. Aanvullende maatregelen kunnen toepasselijk zijn op personeelsleden die op semipermanente (deeltijdse) basis afgevaardigd worden naar andere organisaties. Het informatieveiligheidsbeleid is onderdeel van het algemeen ISMS (Information Security Management System) van de organisatie, waarbij alle risico's en kwetsbaarheden m.b.t. gegevensbescherming worden geïdentificeerd, vermeden en geremedieerd.

3. Beleidsmaatregelen

3.1 Beleid voor informatieveiligheid

DOELSTELLING :
De opmaak en het onderhoud van een documentenpakket (informatieveiligheidsbeleid, informatieveiligheidsplan, procedures, etc.), conform aan de vereisten van informatieveiligheid, en de communicatie ervan aan alle betrokken partijen.

a. De Data Protection Officer (DPO) maakt een documentenpakket op, op maat van de organisatie, dat bestaat uit een beleid (dit document), een informatieveiligheidsplan, gedragscodes, procedures en andere documenten zoals bv verder uitgewerkte policies.. Bij specifieke vragen van de organisatie aangaande een problematiek of een situatie betreffende informatieveiligheid kan de DPO adviezen leveren.

3.2 Organisatie van de informatieveiligheid

DOELSTELLING :
Een correcte organisatie en beheer van de informatieveiligheid binnen de organisatie, conform de desbetreffende wetgeving.

a. De organisatie doet beroep op de dienst Informatieveiligheid en de Data Protection Officer (DPO) van de Welzijnskoepel West-Brabant. Deze is middels een raadsbeslissing en kennisgeving aan de toezichthoudende autoriteit aangesteld voor de organisatie.

b. De DPO van Welzijnskoepel West-Brabant zorgt voor de sturing, opstelling en herziening van het beleid, bijstelling van de beleidsmaatregelen, opstelling van het informatieveiligheidsplan, opstelling van de vereiste en benodigde policies en procedures, de vaststelling van verantwoordelijkheden en het toezicht op veranderde wetgeving, bedreigingen en incidenten.

c. De uitvoering van het informatieveiligheidsbeleid moet opgevolgd worden door de informatieveiligheidscel (IVC) geleid door de DPO. De informatieveiligheidscel heeft een adviserende, stimulerende, documenterende en controlerende opdracht binnen de organisatie.

   Daartoe moet de DPO 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.

d. Het beleid, de bijhorende policies en procedures worden regelmatig geëvalueerd en eventueel aangepast. Belangrijke wijzigingen worden steeds bekend gemaakt.

e. Het informatieveiligheidsplan, dat de evolutie van de veiligheidsmaatregelen weergeeft, wordt ten minste elke 3 jaar opnieuw grondig geëvalueerd. Belangrijke wijzigingen worden steeds bekend gemaakt.

f. Alle verwijzingen naar documenten en procedures vanuit het informatieveiligheidsbeleid (dit beleid) bij de uitvoering van het Information Security Management System (ISMS), maken hiervan integraal onderdeel uit. Deze documenten en procedures kunnen een verdere en meer gedetailleerde beschrijving of uitwerking zijn voor specifieke onderdelen, of een aanvulling vormen bij de uitvoering van dit beleid. Deze documenten en procedures worden tevens geactualiseerd naargelang technologische en organisatorische ontwikkelingen.

g. De organisatie verbindt er zich toe de DPO te voorzien van de noodzakelijke informatie, zodanig dat hij over de nodige gegevens kan beschikken die nodig zijn voor het uitvoeren van zijn opdracht.

h. Bijzondere aandacht wordt besteed aan de organisatorische aspecten van de samenwerking met derden (bv. uitbesteding van taken). De veiligheidsaspecten van de samenwerking worden contractueel vastgelegd.

i. In het kader van de fysieke beveiliging en de beveiliging van de omgeving dienen de informatieveiligheidsdienst en de dienst arbeidsveiligheid (de preventieadviseur) met elkaar samen te werken.

j. In het kader van het operationeel beheer, de logische toegangsbeveiliging en de ontwikkeling en onderhoud van systemen dienen de DPO en de systeembeheerders (informatici, …) nauw met elkaar samen te werken.

k. Het beheer van toegangen naar online toepassingen van de Vlaamse en federale overheden is volledig in handen van de organisatie. Alle aanpassingen betreffende toegangen op deze portalen worden overzichtelijk geregeld en gedocumenteerd, onder verantwoordelijkheid van de algemeen directeur en/of diens adjunct. Verder wordt er een inventaris bijgehouden van alle rollen en verantwoordelijkheden. Op vraag van de organisatie kan de DPO een rol opnemen aangaande het toegangsbeheer.

l. De organisatie beschikt over een beslissingsplatform voor de validatie en goedkeuring van informatieveiligheidsmaatregelen, dat ervoor zorgt dat maatregelen ondersteund kunnen worden en op een gecoördineerde manier uitgevoerd kunnen worden.

m. De DPO neemt deel aan de overlegvergaderingen van de VVSG (Vereniging van Vlaamse steden en gemeenten), KSZ (Kruispuntbank Sociale Zekerheid) , POD-mi,….. en koppelt alle nodige en belangrijke informatie terug naar de organisatie.

4. Informatieveiligheid voor de personeelsleden

DOELSTELLING :
Het zo goed mogelijk benutten en op het vereiste niveau houden van de kennis en de bewustwording van de personeelsleden ter bevordering van de beveiliging, evenals het verminderen van de risico's te wijten aan al dan niet opzettelijk menselijk falen.

a. Personeelsleden moeten zich bewust zijn van de bedreigingen via communicatie- en informatiesystemen en van het belang van informatieveiligheid. Ze moeten daartoe de juiste middelen, kennis en vaardigheden tot hun beschikking hebben.

b. Personeelsleden worden voldoende op de hoogte gebracht van de veiligheidsmaatregelen bij het gebruik van communicatie- en informatiemiddelen die zij verwacht worden te treffen. De DPO staat steeds ter beschikking voor vragen en bijkomende uitleg.

c. De DPO stuurt op regelmatige basis informatie rond, om informatieveiligheid onder de aandacht te houden. Er kunnen ook folders en affiches ter beschikking worden gesteld.

d. Het personeelsbeleid van de organisatie draagt bij door de opname van veiligheidsaspecten en de verantwoordelijkheid van de werknemer op het gebied van informatieveiligheid op te nemen in de deontologische code en/of het arbeidsreglement of verwijzingen te maken naar het informatieveiligheidsbeleid en bijhorende documenten.

e. Elke medewerker heeft de plicht beveiligingsrisico's en beveiligingsincidenten te melden aan zijn leidinggevende, ICT dienst, DPO of aan de informatieveiligheidscel. Afhankelijk van de graad van het incident (datalek) wordt de toezichthoudende autoriteit ingelicht.

f. Personeelsleden worden gewezen op hun eigen verantwoordelijkheid voor het handhaven van een effectieve toegangsbeveiliging, met name het gebruik van wachtwoorden en beveiliging van gebruikersapparatuur en voor de toepassingen. Wachtwoorden zijn strikt persoonlijk en vertrouwelijk. Zie hiervoor het document "Beleid authenticatie en logisch toegangsbeheer" dat kadert in het informatieveiligheidsbeleid van de organisatie.

