Home

Assurance-rapport

Inzake de collegeverklaring ENSIA 2025 van de gemeente Amsterdam en de bijlage Suwinet waarnaar in de collegeverklaring naar verwezen wordt



Auditdienst ACAM

Inhoudsopgave

Aanbieding 3

Hoofdstuk 1 Assurance-rapport 4

Aanbieding



Aan het college van burgemeester en
wethouders van gemeente Amsterdam
Amstel 1
1011 PN Amsterdam

Datum	17 april 2026
Kenmerk	716.600.25-R
Onderwerp	Assurance-rapport over de collegeverklaring ENSIA 2025 van gemeente Amsterdam

Geacht college,

Hierbij ontvangt u het assurance-rapport inzake de collegeverklaring ENSIA 2025 en de bijlage Suwinet waarnaar wordt verwezen in de collegeverklaring van gemeente Amsterdam.

Wij vertrouwen erop dat wij u met dit rapport voldoende hebben geïnformeerd en zijn graag bereid tot een nadere toelichting.

ARJAN PASCAL SUIJKER

A.P. Suijker MSc CISA RA RE
Auditdienst ACAM

Hoofdstuk 1 **Assurance-rapport van de onafhankelijke IT-auditor**

Assurance over de collegeverklaring ENSIA 2025 van gemeente Amsterdam en de bijlage Suwinet waarnaar in de collegeverklaring wordt verwezen



Aan het college van burgemeester en wethouders van de gemeente Amsterdam

Ons oordeel
Ingevolge uw opdracht hebben wij de bijgevoegde collegeverklaring ENSIA 2025 inzake Informatiebeveiliging van Suwinet (hierna: collegeverklaring), inclusief de bijlage Suwinet waarnaar in de collegeverklaring wordt verwezen, van gemeente Amsterdam gecontroleerd.

Naar ons oordeel is de bijgevoegde collegeverklaring, inclusief de bijlage Suwinet waarnaar in de collegeverklaring wordt verwezen, van gemeente Amsterdam, in alle van materieel belang zijnde aspecten, juist.

De basis voor ons oordeel
Wij hebben ons onderzoek uitgevoerd volgens Nederlands recht, de NOREA Richtlijn 3000A "Assurance-opdrachten door IT-auditors (Attest-opdrachten)" en de NOREA Handreiking ENSIA voor IT-auditors (RE's) versie 6.0 d.d. 30 september 2025. Deze opdracht is gericht op het verkrijgen van een redelijke mate van zekerheid. Onze verantwoordelijkheden op grond hiervan zijn beschreven in de sectie 'Verantwoordelijkheden van de IT-auditor'.

Wij zijn onafhankelijk van gemeente Amsterdam en hebben voldaan aan de overige vereisten van het Reglement Gedragscode ('Code of Ethics') van NOREA.

Wij vinden dat de door ons verkregen assurance-informatie voldoende en geschikt is als basis voor ons oordeel.

Object van onderzoek
Met de collegeverklaring geeft het college van burgemeester en wethouders, aan in welke mate de gemeente voldoet aan de informatiebeveiligingsnormen voor Suwinet. De collegeverklaring maakt onderdeel uit van de verantwoording over informatiebeveiliging middels ENSIA en is tot stand gekomen door een zelfevaluatie over de door de toezichthouder geselecteerde eisen uit de 'Baseline Informatiebeveiliging Overheid' versie 1.04zv voor Suwinet. Wij benadrukken dat het specifiek geselecteerde normen zijn en daarmee geen uitspraak wordt gedaan over de informatiebeveiliging als geheel.

Betreffende Suwinet gaat de verantwoording over de opzet en het bestaan van de interne beheersingsmaatregelen per 31 december 2025.

Scope
De scope van ons onderzoek bestond uit de hierna genoemde Suwinet gegevensverwerkingen:

Gebruik van Suwinet voor SUWI-taken

Taak
Participatiewet (Pw)
Inkomensvoorziening voor Oudere en gedeeltelijk Arbeidsongeschikte Werknemers (IOAW)
Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen (IOAZ)

Gebruik van Suwinet voor niet-SUWI-taken

Taak
Hulp aan voortijdig schoolverlaters door het Doorstroompunt
Onderzoek loonbeslag door Gemeentelijke Belastingdeurwaarders
Adresonderzoek door Burgerzaken
Regeling opvang ontheemden Oekraïne

Wij hebben geen onderzoek uitgevoerd naar hierboven niet genoemde gegevensverwerkingen Suwinet en doen daar derhalve ook geen uitspraak over.

