De gemeenteraad

Besluit

2026_GR_00699 Beleidskader informatieveiligheid Stad en OCMW Gent - Goedkeuring

Beslissing: Goedgekeurd in openbare vergadering van 22 juni 2026

Zijn aanwezig bij de beslissing van dit punt:

Rudy Coddens, voorzitter
Zeneb Bensafia, ondervoorzitter; Mathias De Clercq, burgemeester; Hafsa El-Bazioui, schepen; Astrid De Bruycker, schepen; Sofie Bracke, schepen; Joris Vandenbroucke, schepen; Bram Van Braeckevelt, schepen; Burak Nalli, schepen; Filip Watteeuw, schepen; Christophe Peeters, schepen; Johan Deckmyn; Sami Souguir; Freya Van den Bossche; Stephanie D'Hose; Sven Taeldeman; Veli Yüksel; Filip Van Laecke; Karlijn Deene; Anneleen Van Bossuyt; Bert Misplon; Fourat Ben Chikha; Tom De Meester; Patricia De Beule; Ronny Rysermans; Isabelle Heyndrickx; Els Roegiers; Frederik Sioen; Laura Schuyesmans; Gaëlle De Smet; Liesbet De Weder; Sophie Vanonckelen; Sarah Van Acker; Jenna Boeve; Lies Vanpeperstraete; Bob Cammaert; Mathieu Cockhuyt; Dilek Arici; Veerle Baert; Stefaan De Winter; Julie Steendam; Sabena Donkor; Yilmaz Cetinkaya; Simon Smagghe; Jonas Naeyaert; Pascal Vlaeminck; Ywein Joris
Mieke Hullebroeck, algemeen directeur; Liesbet Vertriest, adjunct-algemeendirecteur
Wouter Decoodt, vertrouwenspersoon;

Bevoegd: Mathias De Clercq
Betrokken: Hafsa El-Bazioui

Juridisch kader

De volgende bepalingen zijn van toepassing inzake de bevoegdheid:
Het Decreet over het lokaal bestuur van 22 december 2017, artikel 40, §2.

De beslissing wordt genomen op grond van:

- De wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid (de "NIS2-wet").
- De Verordening (EU) 2016/679 van 27 april 2016 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG, in het bijzonder artikel 32.
- De Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.

- De Wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen.
- De Wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid.
- Het Koninklijk besluit van 12 augustus 1993 houdende de organisatie van de informatieveiligheid bij de instellingen van sociale zekerheid, gewijzigd bij koninklijk besluit van 21 december 2018.
- Het Decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer.
- Het Besluit van de Vlaamse Regering van 23 november 2018 betreffende de functionarissen voor gegevensbescherming, vermeld in artikel 9 van het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer.
- Het Besluit van de Vlaamse Regering van 15 mei 2009 houdende de uitvoering van het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer.

Motivering

Stad en OCMW Gent werken dagelijks met een grote hoeveelheid informatie en data. Een belangrijk deel daarvan bestaat uit persoonsgegevens. Deze informatie is noodzakelijk om de wettelijke opdrachten en de dienstverlening van de Stad en OCMW Gent correct, efficiënt en betrouwbaar uit te voeren.

Data en informatie zijn belangrijke bedrijfsmiddelen voor beide organisaties. Ze moeten daarom op een passende manier worden beveiligd en beschermd. Onvoldoende beveiliging kan leiden tot verlies van vertrouwen, schade aan personen of aan de organisatie, en juridische of financiële gevolgen.

Om die reden werd een gemeenschappelijk beleidskader informatieveiligheid voor Stad en OCMW Gent uitgewerkt. Dit beleidskader legt de basis voor informatiebeveiliging binnen beide organisaties. Het biedt een raamwerk waarbinnen procedures, richtlijnen en technische en organisatorische maatregelen worden uitgewerkt, zoals toegangsbeheer en procedures voor het melden en behandelen van beveiligingsincidenten.

Het beleidskader heeft tot doel de beschikbaarheid, integriteit en vertrouwelijkheid van informatie te waarborgen. Dit betekent dat informatie tijdig beschikbaar is, correct en betrouwbaar blijft, en alleen toegankelijk is voor bevoegde personen.

Het beleidskader geldt voor alle informatievoorziening en informatiegebruik, ongeacht de gebruikte technologieën of systemen. Het is bindend voor iedereen die in opdracht van Stad of OCMW Gent informatie verwerkt, waaronder medewerkers, mandatarissen, stagiairs, vrijwilligers en externe dienstverleners.