g. Men moet er zich steeds bewust van zijn welke informatie men aan wie kan en mag doorgeven. Controleer steeds of de aanvrager wel degelijk recht heeft op de informatie.

h. Wanneer men gebonden is aan het beroepsgeheim en/of de discretieplicht dient men zich hier steeds aan te houden. Zie hiervoor de deontologische code die kadert in het informatieveiligheidsbeleid van de organisatie.

i. Personeelsleden worden gewezen op de veiligheidsrisico's die elektronische systemen met zich meebrengen (vaste computers, mobiele computers, telefoons, mobiele telefoons, smartphones, tablets, e-mail, post, messaging, voicemail, postdiensten, fax, enz.). Deze systemen houden een risico in voor de vertrouwelijkheid van informatie.

j. Het gebruik van bedrijfsmiddelen voor privédoeleinden moet tot een strikt minimum beperkt blijven.

k. Op apparatuur die verbonden is met de infrastructuur en/of netwerk van de organisatie (bv desktop, laptop) mag alleen hardware aangesloten worden en/of software geïnstalleerd worden en/of configuraties ingesteld worden door de bevoegde diensten aangesteld door de organisatie. De gebruiker mag niet in staat gesteld worden om zelf programma's te installeren of te wijzigingen, of aanpassingen uit te voeren aan de beschikbaar gestelde apparatuur.

l. De personeelsleden zorgen ervoor dat hun computers na het beëindigen van de dagtaak steeds uitgezet worden. Het is niet voldoende dat het personeelslid afmeldt, of het toestel in slaapmodus wordt gebracht. Bij gebruik van 'Remote Desktop Services' zorgt het personeelslid er steeds voor dat de sessie afgemeld wordt na gebruik, of dat er een automatische afmelding voorzien wordt. Bij het gebruik van een thin-client wordt deze na het beëindigen van de taken uitgezet.

m. Bij indiensttreding wordt een onthaaldocument of -map voorzien en overhandigd aan het nieuwe personeelslid waarin de omgang en het gebruik met ICT materiaal van de organisatie beschreven wordt.

n. Toegangsrechten en autorisaties voor nieuwe personeelsleden worden door middel van een procedure afgehandeld. Het toekennen van toegangsrechten en autorisaties gebeurt in overleg met de betrokken dienst- of afdelingshoofden.

o. Bij het verlaten van de dienst of bij wijziging van functie-inhoud worden toegangsrechten en autorisaties van de personeelsleden zo vlug mogelijk aangepast in gezamenlijk overleg met de afdelings- of diensthoofden. Materiaal voor fysieke toegangen (sleutels, badge, toegangscodes, …) worden, indien nodig, gerecupereerd of afgesloten.

p. De schending van het informatieveiligheidsbeleid en de beveiligingsprocedures van de organisatie worden door middel van een formeel proces afgehandeld.

q. Vertrouwelijke of persoonlijke gesprekken worden steeds gevoerd met aandacht voor de omgeving. Wanneer men cliënten ontvangt of discrete gesprekken voert, intern of met eventuele bezoekers, dan gebeurt dit in daarvoor voorziene ruimtes die de privacy garanderen.

r. Gezamenlijk overleg wordt zo gepleegd dat enkel de betrokken personeelsleden het gesprek kunnen meevolgen.

5. Mobiele apparatuur en telewerken

DOELSTELLING :
Gepaste maatregelen treffen voor de organisatie van de online-toegang van buiten de organisatie tot de interne - en persoonsgegevens van de organisatie en de informatie op mobiele dragers beschermen.

a. Personeelsleden kunnen in principe géén gebruik maken van eigen ICT middelen bij het uitvoeren van hun professionele opdrachten. De organisatie kan, naargelang de situatie, beslissen vergoedingen voor personeelsleden of mandatarissen voor de aankoop of gebruik van eigen ICT middelen toe te kennen, en/of hiervoor in een abonnement te voorzien. Hierbij dient rekening te worden gehouden met de taken, functie of noden van bereikbaarheid. Het beleid betreffende mobiele toestellen voor personeelsleden en mandatarissen is beschreven in de policy “Mobile devices” en - indien van toepassing - de policy “BYOD” (bring your own device).

b. De online-toegang van buiten de organisatie naar de toepassingen en bestanden op het netwerk van de organisatie (Remote Desktop of VPN) wordt enkel geregeld via een beveiligde en versleutelde verbinding (https/ssl/IPSec). Het certificaat zal worden uitgegeven door een CA (Certificate Authority). Rechtstreekse externe toegang via een afstandsbedieningssessie door een personeelslid naar een computer van de organisatie is niet toegestaan, uitgezonderd een sessie door de eigen ICT dienst voor ICT ondersteunende taken. Het gebruik van ‘Remote Control Software’ en VPN is enkel toegestaan voor de uitvoering van professionele opdrachten.

c. Personeelsleden en/of mandatarissen die gebruik maken van laptop of andere mobiele toestellen van de organisatie gaan hier zorgvuldig mee om. Personeelsleden dienen steeds alle mogelijke maatregelen te treffen om verlies en beschadiging van ICT apparatuur alsook informatieverlies te voorkomen. Er dient een effectieve toegangsbeveiliging toegepast te worden op alle mobiele toestellen (zie hiervoor het document “Beleid authenticatie en logisch toegangsbeheer”). De toestellen mogen niet gebruikt worden door derden. Gebruikers dienen steeds al het mogelijke te doen om te verhinderen dat derden ongeoorloofde toegang zouden verkrijgen tot de toestellen of tot de informatie die ermee geraadpleegd wordt.

d. Het gebruik van eigen externe opslagmedia (USB, disk, smartphone,…) alsook het gebruik van enig andere externe clouddienst (Dropbox, Google Drive, Microsoft OneDrive, enz) vreemd aan de eigen organisatie, voor de opslag van informatie behorend tot de organisatie is niet toegelaten. Indien noodzakelijk stelt de organisatie externe media met – indien mogelijk - een beveiligde partitie ter beschikking. Deze media worden uitgeleend bij de interne uitleendienst. Documenten aangeleverd via externe media, ftp(s) diensten, of via beveiligde online transferdiensten van vertrouwde partners worden eerst gescand op malware vóór gebruik. De uitwisseling van persoonsgegevens via deze methoden moet, waar mogelijk, tot een minimum beperkt blijven. Documenten die op deze wijze digitaal uitgewisseld worden ook eerst gescand op malware vóór gebruik.

e. De organisatie kan d.m.v. een uitleendienst mobiele toestellen (laptops, smartphones, tablets) beschikbaar stellen aan het personeel (gebruik voor korte termijn) en mandatarissen indien deze vereist zijn voor het uitvoeren van een specifieke taak. Na uitvoering van de taak worden de toestellen terug gebracht naar de uitleendienst. Het personeelslid of mandataris waakt erover dat er geen (persoons)gegevens bewaard zijn op deze mobiele toestellen. Deze uitleendienst houdt een nauwkeurig register bij van de toestellen die uitgeleend worden, alsook de tijdstippen van uitlening.

f. Het scannen of fotograferen van documenten behorende tot de organisatie met persoonlijk fotomateriaal is niet toegestaan.

