UITTREKSEL
GEMEENTERAAD
WOENSDAG 28 JANUARI 2026

Aanwezig:	Luc Decrick, Voorzitter Peter Van Cutsem, Burgemeester Kristof De Cuyper, Hanneke Agneessens, Suzanne De Cort, Schepenen Eddy Timmermans, Greta Cochez, Rudi Seghers, Patrick Vanbellinghen, Marleen Pollé, Sander Geerts, Lotte Van Cutsem, Johan Peetroons, Frieda Moriau, Raadsleden Leen Deneyer, Algemeen directeur
Verontschuldigd:	Saskia Beeckmans, Raadslid
Afwezig:	/

In openbare zitting vergaderd,

Betreft: Informatieveiligheidsbeleid 2026. Beslissing

Aanleiding
Jaarlijks wordt het document “Informatieveiligheidsbeleid” voor ons bestuur geüpdatet.
De doelstelling van een informatieveiligheidsplan is een correcte organisatie en beheer van de informatieveiligheid binnen het bestuur, conform de desbetreffende wetgeving.
De informatieveiligheid binnen een 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 het bestuur enerzijds en aan de persoonlijke levenssfeer van de betrokkenen anderzijds.
De DPO/FG van Welzijnskoepel West-Brabant (Filip Haesen) zorgt voor de sturing, opstelling en herziening van het beleid, bijstelling van de beleidsmaatregelen, opstelling van het veiligheidsplan, opstelling van de vereiste en benodigde policies en procedures, de vaststelling van verantwoordelijkheden en het toezicht op veranderde wetgeving, bedreigingen en incidenten.

Regelgeving
Verordening(EU) 2016/79 van het Europees parlement en Raad van 27 april 2016 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 (algemene verordening gegevensbescherming)
Wet 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.
Wet van 8 augustus 1983 tot regeling van een rijksregister van de natuurlijke personen, verder aangeduid als de wet op het rijksregister
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 elektronisch bestuurlijke gegevensverkeer.
Gelet op het decreet van 6 juli 2001 houdende de intergemeentelijke samenwerking;
Decreet Lokaal Bestuur

Feiten en context
Belangrijkste wijzigingen:
- Hfdstk 5.d : persoonlijke media en cloudtoepassingen - verduidelijking

1. Het gebruik van persoonlijke externe opslagmedia (bv. USB, externe disk, smartphone,…) alsook het gebruik van elke andere persoonlijke externe clouddienst (bv. Dropbox, Google apps, Microsoft apps, iCloud apps, enz) vreemd aan de eigen organisatie, voor de opslag van (persoons)gegevens behorend tot de organisatie is niet toegelaten. Indien noodzakelijk stelt de organisatie externe media met een beveiligde partitie of een softwaretoepassing (bv MS Teams, Onedrive,…) ter beschikking. Media kan worden uitgeleend bij de interne uitleendienst. Documenten aangeleverd via externe fysieke media, worden eerst gescand op malware vóór gebruik. De uitwisseling van (persoons)gegevens gebeurt bij voorkeur via beveiligde platformen (ftps of https) van vertrouwde partnerorganisaties. Gegevensdeling met niet- vertrouwde organisaties dient te worden vermeden.

 Hfdstk 10.r. : aanpassingen betreffende AI act

1. Indien de organisatie gebruik maakt van artificiële intelligentie voor publieke dienstverlening of eigen werking en/of het gebruik van publiek toegankelijke generatieve artificiële intelligentie (GenAI) toelaat, zowel tekstueel (genereren, leesbaar maken en vertalen van tekst), als grafisch (genereren van beelden), dan dient dit transparant en met maximale bescherming van persoonsgegevens en vertrouwelijkheid te gebeuren. De Europese AI Act (verordening) is in werking getreden op 1 augustus 2024. Het is het eerste rechtskader betreffende het gebruik van artificiële intelligentie (wereldwijd). De implementatie van de EU AI Act verloopt in verschillende fasen. De EU AI Act is risicogebaseerd en definieert verschillende risico-niveau's. Risico's zijn o.a. een gebrek aan betrouwbaarheid en integriteit. Het gebruik van (Gen)AI moet worden beperkt tot de gevallen waarin de risico's effectief kunnen worden beheerd. Organisaties zijn verplicht medewerkers te trainen in AI- geletterdheid. Voor meer details, zie het 'Beleid Artificiële intelligentie'.

 Hfdstk 15.2 : aanpassing m.b.t. NIS2

1. 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 eigen inschatting is van het beschermingsniveau en getroffen maatregelen tegen cyberaanvallen (risk assessment).
2. De organisatie (gemeente en OCMW) dient NIET te voldoen aan de Europese cybersecurity NIS2 richtlijn (Network en Information Security), die van kracht geworden is op 18 oktober 2024. Deze richtlijn heeft tot doel de cyberweerbaarheid van organisaties te versterken en deelt organisaties in als essentiële en belangrijke 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, …
3. De organisatie beoogt minimale cyberbeveiligingsmaatregelen te treffen overeenkomstig het CCB Cyber-Fundamentals 'Basic' framework (CCB CyberFundamentals). Deze heeft tot doel de cyberweerbaarheid van organisaties te versterken. Het CCB Cyber-Fundamentals 'Basic' framework beschrijft standaard maatregelen voor alle organisaties aan de hand van technologie en processen die in het algemeen beschikbaar zijn, maar mogelijk moeten toegepast en/of verfijnd worden. Het CyberFundamentals framework is gebouwd rond 6 elementen : beheersing (**Governance)**, Identificatie (**Identify**) van de hardware en software middelen, het beschermen (**Protect**) van deze middelen, detectie (**Detect**) van cyberdreigingen, reageren op cyberdreigingen (**Respond**) en het herstellen van cyberincidenten (**Recover**).
4. De aanbeveling (Digitaal Vlaanderen) om aan dit beveiligingsniveau te voldoen is januari 2030.

 Hfdstk 16 : verduidelijking afhandeling cyberincidenten

1. Alle personeelsleden en/of medewerkers alsook mandatarissen hebben de plicht om informatieveiligheidsincidenten, datalekken en cyberincidenten (ook bij verwerkers) te melden aan ofwel de ICT diensten, leidinggevende(n) of DPO. Bij belangrijke incidenten waarbij de werking of dienstverlening in het gedrang komt, zal tevens de informatieveiligheidscel op de hoogte gebracht worden.
2. Incidenten m.b.t. informatieveiligheid, datalekken en cyberaanvallen worden gedetailleerd geregistreerd en nadien geanalyseerd. Meldingen aan toezichthoudende instanties (VTC, CSIRT, CERT/CCB) gebeuren binnen de wettelijk voorgeschreven termijnen.
3. Voor meldingen van cyberincidenten door NIS2 entiteiten gelden specifieke regels. Voor details, zie CRP (Cyber Resilience Plan) Hfdstk 14.3 - Stappenplan bij afhandeling van een cyberincident.

De wijzigingen t.o.v. vorige versie zijn aangegeven in het blauw, zodat het duidelijk is welke de wijzigingen zijn.

Goedgekeurd met eenparigheid van stemmen.

BESLUIT

Enig artikel: De gemeenteraad keurt het geactualiseerde informatieveiligheidsbeleid 2026 goed, zoals gevoegd bij deze beslissing als bijlage - 2026 Informatieveiligheidsbeleid - Lokaal bestuur Pepingen.

Namens de Raad,

(g) Leen Deneyer
Algemeen directeur

(g) Luc Decrick
Voorzitter

Voor eensluidend afschrift,

Leen Deneyer
Algemeen directeur

Luc Decrick
Voorzitter