Het beleidskader informatieveiligheid vervangt de beleidsverklaring informatieveiligheid dat werd goedgekeurd door het college van burgemeester en schepenen op 5 december 2013.

Het ontwerp van beleidskader informatieveiligheid werd goedgekeurd door het managementteam van de Stad Gent op 26 mei.

De NIS2-wet versterkt het belang van cyberveiligheid, risicobeheer, incidentbeheer, passende beveiligingsmaatregelen en bestuurlijke verantwoordelijkheid. Stad en OCMW Gent moeten daarom beschikken over een duidelijk en gedragen beleidskader dat richting geeft aan de organisatie met betrekking tot informatieveiligheid en dat de verantwoordelijkheden binnen beide organisaties vastlegt.

Het beleidskader vertrekt van een risicogebaseerde aanpak. Dit betekent dat beveiligingsmaatregelen worden bepaald op basis van de risico's voor de beschikbaarheid, integriteit en vertrouwelijkheid van informatie. De zwaarste maatregelen worden genomen waar de risico's voor informatie en systemen het grootst zijn.

Het beleidskader voorziet ook in een continu verbeterproces via een beheersysteem voor informatieveiligheid. Daarbij worden maatregelen systematisch gepland, uitgevoerd, gecontroleerd en verbeterd. Daarnaast is rekening gehouden met het CyberFundamentals Framework van het Centrum voor Cybersecurity België, de richtsnoeren van de Gegevensbeschermingsautoriteit en de Vlaamse Toezichtcommissie over informatiebeveiliging van persoonsgegevens, en de minimale normen informatieveiligheid en privacy van de Kruispuntbank van de Sociale Zekerheid.

Het beleidskader informatieveiligheid staat in nauwe relatie tot het beleidskader gegevensbescherming. Informatieveiligheid richt zich op de bescherming van alle soorten informatie, waaronder vertrouwelijke, gevoelige en strategische informatie en persoonsgegevens. Gegevensbescherming richt zich specifiek op het rechtmatig, behoorlijk, transparant en veilig verwerken van persoonsgegevens. Informatieveiligheid is daardoor een noodzakelijke randvoorwaarde voor een goede bescherming van persoonsgegevens.

Door het beleidskader informatieveiligheid Stad en OCMW Gent goed te keuren, legt de gemeenteraad het strategisch kader vast voor de beveiliging van informatie binnen Stad en OCMW Gent. Zo wordt gezorgd voor een gemeenschappelijke aanpak, duidelijke verantwoordelijkheden, een betere beheersing van cyberrisico's en informatieveiligheidsrisico's, en een veilige en betrouwbare dienstverlening aan burgers, medewerkers en partners.

Bijgevoegde bijlage(n):

- Beleidskader informatieveiligheid Stad en OCMW Gent.pdf (deel van de beslissing)

Beslissing

Op voorstel van Het college van burgemeester en schepenen
Beslist het volgende:

- Met unanimiteit

Artikel 1:
Keurt goed het beleidskader informatieveiligheid Stad en OCMW Gent, zoals gevoegd in bijlage waardoor de beleidsverklaring informatieveiligheid, goedgekeurd door het college van burgemeester en schepenen op 5 december 2013, niet langer dient nageleefd te worden.

Elektronisch ondertekend op 24/06/2026 16:32:06 (GMT+02:00) door Mieke Hullebroeck, algemeen directeur stad en OCMW Gent

Elektronisch ondertekend op 24/06/2026 13:46:18 (GMT+02:00) door Rudy Coddens, voorzitter gemeenteraad en raad voor maatschappelijk welzijn

2026_GR_00699 - Beleidskader informatieveiligheid Stad en OCMW Gent

Beleidskader Informatieveiligheid Stad en OCMW Gent

1 april 2026

Stad Gent

Colofon

Stad Gent
Departement Bedrijfsvoering – Dienst Organisatieontwikkeling

Publicatiedatum
1 april 2026

Contact
privacy@stad.gent

Postadres
Stad Gent – Departement Bedrijfsvoering
Stadhuis, Botermarkt 1, 9000 Gent

Foto voorblad
Gravensteen - Robin De Mol (Beeldbank Stad Gent)

Inhoud

1. Inleiding

Een organisatie kan niet zonder **data en informatie**.
Een aanzienlijk deel van die data zijn **persoonsgegevens.**

Data en informatie zijn **bedrijfsmiddelen** die een heel belangrijke waarde hebben voor onze organisatie. Bijgevolg moeten we deze voortdurend op een passende manier beveiligen en beschermen. Onvoldoende beveiliging kan leiden tot verlies van vertrouwen, schade aan personen of de organisatie, juridische of financiële consequenties.

