b&w-voorstel

GEMEENTE WEERT

Afdeling	: INF - Informatie		B&W-voorstel: DJ-1976380
Naam opsteller voorstel	: Manon Krauth (0495-575680)		Zaaknummer: 1976324
Portefeuillehouder	: mr. R.J.H. (Raymond) Vlecken CBM		Publicatie: Openbaar

Onderwerp

Informatie- kwaliteitsbeleid, privacybeleid en informatiebeveiligingsbeleid.

Voorstel

1. Het informatie- kwaliteitsbeleid vast te stellen.
2. Het privacybeleid vast te stellen.
3. Het informatiebeveiligingsbeleid vast te stellen.

Inleiding

Het informatiebeleid uit 2016, het privacybeleid uit 2019 en het informatiebeveiligingsbeleid uit 2019 zijn vanwege de looptijd, maatschappelijke en technologische ontwikkelingen en de wettelijke verplichting rondom informatiebeveiliging aan een herziening toe.

Het informatie- kwaliteitsbeleid geeft kaders en richting over hoe we controle houden op de verwerking en opslag van onze informatiestromen, ergo: informatiemanagement.

Het privacybeleid omschrijft hoe wij invulling geven aan de Algemene Verordening Gegevensbescherming (AVG).

Het informatiebeveiligingsbeleid geeft kaders en richting over hoe we zorgen dat we blijven voldoen aan de verschillende wettelijke normen en voorschriften op het gebied van informatiebeveiliging en hoe we omgaan met afwegingen op dat vlak.

Beoogd(e) doel(en)

Grip houden op de informatiehuishouding en het applicatielandschap, zodat het de organisatie richting geeft bij het nemen van beslissingen op het gebied van informatiemanagement voor de periode 2023-2025.

Weert,
21 maart 2023

S AV		B RV	W MvdH	W WvE	W SW	W LS	W MF
	akkoord						
	bespreken						

Soort besluit: Besluit college

In te vullen door het B&W secretariaat:

☒ Akkoord
☐ Akkoord met tekstuele aanpassing door portefeuillehouder
☐ Anders, nl.:
☐ Niet akkoord
☐ Gewijzigde versie

Beslissing d.d.: 21 maart 2023 Nummer: S

De secretaris,

Invulling geven en daarmee blijven voldoen aan de Algemene Verordening Gegevensbescherming (AVG).

Borgen van de beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening, om zo een optimale dienstverlening aan burgers, bedrijven en samenwerkingspartners te kunnen leveren.

Te behalen resultaten

Er wordt in 2025 een aantoonbare verbetering van de informatiekwaliteit gerealiseerd ten opzichte van de nulmeting van 2022.

Structureel gebruik van strategische/tactische Business Intelligence informatie is in 2025 ingebed in beleidsvraagstukken.

Digivaardigheid is opgenomen in het onboarding programma van 2025.

Onze nieuwe en geactualiseerde plannen en strategieën op het gebied van informatiemanagement, privacy en informatiebeveiliging zijn uiterlijk 2025 bepaald, gecommuniceerd en bekend in de organisatie.

We bereiken in 2025 een adequaat privacyvolwassenheidsniveau op alle privacy-thema's genoemd in het borgingsproduct van de Informatie Beveiligings Dienst (niveau 3: bewust bekwaam).

Alle maatregelen in het kader van informatiebeveiliging zijn zo beschreven dat wordt voldaan aan het normenkader van de Baseline Informatiebeveiliging Overheid (BIO).

Er wordt een positief resultaat gehaald bij de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA).

Uit te voeren activiteiten

Uitvoeren Programma Innovatie 2022-2024
Binnen dit programma wordt de digitale samenwerkingsomgeving vormgegeven en wordt invulling gegeven aan het project digitaal samen informatie beheren.

Uitwerken strategieën op het gebied van informatiemanagement
Dit heeft betrekking op alle strategieën die nodig zijn om vast te stellen hoe we om willen gaan met de huidige ontwikkelingen en onze eigen ambities op het gebied van innovatieve ontwikkelingen. Onder deze ambities valt ook het professionaliseren en verbreden van Business Intelligence toepassingen.

Digivaardigheid verbeteren
We bieden gericht trainingen aan om digivaardigheid op het vlak van digitaal en zaakgericht samenwerken te verbeteren.

Jaarlijks actualiseren van het privacyplan
Naast het aangepaste privacybeleid actualiseren we jaarlijks het privacyplan met behulp van het borgingsproduct van de Informatie Beveiligings Dienst.

Invoeren van Baseline Informatiebeveiliging Overheid maatregelen
Op basis van risicoanalyses invoeren van maatregelen informatiebeveiliging (conform de landelijke Baseline Informatiebeveiliging Overheid standaard).