Benadrukking aangelegenheden
Wij hebben vastgesteld dat de op de uitzonderingen gerichte beheersingsmaatregelen in verbeterplannen zijn opgenomen, zijn belegd en worden gemonitord. Ons onderzoek heeft zich niet gericht op de juistheid, volledigheid en uitvoering van de verbeterplannen. Ons oordeel is niet aangepast als gevolg van deze aangelegenheid.

Beoogde gebruikers en doel
Ons assurance-rapport is bestemd voor gebruikers van de collegeverklaring. De collegeverklaring is opgesteld voor de gemeenteraad en voor de departementen en aangewezen uitvoeringsinstanties die toezien op de veiligheid van Suwinet. Doel van de collegeverklaring is om de gemeenteraad en de departementen die toezien op de veiligheid van Suwinet te informeren over het voldoen aan de geselecteerde normen Suwinet.

Ons assurance-rapport mag enkel worden gebruikt door de beoogde gebruikers voor het doel waarvoor het is opgesteld en dient niet te worden verspreid aan of te worden gebruikt door anderen.

Verantwoordelijkheden van het college van gemeente Amsterdam
Het college van burgemeester en wethouders van gemeente Amsterdam is verantwoordelijk voor het opstellen van de collegeverklaring.

Het college is ook verantwoordelijk voor een zodanige interne beheersing als het noodzakelijk acht om het opstellen van de collegeverklaring mogelijk te maken zonder afwijkingen van materieel belang als gevolg van fraude of fouten.

Verantwoordelijkheden van de IT auditor
Onze verantwoordelijkheid is het zodanig plannen en uitvoeren van ons onderzoek dat wij daarmee voldoende en geschikte assurance-informatie verkrijgen voor het door ons af te geven oordeel.

Ons onderzoek is uitgevoerd met een hoge mate maar geen absolute mate van zekerheid waardoor het mogelijk is dat wij tijdens ons onderzoek niet alle materiële afwijkingen als gevolg van fraude of fouten ontdekken. Afwijkingen kunnen ontstaan als gevolg van fraude of fouten en zijn materieel indien redelijkerwijs kan worden verwacht dat deze, afzonderlijk of gezamenlijk, van invloed kunnen zijn op de beslissingen die gebruikers op basis van de collegeverklaring nemen. De materialiteit beïnvloedt de aard, timing en omvang van onze assurance-werkzaamheden en de evaluatie van het effect van onderkende afwijkingen op ons oordeel.

Onze assurance-opdracht bestond onder andere uit:

- het verkrijgen van kennis omtrent de collegeverklaring en andere omstandigheden rond de opdracht waaronder het verkrijgen van kennis omtrent de interne beheersingsmaatregelen;
- het op basis van deze kennis inschatten van de risico's dat de collegeverklaring afwijkingen van materieel belang bevat;
- het reageren op de ingeschatte risico's, waaronder het ontwikkelen van een algehele aanpak, en het bepalen van de aard, de tijdsfasering en de omvang van verdere procedures;
- het uitvoeren van verdere procedures die duidelijk zijn gekoppeld aan de gesignaleerde risico's, waarbij gebruik wordt gemaakt van een combinatie van inspectie, waarnemingen ter plaatse en inwinnen van inlichtingen;
- het evalueren of de collegeverklaring een getrouw beeld geeft van de onderliggende beheersingsmaatregelen en uitgevoerde werkzaamheden; en
- het evalueren van de uitkomsten van onze werkzaamheden.