Dit beleidskader legt de basis voor informatiebeveiliging binnen Stad en OCMW Gent (hierna Stad Gent). Het biedt een **raamwerk** waarbinnen procedures, richtlijnen, technische en organisatorische maatregelen worden uitgewerkt om de beschikbaarheid, integriteit en vertrouwelijkheid (BIV) van onze gegevens te waarborgen:

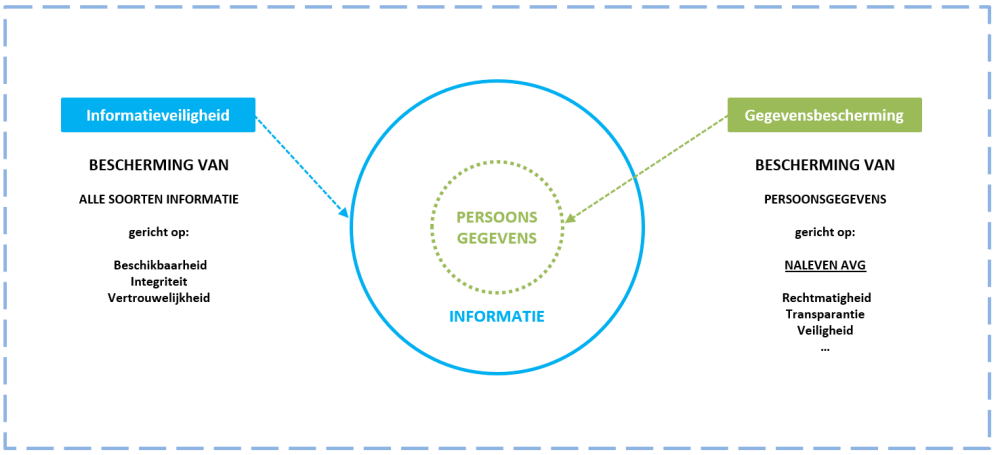
- **Beschikbaarheid** – informatie en systemen zijn tijdig en correct beschikbaar voor bevoegde gebruikers;
- **Integriteit** – informatie is juist, volledig en betrouwbaar;
- **Vertrouwelijkheid** – alleen bevoegde personen hebben toegang tot informatie.

Met dit beleidskader wil Stad Gent:

- het bewustzijn rond informatieveiligheid vergroten bij alle betrokkenen;
- de kwaliteit en continuïteit van de dienstverlening borgen;
- risico's voor inwoners, partners en de organisatie beperken;
- een duidelijke verdeling van rollen en verantwoordelijkheden vastleggen.

Informatieveiligheid richt zich op de **bescherming van alle soorten informatie** zoals vertrouwelijke, gevoelige of strategische informatie en persoonsgegevens binnen onze organisatie. Dit met als doel het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid.

Gegevensbescherming richt zich specifiek op het **beschermen van persoonsgegevens**. Gegevensbescherming is gebaseerd op het naleven van de Algemene Verordening Gegevensbescherming (AVG) met als bedoeling persoonsgegevens rechtmatig, transparant en veilig te verwerken. De specifieke verplichtingen en maatregelen voor de naleving van de Algemene Verordening Gegevensbescherming zijn uitgewerkt in een **apart beleidskader voor gegevensbescherming**.



Verband tussen Informatieveiligheid en gegevensbescherming

Gezien de technologische evoluties en steeds stijgende cyberdreigingen is informatieveiligheid, net als gegevensbescherming, een **continu verbeterproces** met een **risicogebaseerde aanpak**. Terwijl gegevensbescherming vertrekt van risico's voor de betrokkene zoals bijvoorbeeld onze inwoners, vertrekt informatieveiligheid van risico's voor de organisatie op basis van beschikbaarheid, integriteit, vertrouwelijkheid (BIV). Bij informatieveiligheid zoeken we een balans tussen het afwegen van risico's versus kosten en impact van benodigde beveiligingsmaatregelen.

Dit Beleidskader Informatieveiligheid is in lijn met de relevante wet- en regelgeving en is van toepassing op iedereen die in aanraking komt met gegevens van Stad Gent.

2. Begrippenkader

Informatie: gegevens (data) die betekenis krijgen doordat ze in een bepaalde context worden geplaatst, verwerkt of geïnterpreteerd. Informatie kan verschillende vormen aannemen zoals tekst, cijfers, beelden, audio of combinaties daarvan. Informatie kan ook persoonsgegevens omvatten.