6. Beheer van bedrijfsmiddelen

DOELSTELLING :
Het handhaven van een gepaste bescherming voor alle bedrijfsmiddelen.

a. Er worden up-to-date inventarissen bijgehouden van de belangrijkste hard- en software.
Bij voorkeur beschikt de organisatie hiervoor over een softwaretool. In het andere geval kan dit d.m.v. het gebruik van een manueel opgesteld overzicht.

b. Het gebruik van bedrijfsmiddelen en de toegang tot informatie en informatiesystemen worden beperkt door toegangs- en autorisatierechten, zowel fysiek als logisch.

c. Er wordt rekening gehouden met het feit dat binnen de context van het Rijksregister en KSZ omgegaan wordt met vertrouwelijke gegevens. De behandeling van deze gegevens is onderworpen aan de Algemene Verordening Gegevensbescherming (General Data Protection Regulation - GDPR), in voege getreden op 25 mei 2018.

d. Er worden gedragscodes (policies) opgesteld en onderhouden voor het correct gebruik van internet en e-mail. De maatregelen uit deze policies worden correct gecommuniceerd naar alle betrokkenen. De DPO staat steeds ter beschikking voor vragen en bijkomende uitleg. Zie hiervoor de “Internet en e-mail policy”.

e. Alle gebruikers dienen zich bewust te zijn van het feit dat de toegang tot het internet gefilterd, gecontroleerd, opgeslagen en geanalyseerd kan worden in overeenstemming met de ter zake geldende wetgeving en arbeidsreglement of deontologische code. Zie hiervoor de bepalingen opgenomen in de “Internet en e-mail policy”.

f. Er wordt een *‘clear-screen’* beleid toegepast op alle gebruikerscomputers van de organisatie. Wanneer men de werkplaats voor enige tijd verlaat, moet men erop toezien de computer te vergrendelen of ~~om~~ af te melden. Het is aangewezen om alle computers via een centraal beleid na een vooraf ingesteld tijd automatisch te vergrendelen. Het ontgrendelen van de computer gebeurt nadien terug door het opnieuw ingeven van de eigen gebruikersnaam en wachtwoord.

g. Wanneer men cliënten of bezoekers ontvangt, zorgt men dat deze niet onbedoeld kunnen meekijken op het scherm. Indien nodig draait men de monitor weg van de cliënt of bezoeker, of men vergrendeld het scherm wanneer men deze even onbeheerd achterlaat.

h. Er wordt een '*clean-desk*' mentaliteit toegepast op alle werkplaatsen. Dossiers met persoonsgegevens die niet in behandeling zijn, worden bewaard in een afsluitbare kast. Dossiers die in behandeling zijn worden na de werkuren opgeborgen in een afsluitbare kast of lokaal. Wanneer men het bureau verlaat, of wanneer men cliënten ontvangt, worden alle verwijzingen naar persoonsgegevens (i.e. namen op kaften, ingevulde formulieren, …) zorgvuldig uit het zicht verwijderd.

i. Vertrouwelijke of persoonlijke telefoongesprekken worden steeds gevoerd met aandacht voor de omgeving. Het baliepersoneel schakelt liefst geen gesprekken door wanneer het betrokken personeelslid in gesprek verkeert met een cliënt (of men vraagt tenminste of het gesprek kan aangenomen worden). Wanneer een vertrouwelijk telefoongesprek gevoerd moet worden, sluit men best de deur of begeeft men zich naar een aparte ruimte. Indien er onverwachts toch andere personen in de buurt zijn, probeert men het gesprek zo discreet mogelijk te voeren (bv. geen namen noemen, …).

j. Alle digitale bestanden worden steeds bewaard in de daarvoor bestemde netwerkmappen of bibliotheken (libraries). Deze mappen of bibliotheken worden volgens inhoud en per dienst gescheiden. Enkel de personeelsleden van de desbetreffende dienst of met bevoegdheid mogen toegang hebben tot de overeenkomstige mappen of bibliotheken. De personeelsleden hebben enkel toegang naar de netwerkmappen of bibliotheken die vereist zijn voor het vervullen van hun taken en functie binnen de organisatie. De algemeen directeur en diens back-up hebben het recht op toegang tot alle dienst-, project-, applicatiemappen of bibliotheken.

k. Bij het afdrukken van documenten worden deze documenten onmiddellijk door het personeelslid opgehaald. Indien de functionaliteit beschikbaar is, wordt het personeel gestimuleerd om uitgesteld en/of beveiligd af te drukken. Verdwaalde documenten (ook faxen) worden in de juiste postbakjes gelegd. Er blijven geen afgedrukte documenten rond de printers rondslingeren.

l. Bij het scannen van documenten naar een publieke map, zorgt men ervoor dat deze informatie niet ongewild in deze map blijft staan. Deze documenten in een publieke map worden onmiddellijk verplaatst naar een afgeschermde netwerklocatie, of worden na een vooraf ingestelde tijd automatisch verwijderd. Men kan scannen naar het eigen e-mailadres om te voorkomen dat gevoelige informatie bij iemand anders terechtkomt of onderschept wordt.

m. Alle papieren documenten die persoonsgebonden of persoonsgegevens bevatten worden, alvorens deze weg te gooien, versnipperd of gecontroleerd vernietigd. Men laat geen documenten die persoonsgegevens bevatten rondslingeren in een prullenmand of papierbak.

n. Er wordt een algemeen beleid ontwikkeld betreffende de levenscyclus van hard- en software. Systemen of toepassingen die niet meer op een afdoende manier kunnen beschermd worden tegen mogelijk kwaadwillige invloeden worden buiten werking gesteld of vervangen door nieuwere en beter beschermde systemen of toepassingen.

7. Logische toegangsbeveiliging

DOELSTELLING :
Het beheren van de toegang tot informatie in overeenstemming met de functionele behoeften en beveiligingseisen.

a. Er wordt rekening gehouden met het feit dat, binnen de context van het Rijksregister en de KSZ omgegaan wordt met vertrouwelijke gegevens en dat de gepaste beperking van toegang tot informatie van het allergrootste belang is.

b. Functionele eisen voor toegangsbeveiliging (identificatie, authenticatie en autorisatie) worden correct toegepast.

c. Er wordt een procedure vastgelegd om alle fases in de levenscyclus van een autorisatie te beheren (vb. creatie, wijziging, controle, opheffing). Zie hiervoor de procedure “In- en uitdiensttreding”.

d. Authenticatie wordt beheerd aan de hand van een formeel proces, beschreven in het document “Beleid authenticatie en logisch toegangsbeheer” dat kadert in het informatieveiligheidsbeleid van de organisatie.

e. Er wordt steeds een overzicht of inventaris bewaard met accounts naar toepassingen en bestandssystemen. Dit overzicht kan worden uitgebreid naar specifieke rechten voor toepassingen, bestandssystemen en bibliotheken (libraries).

