Gemeente
Soest

Rekenkamercommissie Soest
Arco de Baat
Postbus 2000
3760 CA Soest

Soest, 11 februari 2025 Verzonden: 12 februari 2025

Behandeld door : Marloes Klooster
Zaaknummer : 1059499
Onderwerp : Rekenkameronderzoek Informatieveiligheid

Beste Arco de Baat,

Op 17 januari 2025 heeft u ons de resultaten van uw onderzoek naar het Informatiebeveiligingsbeleid van de gemeente Soest gestuurd. In uw brief vraagt u ons in het kader van bestuurlijk hoor en wederhoor om een inhoudelijke reactie op de conclusies en aanbevelingen in uw rapport. In deze brief leest u onze reactie op uw rapport.

Voordat wij inhoudelijk op uw rapport reageren willen wij onze oprechte waardering uitspreken voor de inspanningen van de Rekenkamer. Uw bevindingen en aanbevelingen hebben wij dan ook aandachtig gelezen.

Zoals u ook in het onderzoeksrapport aangeeft, heeft uw onderzoek plaatsgevonden in een periode waarin wij diverse stappen aan het nemen waren om in te spelen op de huidige ontwikkelingen. Na oktober 2024 is de inzet van de ambtelijke organisatie verder voortgezet. Wij nemen uw conclusies en aanbevelingen mee in het licht van continu verbeteren van onze kennis, kunde en organisatie van dit thema.

Reactie op conclusies en aanbevelingen

In het onderzoeksrapport worden een aantal conclusies getrokken. Deze conclusies herkennen wij grotendeels. Voor een deel vragen deze conclusies wat nuancering. Het strategisch beleidsplan hebben wij in het najaar 2024 vastgesteld. De uitwerking en uitvoering hiervan wordt op dit moment door de organisatie verder opgepakt. Binnenkort ontvangen wij ook de definitieve uitkomsten van de BIO-nulmeting. De uitkomsten van dit onderzoek en de BIO-nulmeting vormen voor de organisatie handvatten om vervolgacties te nemen, zodat de informatieveiligheid verder verbeterd kan worden. We groeien toe naar volwassenheidsniveau 4.

In het onderzoeksrapport wordt ook ingegaan op de bewustwording van informatieveiligheid bij onze medewerkers. De afgelopen periode is hier invulling aan gegeven. Dit doen we op verschillende manieren. Zo ontvangen alle medewerkers wekelijks een vraag over informatieveiligheid. Middels monitoring wordt de deelname en kennisniveau gemonitord en

waar nodig bijgestuurd. Ook volgen alle nieuwe medewerkers trainingen en dit jaar krijgt ook al het zittende personeel een (herhaal)training. Op deze manier proberen we medewerkers bewust te laten zijn van de risico's die wij lopen op het gebied van informatieveiligheid en hen bekend te laten zijn met de stappen die ze moeten nemen op het moment dat er sprake is bijvoorbeeld een datalek of phishingmail.

Onderstaand geven wij een beknopte reactie op uw aanbevelingen.

1. *Investeer in een robuuste digitale veiligheidsorganisatie*

Zoals aangegeven, gaan de ontwikkelingen op het gebied van informatieveiligheid snel. De komende periode geven we nader invulling aan ons strategisch beleid, waarin ook de rol en taken van het lijnmanagement nader zijn uitgewerkt. In de aanbevelingen wordt aangegeven dat er geïnvesteerd moet worden in de tweede en derde lijn van het 'three lines'model, waaronder de functies van CISO, FG en PO, om de benodigde inhaalslag te maken. We zijn aan het onderzoeken op welke wijze deze bestaande functies het beste ingevuld kunnen worden. Hierbij werken we ook samen in de regio, met de RID deelnemers. Gezamenlijk wordt kennis uitgewisseld en worden instrumenten ontwikkeld.

2. *Stel op basis van het strategisch beleid een 'aanvalsplan' Digitale Veiligheid op dat erop gericht is om aan de wettelijke verplichtingen te voldoen*

In het onderzoeksrapport wordt de aanbeveling gedaan om voor 2025 een aanvalsplan Digitale Veiligheid op te stellen. Zoals hiervoor aangegeven gaan we aan de slag met de vertaling van het strategische beleid en de uitkomsten van de BIO-nulmeting om vervolgstappen te nemen. Doel van deze vervolgacties is om door te groeien naar volwassenheidsniveau 4. We stellen voor de raad via de P&C cyclus, in de paragraaf Bedrijfsvoering, te informeren over de voortgang en uitvoering.

3. *Ontwikkel in samenwerking met de raad een begrijpelijke rapportage gebaseerd op gangbare normenkaders, risico's en kosten*

In het rapport doet u de aanbeveling om een jaarlijkse rapportage op te stellen over de stand van zaken van de informatieveiligheid. Deze aanbeveling nemen wij graag over. We zullen in overleg met de agendacommissie van de raad een informatiebijeenkomst plannen.

Heeft u nog vragen of opmerkingen over deze brief?

Dan kunt u terecht bij Marloes Klooster, manager bedrijfsvoering. Bellen kan op werkdagen tot 12.30 uur op 035-609 34 11. Mailen kan via het contactformulier op soest.nl/contact. Tip: noem uw zaaknummer. Dan kunnen wij u sneller helpen.

Met vriendelijke groet,

Burgemeester en wethouders

LV
11-02-2025
Leontine Vermond

Gemeentesecretaris

RM
11-02-2025
Rob Metz

Burgemeester