Informatieveiligheid: de verzamelnaam die gebruikt wordt om alle processen en maatregelen aan te duiden die handelen over de beveiliging van informatie en in het bijzonder over de beveiliging van persoonsgegevens. Dat kan gaan over gedragsregels, procedures, organisatiestructuren, technische maatregelen, enz. De integriteit, de beschikbaarheid en de vertrouwelijkheid van de gegevens staan hierbij centraal.

Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (en dus geen rechtspersoon).

Gegevensbescherming: het zorgvuldig omgaan met persoonsgegevens zodat de rechten van natuurlijke personen waaronder burgers en medewerkers worden gerespecteerd. Persoonsgegevens worden enkel voor duidelijke en rechtmatige doeleinden verwerkt en dit in overeenstemming met de Algemene Verordening Gegevensbescherming (AVG).

3. Toepassingsgebied

Dit beleidskader voor informatieveiligheid is van toepassing op:

1) Wat?

   Dit beleidskader geldt voor alle informatievoorziening en informatiegebruik ongeacht de technologieën en systemen die daartoe worden ingezet en ongeacht welke informatie het betreft.

2) Wie?

   Dit beleidskader is bindend voor iedereen die in opdracht van Stad Gent of OCMW Gent informatie (bedrijfsgegevens en/of persoonsgegevens) verwerkt.

   Dit omvat alle medewerkers, ongeacht hun statuut, mandatarissen, stagiairs, vrijwilligers en externe dienstverleners die in opdracht van de organisatie informatie verwerken.

3) Welke organisaties?

   - In de eerste plaats onze eigen organisatie Stad Gent en OCMW Gent.
   - AGB District09 als IT-partner.
   - Elke andere externe organisatie die voor of samen met Stad of OCMW Gent informatie verwerkt.

Visualisatie toepassingsgebied

4. Doelstellingen

Het Beleidskader Informatieveiligheid is het kader voor passende procedurele, technische en organisatorische maatregelen om informatie van Stad Gent te beschermen en te waarborgen.

Met dit beleidskader formuleren we een **duidelijke richting** op gebied van informatie-beveiliging en streven we volgende doelstellingen na om een adequaat niveau van beveiliging conform alle wet- en regelgeving te bereiken:

- Het garanderen van correcte en veilige informatievoorzieningen.
- Het beschermen van kritieke bedrijfsprocessen.
- Het minimaliseren van risico's via een risicogebaseerde bescherming van bedrijfsmiddelen.
- Het managen van de informatiebeveiliging met een informatiebeveiligingsproces op basis van een Plan-Do-Check-Act cyclus.
- Het creëren van bewustzijn over het belang van informatieveiligheid en cybersecurity bij medewerkers.
- Het beheersen van de toegang tot informatiesystemen en het voorkomen van ongeautoriseerde toegang.
- Het adequaat reageren op incidenten.
- Het beschermen en verwerken van persoonsgegevens van burgers en medewerkers in overeenstemming met de AVG[1].
- Het waarborgen van de naleving van dit beleidskader.

[1] *Uitgewerkt in het beleidskader voor gegevensbescherming Stad en OCMW Gent.*

5. Uitgangspunten

Stad Gent hanteert erkende kaders als leidraad voor het informatieveiligheidskader:

- **ISO/IEC 27001** – de internationale norm voor informatiebeveiligingsbeheersystemen.
- **CyberFundamentals (CyFun®)** – het Belgische referentiekader van het Centrum voor Cybersecurity België (CCB).

Het gebruik van deze kaders sluit elkaar niet uit. Waar mogelijk past Stad Gent ze **geïntegreerd** toe.

Het informatieveiligheidsbeleidskader voldoet bovendien aan de minimale veiligheidsnormen van de Kruispuntbank Sociale Zekerheid (KSZ) en aan de richtsnoeren informatiebeveiliging van persoonsgegevens van de Gegevensbeschermingsautoriteit (GBA).

Informatiebeveiliging is een **verantwoordelijkheid van alle medewerkers**: medewerkers dienen verantwoord om te gaan met informatie en persoonsgegevens; de diensthoofden zijn verantwoordelijk voor een goede informatiebeveiliging binnen hun dienst en het managementteam volgt de praktische uitwerking van dit beleidskader op.

Het beleidskader gaat uit van de zogenaamde **"risk based-approach"** of risicobenadering om tijdig relevante risico's effectief te kunnen aanpakken. Dit betekent dat Stad Gent passende beveiligingsmaatregelen zal nemen op basis van het risico dat een bepaalde verwerking van informatie met zich meebrengt.