f. De toewijzing en het gebruik van beheerdersprofielen, speciale en kritieke bevoegdheden worden beperkt en gecontroleerd. Specifieke maatregelen worden uitgewerkt voor de toegangsbeveiliging voor beheerders van besturingssystemen en toepassingen (administratorrechten).

g. Bijzondere aandacht wordt besteed aan de beveiliging van de toegang voor diagnose en hulp op afstand. Er wordt een historiek (logging) bijgehouden voor dergelijke interventies. Externe partners dienen de organisatie op de hoogte te brengen vooraleer interventies op afstand uitgevoerd worden.

h. Gebruikers worden gewezen op hun verantwoordelijkheid voor het handhaven van een effectieve toegangsbeveiliging, met name met betrekking tot het gebruik van wachtwoorden en beveiliging van gebruikersapparatuur. Wachtwoorden zijn strikt persoonlijk en vertrouwelijk.

i. Toegangen tot interne en externe netwerkdiensten worden op afdoende manier beschermd, via een beheersysteem (rechten) eigen aan het bestuurssysteem of toepassing.

j. Toegang en gebruik van systemen wordt gemonitord om afwijkingen van het toegangsbeleid of anomalieën te detecteren.

k. Voor toegang op afstand worden de noodzakelijke veiligheidsmaatregelen genomen in overeenstemming met de risico's verbonden aan deze manier van werken.

l. Voor gebruik van mobiele opslagmedia die de beveiligingsperimeter van de instelling kunnen verlaten, worden gepaste veiligheidsmaatregelen genomen.

8. Cryptografie

DOELSTELLING :
Het ontwikkelen van een cryptografisch beleid en de gepaste en noodzakelijke maatregelen nemen wanneer de vertrouwelijkheid van informatie van belang is.

a. Het internetportaal van de organisatie (website) wordt versleuteld (SSL encryptie), voorzien van een certificaat uitgegeven door een Certificate Authority (CA). Dit geldt specifiek voor het e-loket waarbij een burger of cliënt online aanvragen kan indienen, aangiften meedelen en attesten kan opvragen.

b. Tenminste alle extern toegankelijke en interne webapplicaties van de organisatie waarbij mogelijkheden bestaan tot gegevensuitwisseling, zullen worden voorzien van versleuteling (SSL encryptie). Hiervoor zal de webtoepassing voorzien worden van een certificaat, uitgegeven door een Certificate Authority (CA).

c. De organisatie zal, in het geval van gegevensuitwisseling via een webtoepassing aangeboden wordt door een externe partij , uitsluitend dergelijke webtoepassingen gebruiken indien deze voorzien zijn van een certificaat, uitgegeven door een Certificate Authority (CA).

d. Mobiele toestellen (laptops) die gegevens van de organisatie kunnen bevatten en die de veiligheidsperimeter van de organisatie kunnen verlaten, worden beschermd door algemene versleuteling (encryptie) van de gegevensdrager. De ICT dienst is verantwoordelijk voor de versleuteling. De sleutels om de versleuteling te activeren of te deactiveren worden op een afgeschermde plaats bewaard bij de ICT dienst.

9. Fysieke beveiliging en beveiliging van de omgeving

DOELSTELLING :
Onbevoegde of onnodige fysieke toegang tot informatie en informatiesystemen voorkomen (dit ter beperking van onbevoegde kennisneming, vervalsing of diefstal van informatie) en schade aan of hinderlijke storing van informatiesystemen voorkomen.

a. Bij integratie van andere diensten in het gebouw wordt er rekening gehouden met het verhoogde risico op onbevoegde toegang. De nodige maatregelen worden getroffen om geen onbevoegde toegangen te verlenen.

b. De ramen en deuren van alle lokalen worden na de werkdag steeds afgesloten. Lokalen worden afgesloten indien mogelijk. Ieder personeelslid is verantwoordelijk voor het correct afsluiten van zijn eigen opbergruimten, kasten en bureel. Betreffende de gezamenlijke ruimtes, de afsluiting van het gebouw en het activeren van het alarm wordt een verantwoordelijke aangeduid of worden er afspraken gemaakt.

c. Tijdens de openingsuren bewaart het baliepersoneel het overzicht over wie het gebouw betreedt. Alle bezoekers moeten zich steeds aanmelden alvorens ze zich naar hun afspraak kunnen begeven. Alle bezoekers worden steeds afgehaald en begeleid door een personeelslid tijdens het bezoek. Bij het beëindigen van de afspraak wordt elke bezoeker tevens naar de uitgang begeleid. Indien mogelijk wordt een bezoekersregister bijgehouden.

d. Alle gebouwen van de organisatie zijn beveiligd met een inbraak- en beveiligingssysteem. Deze gebouwen zijn, indien mogelijk, opgedeeld in verschillende zones met eigen toegangsbeheer als maatregel tegen onbevoegde toegang. Personeelsleden hebben toegang tot de gebouwen (binnen en buiten de openingsuren) door middel van een elektronisch toegangssysteem, of een persoonlijke- , of een elektronische sleutel of badge. De elektronische toegangscodes worden op regelmatige tijdstippen veranderd.

e. Tijdens vergaderingen, bijeenkomsten enz. buiten de openingsuren wordt erop gelet dat alle toegangen naar de gebouwen of kantoren afgesloten zijn tegen mogelijke indringing.

f. Personen die een afspraak hebben buiten de openingsuren, worden binnengelaten door iemand van het personeel en naar hun afspraak begeleid. Men verzekert zich ervan dat alle bezoekers het gebouw nadien ook effectief verlaten.

g. Bij het opmerken van “verdwaalde” personen, probeert men te voorkomen dat deze personen ergens terecht komen waar ze niet moeten zijn. Een simpele “*Kan ik u helpen ?*” doet wonderen.

h. Worden er personen aangetroffen waar ze niet horen, dan wordt hen vriendelijk maar kordaat duidelijk gemaakt dat zij zich moeten verwijderen.

i. De lokalen waarin zich informatiesystemen (serverlokaal) bevinden worden steeds op afdoende wijze afgesloten. De toegang tot de lokalen met informatiesystemen wordt beperkt en is enkel toegankelijk voor bevoegd personeel.

j. Voor de gebouwen worden er gepaste maatregelen genomen om bescherming te bieden tegen brand, waterschade, diefstal en andere fysieke bedreigingen.

k. De IT infrastructuur (servers, disk units, switches, routers,…) wordt beschermd tegen onverwachte stroomonderbrekingen door middel van een noodvoeding of een alternatieve stroomvoorziening.

l. Gegevens op opslagmedia worden permanent gewist of ontoegankelijk gemaakt alvorens de media uit dienst te stellen, te verwijderen of te hergebruiken (bv multifunctionele printers).