Argumenten

1.1. We voldoen aantoonbaar aan wettelijke verplichtingen rondom informatiemanagement.
Door te werken conform het informatie- en kwaliteitsbeleid voldoen we aan normen op het gebied van archivering en vernietiging.

1.2. We zorgen voor een flexibele en transparante organisatie.
Door grip te houden op informatie kunnen we inzicht geven in de status van processen, hierover communiceren en data ter beschikking stellen. Ook kunnen we zo snel inspelen op maatschappelijke en technologische ontwikkelingen.

1.3. We zijn betrokken en zorgen voor goede dienstverlening.
We zorgen dat inwoners meer zelf kunnen regelen en beter op de hoogte zijn. Door grip te houden op architectuur bieden we een goede informatiepositie voor inwoners en kunnen we processen optimaliseren ten behoeve van de dienstverlening.

2.1. Inwoners en medewerkers kunnen blijven vertrouwen op een zorgvuldige omgang met hun persoonsgegevens.
Het geactualiseerd privacybeleid geeft de medewerkers de juiste handvatten om zorgvuldig om te gaan met persoonsgegevens.

2.2. We mitigeren risico's op imagoverlies, juridisch en financieel gebied.
Het geactualiseerd privacybeleid geeft de medewerkers de juiste handvaten om op een zorgvuldige wijze te werken met persoonsgegevens. Hierdoor worden boetes van rechtbanken/de nationale toezichthouder gemitigeerd.

3.1. Inwoners kunnen blijven vertrouwen op veilige omgang met hun gegevens.
Door te werken conform een geactualiseerd informatiebeveiligingsbeleid kunnen wij hun vertrouwelijke gegevens afdoende beveiligen. Voor dit beleid is de Baseline Informatiebeveiliging Overheid als uitgangspunt genomen en aangescherpt op een aantal punten.

3.2. We zorgen dat we een positief resultaat krijgen bij de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA).
We voldoen zo aan de verplichting om een actueel en door het college vastgesteld informatiebeveiligingsplan te hebben.

Kanttekeningen en risico's

Er zijn geen kanttekeningen of risico's te benoemen bij het vaststellen van de drie beleidsstukken.

Financiële, personele en juridische gevolgen

Het vaststellen van het informatiebeleid, bestaande uit de drie beleidsdocumenten heeft geen financiële, personele of juridische gevolgen.

Overleg gevoerd met

Intern:
Ron Meerts (Afdelingshoofd Informatie)
Menno Spijker (Informatieadviseur)
Nico Murk (Expert Informatiebeheer)
Marco van Dijk (Innovatiemanager)
Sandra Metten (Functionaris Gegevensbescherming)

Janine Wolters (Privacy Officer)
Natascha Westen (Chief Information Security Officer)
John Bijnen (Procesmanager)
Hamid Dardour (Gegevensbeheerder)

Extern:
Niet van toepassing.

Participatie

Niet van toepassing, deze drie beleidsstukken hebben betrekking op de interne bedrijfsvoering.

Communicatie

De afdelingen zijn geïnformeerd over de beleidsstukken van het informatiebeleid. Door regelmatig met de afdelingen in gesprek te blijven borgen we de beoogde doelen. (Grip houden op de informatie architectuur en in control zijn, informatieveiligheid en privacy.)

De drie beleidsstukken worden nadat ze zijn vastgesteld gecommuniceerd op Octo.

Planning

Het informatiebeleid geldt vanaf moment van besluitvorming tot en met 2026.

Het privacybeleid geldt vanaf het moment van besluitvorming tot en met 2026.

Het informatiebeveiligingsbeleid geldt tot en met 2023. Jaarlijks wordt een evaluatie uitgevoerd op dit beleid, waarna het opnieuw wordt vastgesteld.

Met de vaststelling van deze beleidsdocumenten worden alle voorgaande versies van deze beleidsdocumenten vervangen.

Evaluatie

Voor dit beleid of een van de afzonderlijke onderdelen gelden de wettelijke evaluatiemomenten waar het rijk in voorziet zoals het normenkader van de beheerder van MijnOverheid (Logius), de Eenduidige Normatiek Single Information Audit (ENSIA) en andere audits.

Voor alle drie beleidsstukken kan er een tussentijdse herziening of addendum ter besluitvorming voorgelegd worden. Dit vanwege maatschappelijke-, wettelijke- en technologische ontwikkelingen.

Bijlage(n)

1. Informatie- en kwaliteitsbeleid
2. Privacybeleid
3. Informatiebeveiligingsbeleid
4. Aanpassingen privacybeleid en Informatiebeveiligingsbeleid
5. Bijlage A: De 10 bestuurlijke principes voor informatiebeveiliging
6. Bijlage B: Dreigingsbeeld informatiebeveiliging