Informatiebeveiliging is een **continu proces**. Technologische en organisatorische ontwikkelingen maken het noodzakelijk om periodiek na te kijken of alle genomen technische en organisatorische maatregelen nog effectief zijn.

We passen informatiebeveiliging, **'security en privacy-by-design'**, toe op de volledige levenscyclus van informatie. Vanaf de vraag voor een nieuwe toepassing tot en met het uit dienst nemen van een toepassing en het archiveren van de informatie.

Medewerkers dienen de waarde van informatie te kennen en daarnaar te handelen. De waarde wordt bepaald door de schade als gevolg van verlies van integriteit, vertrouwelijkheid en beschikbaarheid. Hiervoor passen we **dataclassificatie** toe op onze gegevens.

6. Organisatie informatiebeveiliging

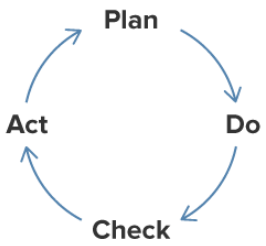
De aanpak van informatieveiligheid steunt op een gestructureerd en continu verbeterproces dat ervoor zorgt dat informatie binnen Stad Gent op een passende manier beschermd wordt. We hanteren een kwaliteitssysteem dat de veiligheid van onze informatie waarborgt via een risicogebaseerde aanpak.

6.1. Informatiebeveiligingsproces

Het beveiligen van informatie is geen eenmalige actie, maar een **continu proces**.

Stad en OCMW Gent gebruiken hiervoor een **Information Security Management System** (ISMS). Dit is het geheel van beleidsafspraken, processen, rollen, hulpmiddelen en maatregelen waarmee we de informatieveiligheid structureel organiseren, bewaken en verbeteren.

Het ISMS werkt volgens de **Plan–Do–Check–Act** cyclus (PDCA), een methodiek voor kwaliteits- en veiligheidsbeheer. Door deze cyclus regelmatig te doorlopen, controleren we of onze beveiligingsmaatregelen nog effectief zijn en spelen we tijdig in op nieuwe risico's.



- Plan:
    - Vaststellen of actualiseren van het informatieveiligheidsbeleidskader.
    - In kaart brengen van bedrijfsmiddelen (hardware, software, data) en de verantwoordelijken ervan.
    - Uitvoeren van risicoanalyses om bedreigingen, kwetsbaarheden en mogelijke gevolgen in te schatten.
    - Bepalen van passende beheersmaatregelen en verantwoordelijkheden.
- Do:
    - Implementeren van technische en organisatorische beveiligingsmaatregelen.
    - Uitvoeren van bewustwordings- en opleidingsactiviteiten voor medewerkers.

- Check:
    - Controleren of de technische en organisatorische beveiligingsmaatregelen zijn uitgevoerd en werken zoals bedoeld.
    - Uitvoeren van interne controles, testen en -indien van toepassing- audits.
    - Opstellen van rapportages over informatieveiligheid, inclusief resultaten van controles.
- Act:
    - Analyseren van de bevindingen uit controles, rapportages en audits.
    - Vastleggen van tekortkomingen, verbeterpunten en nieuwe risico's.
    - Aanpassen van het beleidskader en het ISMS om de informatieveiligheid blijvend te verbeteren.

6.2. Risicobeoordeling en -beheer

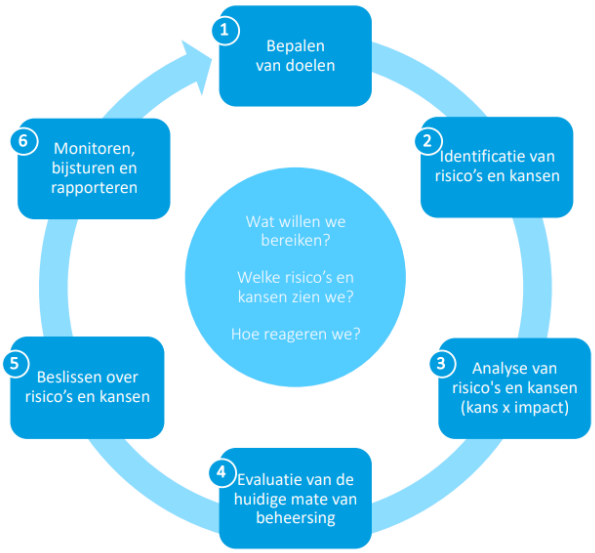
Centraal in het beleidskader staat de risicogebaseerde aanpak waarbij, op basis van een risicoanalyse, het **niveau van de beveiligingsmaatregelen** worden bepaald. De resultaten van de risicoanalyse geven richting bij het bepalen van passende maatregelen en prioriteiten.