10. Operationeel beheer

DOELSTELLING :
Het garanderen van een correcte en veilige bediening en werking van ICT-voorzieningen.

a. Er moet rekening gehouden worden met het feit dat, naarmate de zichtbaarheid van de elektronische toepassingen van de Vlaamse en/of federale overheid toeneemt, ook het risico op aanvallen op het systeem toeneemt.

b. Bij uitbesteding van ICT-activiteiten naar een extern bedrijf, wordt extra aandacht besteed aan eventuele beveiligingsrisico's. De beveiligingsmaatregelen bij uitbesteding worden contractueel vastgelegd.

c. Door gepaste capaciteitsplanning en acceptatieprocedures (change management) voor nieuwe of wijzigingen in ICT-systemen, wordt het risico van systeemstoringen tot een minimum beperkt.

d. Er worden maatregelen genomen om potentiële aanvallen met kwaadwillige software en malware (virus, spam, hacking,…) te voorkomen, snel te ontdekken en de eventuele gevolgen ervan zo veel mogelijk in te perken. De endpoint protection wordt nauwkeurig up-to-date gehouden en gecentraliseerd beheerd. Software en toepassingen voor de algemene bescherming van personal computers en servers mogen nooit uitgeschakeld worden zonder toestemming van een bevoegde ICT verantwoordelijke of ICT beheerder.

e. Er worden proactieve maatregelen genomen en een beleid wordt ontwikkeld om gekende kwetsbaarheden in systemen en toepassingen te voorkomen. Indien systemen of toepassingen kunnen uitgerust worden met de laatste releases of upgrades, dan worden deze, na (interne) evaluatie, zo snel als mogelijk toegepast. Externe ICT dienstenleveranciers dienen steeds het de organisatie op de hoogte te brengen via de interne ICT dienst, voorafgaand aan de uitvoering van de geplande werken.

f. De mogelijkheid wordt geboden aan bezoekers en gasten van de organisatie om zich met persoonlijke of eigen bedrijfstoestellen te connecteren met het internet via een gasten- of bezoekersnetwerk. Dit netwerk dient volledig gescheiden te zijn van het interne netwerk van de organisatie. Enkel externe personen gemachtigd door de organisatie, mogen een verbinding maken met eigen of hun bedrijfstoestellen op het interne netwerk in het kader van de taken die zij dienen uit te voeren voor de organisatie (bv externe ICT beheerders).

g. Op werkdagen worden minstens dagelijks back-ups gemaakt van alle essentiële gegevens (fileserver, database,…). Indien mogelijk worden meerdere back-up sets aangemaakt. Dit verhoogt aanzienlijk de kans op gegevensrecuperatie bij technische storingen of cyberincidenten. Het resultaat van elke back-up job wordt telkens gecontroleerd. Back-up problemen worden zo snel als mogelijk opgelost om de integriteit, beschikbaarheid en continuïteit van de diensten te handhaven. Ten minste 1 back-up set wordt bewaard op een beveiligde locatie (fysieke en/of logisch), op voldoende afstand en op een plaats verschillend van de systemen die back-upt worden.

h. Speciale aandacht wordt besteed aan de beveiliging van informatie in netwerken buiten de bescherming van de eigen infrastructuur. Maximale beveiligingsmaatregelen worden genomen bij het verzonden/ontvangen van gevoelige gegevens via openbare netwerken zoals het internet.

i. Wachtwoorden opgeslagen op ICT systemen (PC, server, externe disk, USB,…) worden steeds met maximale bescherming bewaard. Bescherming kan o.a. via het gebruik van een wachtwoordkluis of document bescherming (wachtwoord). Het bewaren en noteren van wachtwoorden op papier of in browsers moet vermeden worden. De gebruiker of eigenaar van het wachtwoord zorgt ervoor dat het wachtwoord niet zichtbaar kan gemaakt worden. Er wordt nauwlettend, discreet en gecontroleerd gewaakt over het beheer van wachtwoorden voor beheerdersfuncties.

j. Externe opslagmedia worden beveiligd tegen schade, diefstal en ongeoorloofde toegang.

k. Met het oog op de naleving van de wettelijke bepalingen op de bewaring en het gebruik van gearchiveerde gegevens, moet bij elke evolutie van de informatica-infrastructuur en het informatiesysteem nagegaan worden of de gearchiveerde gegevens, de opslagmedia en de noodzakelijke applicaties nodig voor hun exploitatie, op elkaar afgestemd blijven.

l. Maatregelen worden genomen om te voorkomen dat informatie die wordt uitgewisseld met andere organisaties, verloren gaat, gewijzigd of misbruikt wordt.

m. Aandacht wordt besteed aan het beschermen van de integriteit van informatie op publiek toegankelijke systemen (zoals eigen websites) om ongeoorloofde wijzigingen te voorkomen die de organisatie zou kunnen schaden. Ongeoorloofde wijzigingen moeten worden voorkomen die de organisatie of één van de organisaties, in het kader van de uitvoering van hun opdrachten, zouden kunnen schaden.

n. Er wordt een beleid ontwikkeld bij de uitdienststelling van computermateriaal en gegevensdragers. Er wordt voor gezorgd dat gegevens op de gepaste en veilige manier verwijderd worden van servers, personal computers, mobiele gegevensdragers en multifunctionele printers.

o. De organisatie bepaalt en voorziet in eigen communicatiemiddelen voor de uitwisseling van gegevens door personeelsleden en medewerkers (inclusief mandatarissen) met externe partijen. Alle professionele communicatie dient uitsluitend te gebeuren via deze communicatiemiddelen. Elke uitzondering hiervan zal voorafgegaan worden door een gezamenlijk overleg binnen de eigen organisatie en kan niet op eigen initiatief van personeelsleden of medewerkers opgestart worden.

p. In het geval een nieuwe of een bepaalde verwerking van persoonsgegevens een waarschijnlijk hoog risico met zich meebrengt voor de rechten en vrijheden van de betrokkenen, zal het bestuur een gegevensbeschermingseffectbeoordeling / Data Protection Impact Assessment (GEB/DPIA) uitvoeren. De risicobeoordeling zal per geval afzonderlijk plaatsvinden voor de bepaalde verwerking of voorafgaandelijk aan de aanvang van de nieuwe verwerking. Het uitvoeren van een gegevensbeschermingseffectbeoordeling is een verplichting volgens de GDPR.

11. Communicatiebeveiliging

DOELSTELLING :
Gepast beheer van de netwerken op gebied van veiligheid en beschikbaarheid.

a. Elk netwerk behorend tot de organisatie (administratief centrum, OCMW & WZC, scholen & CVO, bibliotheken, cultureel centrum, …) wordt beschermd door een firewall (bij voorkeur met IDS / IPS) en wordt correct geconfigureerd. Hiermee wordt het netwerk van de organisatie afdoende beschermd tegen softwarematige inbraken of aanvallen en diefstal van informatie. Elke firewall beschikt over een historiek (logging) van het in- en uitgaand dataverkeer. Een analyse van het in- en uitgaand dataverkeer kan worden uitgevoerd. In het geval van een gedeelde ICT infrastructuur voor verschillende entiteiten wordt een centrale firewall geïmplementeerd voor de betrokken entiteiten. Optioneel wordt, in het geval van een gedeelde ICT infrastructuur tussen entiteiten een firewall cluster (high availability) geïmplementeerd voor de entiteiten. Deze opstelling garandeert een redundante internetverbinding.

