Agendapunt: 07.

Onderwerp:	Nieuw Informatieveiligheid en privacybeleid
Datum:	4 december 2025
Portefeuillehouder:	Dhr. A. van der Tuuk
Sector:	Bedrijfsvoering
Bijlage(n):	1. Informatieveiligheid en privacybeleid 2025
Ter besluitvorming/ter bespreking/ter informatie:	Ter informatie

Gevraagd besluit

Het Algemeen Bestuur wordt gevraagd:

- Kennis te nemen van het (vernieuwde) Informatieveiligheid en privacybeleid van de VRG.

Toelichting voorstel

Toelichting voorstel
Op het gebied van Informatieveiligheid en privacy gaan de ontwikkelingen snel. Om te zorgen dat de VRG zo goed mogelijk beschermd is tegen cybercriminaliteit en voldoet aan wet- en regelgeving is er nieuw Informatieveiligheid en privacybeleid opgesteld. In het beleid is nu expliciet opgenomen dat het Algemeen Bestuur van de VRG middels een jaarrapportage wordt geïnformeerd over eventuele incidenten en afwijkingen, en dat een vooruitblik wordt gegeven naar de nieuwe ontwikkelingen op het gebied van Informatieveiligheid en Privacy.

(Historische) context
Eind 2019 heeft de VRG het beleid inzake informatieveiligheid en privacy vastgesteld. In de daaropvolgende jaren zijn diverse onderdelen geactualiseerd. Ter bevordering van de onderlinge samenhang en om de leesbaarheid te vergroten, is besloten het beleidsdocument integraal te herzien. Het herziene beleidsdocument is als bijlage bij deze oplegger opgenomen.

Motivering
In dit nieuwe beleid is niet alleen rekening gehouden met de geldende wet- en regelgeving, maar tevens met de koers die landelijk is uitgezet binnen het programma Informatiegestuurde Veiligheid (IGV). Hiermee wordt beoogd de samenwerking en informatie-uitwisseling met andere regio's zo efficiënt en effectief mogelijk te organiseren.

Waar het eerdere beleid voornamelijk was gericht op het ontwikkelen en implementeren van afzonderlijke procedures, legt dit herziene beleid nadrukkelijk de focus op de werking en effectiviteit van het geheel. Procedures en maatregelen worden periodiek getoetst en geëvalueerd, en waar nodig aangepast.

Deze werkwijze draagt bij aan een continue ontwikkeling van de organisatie en leidt tot een structurele verhoging van het volwassenheidsniveau van de VRG op het gebied van informatieveiligheid en privacy.

Kanttekeningen/risico's
Het nieuwe beleid vormt het overkoepelende strategische kader voor informatieveiligheid en privacy binnen de VRG. In dit beleid wordt niet alleen uiteengezet waarom de organisatie verantwoordelijkheid moet nemen op dit terrein, maar worden tevens de rollen en verantwoordelijkheden van zowel managers als medewerkers helder beschreven.

De naleving van deze verantwoordelijkheden is van cruciaal belang. Hoewel technische en organisatorische maatregelen onmisbaar zijn, blijft menselijk handelen een bepalende factor. Menselijk gedrag vormt nog altijd één van de kwetsbaarste schakels in de waarborging van cyberveiligheid. Het is daarom noodzakelijk dat iedere medewerker zich bewust is van zijn of haar rol en consequent handelt in lijn met de afgesproken kaders. Alleen op die manier kan de VRG de integriteit, vertrouwelijkheid en beschikbaarheid van informatie duurzaam borgen.

Financiële paragraaf
Er zijn met dit voorstel geen extra kosten gepaard. Vanuit Informatieveiligheid en privacy worden in het jaarplan van IM/ICT financiële middelen geraamd voor diverse werkzaamheden/projecten.

Vervolgtraject
VRG is reeds gestart met het implementeren en uitrollen van de diverse onderdelen die raken aan informatieveiligheid en privacy, zoals beschreven in het (vernieuwde) beleid.

Afstemming/consequenties

	Afgestemd	Consequenties
Juridisch	☐	
Financieel	☐	
Personeel	☐	
IM/ICT	☒	De strategische koers zoals geschetst in het beleid past binnen de plannen van team IM/ICT.
Communicatie	☒	Naast een presentatie van het beleid aan de OR, worden de onderdelen die impact hebben op de medewerkers in de organisatie o.a. via berichten op VRGnet en de beveiligingsbeheerders gedeeld en toegelicht.
Inkoop	☐	
Overig	☐	