Deze aanpak bestaat uit 4 stappen: risicoanalyse, risico-evaluatie, beslissing en monitoring & rapportering.

1. Risicoanalyse: in de analyse wordt de kans bepaald dat het risico zich zou voordoen, alsook een inschatting gemaakt van de impact op de beschikbaarheid, integriteit en vertrouwelijkheid van de data. Hieronder valt ook de impact op vlak van reputatie, op burgers, operationele impact, legale en regelgevende impact. De risicoanalyse wordt periodiek uitgevoerd om voldoende in te spelen op wijzigingen in de situatie of wet- en regelgeving. De kans en de impact bepalen de ernst van het risico.
2. Risico-evaluatie: na de analyse volgt de evaluatie van het risico: in welke mate is het risico op vandaag beheerst?
3. Beslissing: de vorige resultaten (ernst van het risico en de huidige mate van beheersing) leiden tot het stellen van prioriteiten en definiëren van passende acties. Risico's worden tot een zo aanvaardbaar mogelijk niveau ingeperkt, waarbij we moeten erkennen dat er nooit voldoende middelen voorhanden zijn om volledige risicobeheersing te bereiken.
4. Monitoring en rapportering: de vastgestelde prioriteiten en acties worden gemonitord en gerapporteerd aan de organen zoals beschreven in punt 6.8.

Om onze risico's te beheersen gebruiken we het 'kader voor organisatiebeheersing' van de Stad Gent.[2]

[2] *Zie Kader voor Organisatiebeheersing Stad Gent.pdf*



Stappenplan risicobeheersing

6.3. Incidentenbeheer

Ondanks alle preventieve maatregelen kunnen zich incidenten voordoen die onze gegevens in gevaar brengen. Stad Gent beschikt over een **gedocumenteerde procedure** voor het detecteren, melden en afhandelen van beveiligingsincidenten. De nodige maatregelen worden genomen om de gevolgen van een beveiligingsinbreuk te minimaliseren.

Het melden van beveiligingsincidenten aan de relevante autoriteiten en eventuele betrokkenen wordt strikt uitgevoerd in overeenstemming met de wettelijke vereisten en binnen de gestelde termijnen.

Alle beveiligingsincidenten worden geregistreerd, gerapporteerd en geëvalueerd om indien nodig bijkomende maatregelen uit te werken om toekomstige incidenten te voorkomen.

6.4. Samenhangend beleidskader

Het informatieveiligheidsbeleidskader steunt op een gelaagd stelsel van beleidskaders, standaarden, richtlijnen en maatregelen. Dit overkoepelende beleidskader staat bovenaan. Onderwerpspecifieke beleidskaders vertalen dit kader naar bindende verplichtingen per thema. Standaarden leggen vast hoe die verplichtingen technisch worden ingevuld. Richtlijnen bieden praktische aanwijzingen waar geen standaard van toepassing is. Maatregelen beschrijven de feitelijke uitvoering in processen, systemen en tools. Alle documenten zijn onderling consistent en worden beheerd als een samenhangend geheel.

6.5. Bewustwording en vorming

Een goede informatieveiligheid hangt niet alleen af van technische maatregelen maar in grote mate ook van het **gedrag van medewerkers**. De beveiligingsketen is zo sterk als de zwakste schakel; dit blijkt vaak het gedrag van medewerkers te zijn - niet steeds bewust van de risico's van hun handelen. Technische maatregelen kunnen dit in veel gevallen niet oplossen. Iedere medewerker heeft daarom een eigen verantwoordelijkheid om zorgvuldig en integer om te gaan met de informatie die hij of zij verwerkt in overeenstemming met dit beleidskader.

Om dit te ondersteunen, krijgen medewerkers passende opleidingen over informatieveiligheid. We voeren ook periodieke bewustmakingscampagnes rond informatieveiligheid en cybersecurity.

Bij het aannemen of inhuren van nieuwe medewerkers, en het laten verrichten van werkzaamheden door externe medewerkers, wordt bewerkstelligd dat zij hun **verantwoordelijkheden begrijpen** ten aanzien van informatieveiligheid.

De leden van de gemeenteraad en van de raad voor maatschappelijk welzijn volgen de nodige vorming om cyberbeveiligingsrisico's te kunnen beoordelen en gepaste beslissingen te nemen. Dit is een wettelijke verplichting onder de NIS2-wetgeving.