b. In het geval van een gedeelde ICT infrastructuur (netwerk, server) tussen entiteiten moeten de specifieke gegevens voor elk entiteit (bv gemeente en OCMW) strikt gescheiden worden gehouden (Richtsnoeren en KSZ Minimale Normen). Een uitzondering kan worden gemaakt voor geïntegreerde diensten (decreet lokaal bestuur) over de entiteiten (bv personeelsdienst).

c. Er wordt een webfilter (geïntegreerd in firewall) of proxyserver geconfigureerd die het mogelijk maakt om de toegang naar bepaalde websites of web categorieën te beheren of te beperken. Dit voorkomt opzoekingen of consultaties door personeelsleden die niet gerelateerd of noodzakelijk zijn voor de uitvoering van hun opdrachten.

d. Er worden specifieke maatregelen genomen voor de beveiliging van vertrouwelijke informatie en de integriteit bij het verzenden en ontvangen van gegevens over publieke netwerken. Dit gebeurt door middel van VPN (Virtual Private Network) Webservers die extern bereikbaar zijn worden uitgerust met een certificaat (versleuteling van gegevens bij communicatie).

e. Externe digitale dienstenleveranciers (bv ICT) kunnen, voor het uitvoeren van hun ondersteuningsopdrachten en taken, uitsluitend gebruik maken van methodes voorzien van een sterke communicatie en accountbeveiliging bv. beveiligde VPN verbinding, secure remote desktop… Voor externe toegangen is een sterke authenticatie een absolute vereiste. Externe toegangen kunnen niet gedeeld worden over verschillende organisaties en dienen, waar mogelijk, persoonsgebonden zijn. De organisatie inventariseert en behoudt een nauwkeurig toezicht op deze toegangen, zoals voorgeschreven in de NIS2 richtlijn.

12. Verwerving, ontwikkeling en onderhoud van systemen

DOELSTELLING :
Het verzekeren van de vereiste beveiliging in verband met de gebruikte systemen en dit gedurende de volledige levenscyclus. Het bestuur verwacht het naleven van deze norm tevens van zijn softwareleveranciers.

a. Voor nieuwe systemen of uitbreidingen van bestaande systemen dienen de veiligheidsvereisten gespecificeerd te worden aan de uitvoerders of ontwikkelaars van deze systemen.

b. De ontwikkeling van toepassingssoftware wordt gebaseerd op een gestructureerde aanpak die de veiligheidsvereisten oplegt. *(Niet van toepassing)*

c. Bij de ontwikkeling van toepassingssoftware dient bijzondere aandacht besteed te worden aan de validatie van invoergegevens, de beveiliging van interne verwerking en de validatie van uitvoergegevens. *(Niet van toepassing)*

d. Maximale maatregelen worden genomen om te vermijden dat geheime communicatiekanalen in systemen (door de ontwikkelaars van deze systemen) verborgen worden. Een controle door nazicht van software door een 3e partij is een methode om deze risico's te bepalen of in te perken. *(Niet van toepassing)*

e. Bij de ontwikkeling van toepassingssystemen moet rekening worden gehouden met gekende zwakke punten op gebied van veiligheid, eigen aan programmeertalen. Een controle door nazicht van software door een 3e partij is een methode om deze risico's te bepalen of in te perken. *(Niet van toepassing)*

f. Het beschermen van de vertrouwelijkheid, de authenticiteit en de integriteit van de informatie steunt op gepaste cryptografische beveiligingsmaatregelen (versleuteling, digitale handtekening, enz.). Hierbij wordt bijzondere aandacht besteed aan de bescherming van cryptografische sleutels. Waar nodig ondersteunen deze technieken ook de onweerlegbaarheid van de gegevens.

g. De integriteit van informaticasystemen wordt gewaarborgd door een goed beheer van de software op operationele systemen en de toegangsbeveiliging voor softwarebibliotheken.

h. Formele procedures voor het beheer van wijzigingen worden gebruikt om de kans op verminderde beschikbaarheid of uitval van informatiesystemen tot een minimum te beperken. In het bijzonder worden nieuwe versies van besturingssystemen met de nodige omzichtigheid benaderd.

i. Veiligheidsmaatregelen worden genomen bij het uitbesteden van softwareontwikkeling. De veiligheidsaspecten van de samenwerking worden contractueel vastgelegd. Wijzigingen aan softwarepakketten geleverd door derden dienen zo veel mogelijk beperkt te worden. *(Niet van toepassing)*

j. De vertrouwelijkheid van testgegevens moet op hetzelfde niveau gegarandeerd worden als operationele gegevens. *(Niet van toepassing)*

k. Updates van besturingssystemen en toepassingen worden op gepaste wijze uitgevoerd om de veiligheid en weerbaarheid ervan te kunnen garanderen.

13. Website

DOELSTELLING :
Middelen voor publieke communicatie en verwerking van persoonsgebonden gegevens correct beheren.

a. De organisatie voorziet in een beveiligde webtoepassing, voorzien van een certificaat (SSL), uitgegeven door een CA (Certificate Authority).

b. Met cookies kan informatie worden verzameld of opgeslagen over het websitebezoek of over (het apparaat) van de gebruiker. Men onderscheid hierbij noodzakelijke, functionele, statistische en marketing cookies. Het gebruik van deze cookies moet in overeenstemming zijn met de huidige wetgeving hieromtrent en mogen geen nadelige gevolgen hebben voor de privacy van de bezoekers.

c. Op grond van de GDPR worden 'cookiewalls' op de publieke websites van de organisatie niet toegestaan. Cookiewalls verhinderen mogelijk de geldige toestemming van de bezoekers.

d. Men dient rekening te houden met het gegeven dat het (eventueel) gebruik van Google Analytics (GA) op websites niet volledig GDPR compliant is. Vanaf GA4 (versie 4) is het mogelijk om privacy features specifieker te beheren. Privacy features in strijd met GDPR dienen te worden uitgeschakeld. Een andere optie is om alternatieve web analytics software te gebruiken voor het beheren van statistieken en analyses voor (eigen) websites.

e. Publieke websites bevatten de privacyverklaring van de entiteiten en/of organisatie.

14. Leveranciersrelaties

DOELSTELLING :
Het correct vastleggen van verantwoordelijkheden in kader van onderaanneming of uitbesteding.

f. In geval van onderaanneming of uitbesteding van diensten door een derde partij worden de bepalingen inzake de geleverde diensten contractueel vastgelegd in een samenwerkings- of dienstenovereenkomst.

g. In geval van verwerking van persoonsgegevens via onderaanneming of door een derde partij, zal tussen de verwerkingsverantwoordelijke (de organisatie) en de verwerker van deze gegevens een verwerkingsovereenkomst opgesteld worden volgens de richtlijnen van de AVG (GDPR). Voor de verwerking van persoonsgegevens met Vlaamse instanties zal een protocol worden opgesteld.

h. Elke organisatie die professionele, vertrouwelijke of gevoelige gegevens wenst te verwerken in een 'cloud' of SAAS (Software-as-a-service) omgeving moet de volgende garanties verkrijgen van de betrokken CSP (Cloud Service Provider) : onvoorwaardelijke bescherming van de vertrouwelijke gegevens, fysieke beveiliging van het datacenter, logische toegangsbeveiliging, systeembeveiliging, netwerkbeveiliging.

15. Business Continuity Planning

DOELSTELLING :
Business Continuity Planning (BCP) is een bedrijfsproces dat preventieve en reactieve maatregelen beschrijft en ontwikkelt, alsook herstelprocessen tegen potentiële risico's die de organisatie en de interne werking kunnen bedreigen.

15.1 Disaster Recovery Procedure

DOELSTELLING :
Kunnen reageren op verstoring van bedrijfsactiviteiten en het beschermen van kritieke bedrijfsprocessen in geval van belangrijke technische incidenten.

a. Gebeurtenissen en elementen die kunnen leiden tot onderbreking in de dienstverlening door falen van ICT apparatuur, natuur- of weerfenomenen, stroomonderbreking, brand, waterschade, … worden geïdentificeerd en de impact van zulke gebeurtenissen wordt op voorhand geanalyseerd. Maatregelen worden genomen om mogelijke herhaling van dergelijke feiten te voorkomen.

b. De organisatie beschikt of zorgt voor de opmaak van een Disaster Recovery Procedure (DRP) in het geval van een gedeeltelijke of volledige onderbreking van de dienstverlening, om deze dienstverlening te herstellen binnen een vooraf bepaald tijdsbestek. Een Disaster Recovery Procedure beschrijft hoofdzakelijk de ICT herstelprocessen. Dit plan wordt up-to-date gehouden en indien de financiële en organisatorische middelen beschikbaar zijn, op regelmatige tijdstippen getest. Het plan beschrijft de te volgen stappen om de werkzaamheden en dienstverlening te hervatten, alsook de nodige contactgegevens van bedrijven en contactpersonen verantwoordelijk voor de uitvoering van dit plan. De organisatie kan hierin worden bijgestaan door de DPO.

c. De organisatie voorziet in, of maakt voorafgaandelijke afspraken met andere organisaties voor een eventuele fysieke uitwijkmogelijkheid in geval van totale ramp. Dit kunnen bv naburige lokale besturen zijn. De organisatie kan ook preventieve maatregelen treffen zodat de werking kan gegarandeerd worden vanuit eender welke (individuele) telewerklocatie (thuis, andere organisatie,…)

15.2 Cyber Resilience Plan

DOELSTELLING :

Het nemen van preventieve en reactieve maatregelen bij cyberaanvallen

a. De organisatie dient te voldoen aan de Europese cybersecurity NIS2 richtlijn (Network en Information Security), die van kracht wordt in oktober 2024. Deze richtlijn beeft tot doel de cyberweerbaarheid van organisaties te versterken en deelt organisaties in als essentiële en belangrijke entiteiten. Lokale overheden worden beschouwd als essentiële entiteiten. Hiervoor gelden bijkomende regels zoals een mogelijk proactief toezicht door het nationaal CSIRT (Cyber Security Incident Response Team). De richtlijn houdt volgende algemene verplichtingen in : het uitwerken van een cyberveiligheidsbeleid, , training en sensibilisering van medewerkers, gefaseerde meldingsplicht bij cyberincidenten en beveiliging van de aanvoerketens, …

b. De organisatie neemt de gepaste preventieve technologische en organisatorische maatregelen tegen cyberaanvallen op de volledige onder eigen verantwoordelijkheid beheerde ICT infrastructuur. Dit is de ICT infrastructuur die lokaal aanwezig is en/of ondergebracht is in een datacenter. Het omvat ook alle websites die via interne of externe hosting onder verantwoordelijkheid van de organisatie vallen.

   Voorbeelden van cyberaanvallen zijn :

   - DOS (Denial of service) en DDOS aanval (Distributed Denial of service) ;
   - Ransomware aanvallen (data encryptie) ;
   - Spionage, desinformatie (fake news);
   - Phishing en social engineering ;
   - ‘Brute force’ attacks (password guessing on internet facing systems) ;
   - Malware aanvallen / virussen (spyware, adware, key-loggers, trojan,…);
   - ‘Man-in-the-middle’ attacks (fraudulent websites) ;
   - ‘Drive-bij attacks’ (unsecure website) ;
   - Supply chain attacks (trusted third-party vulnerability) ;
   - Kaping van de ICT systemen voor blockchain verwerkingen (cryptocurrency mining) ;
   - SQL injections (unsecure databases).
   - XSS Cross Site Scripting (malicious scripts in websites)
   - Clickjacking (misleiding door verborgen of vermomd element op webpagina)

c. De organisatie stelt zich weerbaar op tegen cyberaanvallen en voorziet hiervoor in een procedure : Cyber Resilience Plan. Het plan bevat een cybersecurity checklist welke een inschatting is om de eigen digitale informatie te beschermen (risk assessment) tegen cyberaanvallen.

d. De informatieveiligheidscel neemt de taak van 'Cyber Response Team' waar, dewelke instaat voor de coördinatie van noodzakelijke maatregelen en acties bij eventuele cyberaanvallen gericht aan één of meer entiteiten van de organisatie. Dit team heeft bovendien de opdracht om cybersecurityrisico's in te schatten, te beperken en te voorkomen, in nauw samenwerkingsverband met de ICT verantwoordelijken en/of ICT dienstverleners.

e. De organisatie zorgt voor een noodplanning en communicatiestrategie in het geval de ICT infrastructuur en/of dienstverlening gedeeltelijk of volledig door een cyberaanval onbeschikbaar zou zijn.

16. Beheer van incidenten in verband met informatieveiligheid

DOELSTELLING :
Incidenten, datalekken en cyberincidenten correct evalueren en nadien voorkomen

a. Alle personeelsleden en/of medewerkers alsook mandatarissen hebben de plicht om informatieveiligheidsincidenten, datalekken en cyberincidenten te melden aan ofwel de ICT diensten, leidinggevende(n) of DPO. Bij belangrijke incidenten waarbij de dienstverlening in het gedrang komt, zal tevens de informatieveiligheidscel op de hoogte gebracht worden.

b. Incidenten m.b.t. informatieveiligheid, datalekken en cyberaanvallen worden gedetailleerd geregistreerd en nadien geanalyseerd. Meldingen aan toezichthoudende instanties (GBA, VTC, CSIRT) gebeuren binnen de wettelijk voorgeschreven termijnen.

c. Voor een efficiënte afhandeling van incidenten wordt een incidentenregister bijgehouden door de organisatie, samen met de DPO.

d. Adequate maatregelen worden getroffen om herhaling te voorkomen.

17. Communicatie betreffende informatieveiligheid

DOELSTELLING :
Communicatie over de verwerking van persoonsgegevens door de organisatie bekendmaken.

a. De organisatie voorziet een in privacyverklaring. De privacyverklaring omvat de wijze van verwerking van persoonsgegevens door de organisatie. Deze verklaring moet bondig, transparant en in begrijpbare taal opgemaakt zijn. De contactgegevens van de DPO zijn kenbaar gemaakt op de privacyverklaring. Elke belanghebbende moet is staat gesteld worden om informatie aangaande de verwerking van de eigen persoonsgegevens te bekomen zoals wettelijk is voorzien.

b. Deze privacyverklaring wordt tevens gepubliceerd op de website. Deze is gemakkelijk vindbaar aangegeven voor alle bezoekers van de website.