6.6. Gedragen informatieveiligheid

Een doeltreffend beleidskader voor informatieveiligheid vraagt dat alle medewerkers begrijpen waarom informatieveiligheid belangrijk is en wat hun rol daarin is. We zorgen daarom dat het informatieveiligheidskader en de onderlinge verwachtingen actief gecommuniceerd worden aan alle medewerkers, op een manier die aansluit bij hun functie en context.

6.7. Naleving beleidskader

Het is belangrijk dat alle medewerkers, derde partijen en partners zich houden aan het beleidskader informatieveiligheid en de onderwerp-specifieke beleidskaders. De beleidskaders worden openbaar gepubliceerd in het kader van transparantie naar externe partijen met wie we samenwerken en naar de burger. Medewerkers worden regelmatig gesensibiliseerd en geïnformeerd over hoe ze op een veilige manier met informatie moeten omgaan en wat dit beleidskader daarbij van hen verwacht.

Niet naleving van dit beleidskader kan voor personeelsleden aanleiding geven tot passende maatregelen overeenkomstig de toepasselijke rechtspositieregeling of het arbeidsreglement. Voor niet-personeelsleden worden passende maatregelen bij niet naleving van dit beleidskader contractueel vastgelegd.

6.8. Rollen en verantwoordelijkheden

Het verantwoord omgaan met informatie is een **opdracht voor iedereen** binnen onze organisatie; elke medewerker draagt bij aan het waarborgen van de informatieveiligheid.

Onderstaande beschrijving concretiseert de rollen en verantwoordelijkheden voor informatieveiligheid. De specifieke rollen en verantwoordelijkheden voor de verwerking van persoonsgegevens zijn uitgewerkt in het beleidskader voor gegevensbescherming van Stad en OCMW Gent.

Gemeenteraad en raad voor maatschappelijk welzijn
De gemeenteraad (Stad Gent) en de raad voor maatschappelijk welzijn (OCMW Gent) vormen het hoogste bestuursorgaan en zijn eindverantwoordelijk voor het informatieveiligheids-beleidskader. Zij keuren het beleidskader goed en zorgen ervoor dat het als strategisch kader richtinggevend is voor de hele organisatie.

College van burgemeester en schepenen en vast bureau
Het college van burgemeester en schepenen (Stad Gent) en het vast bureau (OCMW Gent) zijn verantwoordelijk voor het toezicht op de uitvoering van het beleidskader via de onderwerp-specifieke beleidskaders. De onderwerp-specifieke beleidskaders vertalen het beleidskader informatieveiligheid naar bindende verplichtingen per thema en worden goedgekeurd door het college van burgemeester en schepenen en het vast bureau.

Managementteam, algemeen directeur en departementshoofden
Het managementteam bestaande uit de algemeen directeur en de departementshoofden ziet toe op een correcte toepassing en naleving van het beleidskader. De departementshoofden zijn primair verantwoordelijk voor informatieveiligheid binnen hun departement en houden daarbij rekening met adviezen vanuit het overleg Coördinatie Informatieveiligheid (CI).

Informatieveiligheidsverantwoordelijke
De informatieveiligheidsverantwoordelijke is eigenaar van dit beleidskader informatie-veiligheid, ziet toe op de correcte toepassing en naleving van het beleidskader en coördineert de uitbouw, werking en verbetering van het beleidskader. De informatieveiligheids-verantwoordelijke rapporteert aan het managementteam, het college van burgemeester en schepenen, het vast bureau, de gemeenteraad en de raad voor maatschappelijk welzijn.

Dienstchefs
Binnen de diensten zijn de dienstchefs verantwoordelijk voor de uitvoering van het beleidskader op operationeel niveau en waken zij over de naleving van vastgelegde procedures en afspraken.

Medewerkers

Elke medewerker is verantwoordelijk voor het zorgvuldig omgaan met informatie en persoonsgegevens die men verwerkt conform dit beleidskader. De medewerkers kennen dit beleidskader, passen het toe en melden ieder vermoedelijk beveiligingsincident of datalek.

Chief Information Security Officer (CISO)

De CISO-rol wordt ingevuld door District09 als strategische ICT-partner van Stad en OCMW Gent. De CISO adviseert over en ondersteunt bij de uitvoering van technische beveiligingsmaatregelen.