18. Naleving

DOELSTELLING :
Een correcte naleving van alle wettelijke en contractuele beveiligingseisen waaraan de gebruikte informatiesystemen onderworpen zijn, de correcte behandeling van persoonsgegevens en naleving van het informatieveiligheidsbeleid van het bestuur.

a. De organisatie zal de wettelijke en contractuele beveiligingseisen naleven waaraan de gebruikte informatiesystemen onderworpen zijn.

b. De toestand van het niveau van de beveiliging van de informatiesystemen (inclusief de herziening en de opvolging van de procedures) wordt regelmatig geëvalueerd op basis van het desbetreffende beleid. Dit zal gebeuren door interne begeleiding, interne controle, interne audit en/of een externe audit.

c. De controle op de uitvoering van het informatieveiligheidsbeleid zal mogelijk worden gemaakt met ICT-hulpmiddelen die ter beschikking gesteld worden van interne en externe auditeurs.

d. Het beleid (policies), de bijhorende procedures en eventuele andere nuttige documenten worden ter beschikking gesteld op een voor elk personeelslid toegankelijke plaats. Elke belangrijke toevoeging, aanpassing of verwijdering wordt steeds bekend gemaakt. De DPO staat steeds ter beschikking voor vragen en bijkomende uitleg.

e. Sommige policies en procedures zullen een verklaring inhouden die ondertekend moet worden door elk personeelslid. Zo verklaart hij/zij dat hij/zij het document gelezen heeft en verbindt hij/zij zich ertoe zich te houden aan de richtlijnen die beschreven staan in het document.

f. De DPO heeft een intern-auditerende functie. Hij/zij adviseert, motiveert, documenteert en sensibiliseert waar en wanneer nodig.

g. De eigenlijke implementatie en controle op de naleving van de informatie-veiligheidsmaatregelen die beschreven worden in het beleid, de bijhorende policies, procedures en andere documenten behorende tot het informatieveiligheidsdomein behoort tot de verantwoordelijkheid van de persoon die belast is met het dagelijks bestuur (algemeen directeur). Bij een eventuele niet-naleving van de informatieveiligheidsmaatregelen gebeurt de sanctionering conform de rechtspositieregeling en/of de wetgeving.

19. Handhaving, opvolging en herziening

DOELSTELLING :
Het ter kennis brengen van het bestaan of uitvoering van controles door bevoegde instanties. Een mogelijke herziening van dit beleid is gebaseerd op de richtsnoeren en naargelang de beleidsmatige en technologische evoluties.

a. De Vlaamse gegevensbeschermingsautoriteit (VTC - Vlaamse Toezichtcommissie voor de verwerking van persoonsgegevens) en/of elk ter zake bevoegd comité of instantie (bv Audit Vlaanderen) kunnen controles uitvoeren of door een externe instantie laten uitvoeren op de naleving van specifieke aspecten met betrekking tot de informatiebeveiliging van de persoonsgegevens. Deze zijn in beginsel slechts van kracht bij de verwerking van persoonsgegevens, ze moeten echter eveneens worden toegepast in het kader van machtigingen verleend door elk van de (eerdere) sectorale comités ingesteld bij de Commissie voor de bescherming van de persoonlijke levenssfeer en volgens de Europese regelgeving AVG (GDPR).

b. De organisatie draagt de verantwoordelijkheid om in functie van de voor hun specifieke situatie en al naargelang de belangrijkheid van de te beveiligen werkingsmiddelen, de meest aangewezen beveiligingsmiddelen te implementeren. Tot slot dient worden opgemerkt dat maatregelen voor informatiebeveiliging voor herziening vatbaar zijn. Ze zullen aldus worden aangepast in functie van de evoluties die zich wettelijk, technisch, en in het bijzonder inzake veiligheidsrisico's, ISO-normeringen of op ander vlak, voordoen.

20. Overzicht beleidsdocumenten en procedures informatieveiligheid

Algemene documenten

- Arbeidsreglement lokaal bestuur Pepingen v2022 – **GR / RvMW 28/06/2022 : OK ; (CBS / VB 16 05 2022)**
  - *'Internet en-e-mail policy' :* (in bijlage in arbeidsreglement) ;
- Deontologische code v20xx ??

Beleidsdocumenten en procedures (ISMS)

- Informatieveiligheidsbeleid v2022 – **GR 30/05/2023 : OK ;**
  - *Informatieveiligheidsplan* ***: OK / up-to-date :***
  - *Beleid authenticatie en logisch toegangsbeheer* ***: OK / up-to-date ;***
  - *Beleid telewerken' : beschikbaar, wachten op reactie bestuur ;*
  - *Beleid mobiele devices : niet beschikbaar;*
  - *Beleid BYOD : beschikbaar, wachten op reactie bestuur;*
  - *Beleid encryptie : niet beschikbaar ;*
  - *Cyber Resilience Plan :* ***OK*** *;*
  - *Disaster recovery procedure : niet beschikbaar ;*
  - *Procedure 'In-en uitdiensttreding' : niet beschikbaar ;*
- Informatieveiligheidscel ; **OK ;**
- Incident management incl. datalekken, cyberincidenten : **OK** ;

Andere documenten en procedures (ISMS)

- Netwerkschema (ICT partner – last update 13/2/2018) : beschikbaar ;
- Netwerkschema (Basic Network Layout - DPO) : voorzien 2023 ;
- Disaster recovery procedure : niet beschikbaar ;
- Samenwerkingsovereenkomst gemeentebestuur / OCMW : Niet beschikbaar ;

Audits met aspecten informatieveiligheid

- Cyberveilige gemeenten 'Ethical hacking' HoWest / VVSG (Q4/2021)
- Thema audit 'Beheer van ICT risico's' – Audit Vlaanderen (Q4/2021)

21. Overzicht aanpassingen en correcties

Basisdocument : Q1 2019 - goedkeuring GR op 28/05/2019

Update 2020 - goedkeuring GR voorzien op <datum> - geen info / niet behandeld

Update 2021 – goedkeuring GR op 25/1/2022

Update 2022 – goedkeuring GR op 30/05/2023

Update 2023 – goedkeuring GR / RvMW voorzien op < datum >

- Hfdstk 3.2 f – verwijzingen naar andere documenten vormen integraal onderdeel van Informatieveiligheidsbeleid, inclusief informatieveiligheidsplan
- Hfdstk 11 d : Communicatie – toevoeging NIS2 richtlijn en bepalingen
- Hfdstk 13 d : Website – Google Analytics
- Hfdstk 15.1 c : DRP - fysieke uitwijkmogelijkheden
- Hfdstk 15.2 a : CRP – toevoeging NIS2 richtlijn en bepalingen
- Hfdstk 16 : Incidentenbeheer - verbeterde bepaling en toevoeging NIS2 richtlijn