Data Protection Officer van Stad en OCMW Gent

Stad en OCMW Gent hebben -zoals wettelijk verplicht- een Data Protection Officer (DPO).
De DPO van Stad en OCMW Gent richt zich op het adviseren, sensibiliseren en toezien op de verschillende verwerkingen van persoonsgegevens. De DPO Stad en OCMW Gent neemt nooit deel aan beslissingen of keurt geen maatregelen goed in verband met informatieveiligheid.

Overleg Coördinatie Informatieveiligheid (CI)

De opvolging van het beleidskader en de coördinatie van acties gebeurt via het Overleg Coördinatie Informatieveiligheid (CI). Dit overleg komt maandelijks samen en fungeert als coördinerend en beslissingsorgaan voor het bepalen en opvolgen van technische en organisatorische maatregelen op vlak van informatieveiligheid en gegevensbescherming, het bespreken van datalekken en kwetsbaarheden en het voorbereiden van rapportages.

De Stad Gent doet beroep op District09 als IT-partner waardoor District09 een cruciale rol heeft om ervoor te zorgen dat de noodzakelijke technische beveiligingsmaatregelen worden geïmplementeerd en onze informatiesystemen en netwerken adequaat beschermd zijn tegen cyberdreigingen. In het CI is daarom zowel de Stad Gent als District09 vertegenwoordigd.

7. Evaluatie en actualisering

Dit beleidskader voor informatieveiligheid wordt jaarlijks herzien.

Eventuele wijzigingen worden goedgekeurd door de gemeenteraad en de raad voor maatschappelijk welzijn en gecommuniceerd aan alle betrokkenen. Nieuwe bedreigingen, technologische ontwikkelingen, resultaten van risicoanalyses, incidentrapportages, audits en wijzigingen in regelgeving worden in de actualisering verwerkt.

8. Relevante wet- en regelgeving

Dit overzicht bevat de belangrijkste Europese, federale en Vlaamse wet- en regelgevende kaders aangevuld met relevante normenkaders en richtlijnen. Het vormt een leidraad bij het opstellen en uitvoeren van het informatieveiligheidsbeleidskader en het beleidskader voor gegevens-bescherming van Stad en OCMW Gent.

Informatiebeveiliging

- De wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid (de "NIS2-wet") heeft in België de richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 (de "NIS2-richtlijn") omgezet naar een wet.
- De minimale normen van de Kruispuntbank Sociale Zekerheid (KSZ) ten aanzien van informatieveiligheid.[3]
- Richtsnoeren met betrekking tot de informatiebeveiliging van persoonsgegevens van steden en gemeenten.[4]
- Cyberfundamentals framework - een door het Centre for Cybersecurity Belgium (CCB) ontwikkeld kader met minimale beveiligingsvereisten en aanbevolen maatregelen om organisaties, waaronder lokale besturen, te beschermen tegen cyberdreigingen. Ze zijn gebaseerd op internationale standaarden (zoals ISO27001, NIST en CIS Controls) en zijn bedoeld als praktische leidraad om de wettelijke verplichtingen inzake informatieveiligheid concreet te vertalen naar werkbare veiligheidsmaatregelen.

Privacy - bescherming van persoonsgegevens

De bescherming van persoonsgegevens is onlosmakelijk verbonden met informatieveiligheid. Informatieveiligheid is een randvoorwaarde voor een zorgvuldige omgang met persoons-gegevens. Hiervoor is een apart beleidskader voor gegevensbescherming uitgewerkt.

- Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van

[3] *https://www.ksz-bcss.fgov.be/nl/gegevensbescherming/informatieveiligheidsbeleid*

[4] *https://www.gegevensbeschermingsautoriteit.be/publications/richtsnoeren-met-betrekking-tot-informatiebeveiliging.pdf*

persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (Algemene Verordening Gegevensbescherming).

- Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (Kaderwet).
- Wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen.
- Wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid.
- Koninklijk besluit van 12 augustus 1993 houdende de organisatie van de informatieveiligheid bij de instellingen van sociale zekerheid, gewijzigd bij koninklijk besluit van 21 december 2018.
- Decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer (E-gov decreet).
- Besluit van de Vlaamse Regering van 23 november 2018 betreffende de functionarissen voor gegevensbescherming, vermeld in artikel 9 van het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer.
- Besluit van de Vlaamse Regering van 15 mei 2009 houdende de uitvoering van het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer.
- Besluit van de Vlaamse Regering van 29 november 2013 tot uitvoering van het decreet van 13 juli 2012 houdende de oprichting en organisatie van een Vlaamse dienstenintegrator.
- Bestuursdecreet van 7 december 2018.
- Decreet van 22 december 2017 over het lokaal bestuur.