Amsterdam, 17 april 2026

ARJAN PASCAL SUIJKER Digitally signed by ARJAN PASCAL SUIJKER
Date: 2026-04-17 16:45:07+02:00

A.P. Suijker MSc CISA RA RE
Auditdienst ACAM



Auditdienst ACAM
Oudezijds Voorburgwal 300
1012 GL Amsterdam
Postbus 1078
1000 BB Amsterdam
Telefoon (020) 2549000
Email info.acam@amsterdam.nl

Gemeente Amsterdam

Collegeverklaring informatiebeveiliging Suwinet 2025



Gemeente Amsterdam

Collegeverklaring informatiebeveiliging Suwinet 2025

Gemeente Amsterdam

Doel en achtergrond verklaring
De aansluitingen die we als gemeente op Suwinet hebben, vereisen dat voorzieningen moeten zijn beveiligd en (privacygevoelige) data moet worden beschermd tegen onrechtmatig gebruik. De gemeente treft interne beheersingsmaatregelen om veilig gebruik te maken van deze aansluitingen.

Met deze verklaring geeft het college van Burgemeester en Wethouders aan in welke mate de gemeente Amsterdam voldoet aan de informatiebeveiligingsnormen voor Suwinet. Deze verklaring maakt onderdeel uit van de verantwoording via de ENSIA-systematiek en is tot stand gekomen door een audit op informatiebeveiligingsnormen gebaseerd op de door de landelijk toezichthouder geselecteerde eisen uit de Baseline Informatiebeveiliging Overheid versie 1.04zv voor Suwinet.
De inhoud van deze collegeverklaring is getoetst door een onafhankelijke IT-auditor/RE.

Deze verklaring is bestemd voor de toezichthouder van Suwinet, te weten het Ministerie van Sociale Zaken en Werkgelegenheid via het Bureau Keteninformatie Werk en Inkomen (BKWI) alsmede de stelselhouder: het ministerie van Sociale Zaken en Werkgelegenheid.

Reikwijdte en diepgang verklaring
De aansluitingen die we als gemeentelijke organisatie op Suwinet hebben, vereisen dat onze voorzieningen moeten zijn beveiligd en dat (privacygevoelige) data moet worden beschermd tegen onrechtmatig gebruik. Hiervoor stellen de stelselhouders een aantal informatiebeveiligingsnormen verplicht. De gemeentelijke organisatie moet interne beheersingsmaatregelen treffen om te voldoen aan deze gestelde normen teneinde gebruik te mogen blijven maken van deze aansluitingen.

De audit gaat over de opzet en het bestaan van deze beheersingsmaatregelen om te kunnen voldoen aan de relevante beveiligingsnormen voor Suwinet op 31 december 2025.

Voor Suwinet wordt de Verantwoordingsrichtlijn GeVS 2025 gehanteerd waarin zijn opgenomen de geselecteerde eisen uit de 'Baseline Informatiebeveiliging Overheid' versie 1.04zv.
Deze Verantwoordingsrichtlijn betreft opzet, bestaan en optioneel voor 7 maatregelen de werking van de interne beheersingsmaatregelen.

Gemeente Amsterdam

Collegeverklaring en samenvattend beeld van de auditbevindingen

Verklaring / Conclusie
Het college van Burgemeester en Wethouders van de gemeente Amsterdam verklaart dat de gemeentelijke organisatie op 31 december 2025 niet voldoet aan alle geselecteerde normen inzake Suwinet.

Samenvattend beeld
Deze collegeverklaring betreffende de gemeentelijke organisatie en de serviceorganisaties dekt de geselecteerde normen inzake Suwinet af. Het detailoverzicht van normen en of we hier als gemeente aan voldoen, is opgenomen in de volgende bijlagen:

- Verantwoording Suwinet 2025 met kenmerk AD2026-015888

Onderwerp	Wordt aan alle normen voldaan?	Zijn de uitzonderingen in verbeterplannen opgenomen en zijn de verbetermaatregelen belegd en worden deze gemonitord?
Suwinet voor SUWI-taken	Nee	Ja
Suwinet voor niet-SUWI-taken	Nee	Ja

Namens het college van Burgemeester en Wethouders gemeente Amsterdam

Amsterdam, 31 maart 2026

Femke Halsema
Burgemeester

Gemeente Amsterdam

Bijlage: Gebruik van Suwinet
Kenmerk: AD2026-015888
Classificatie: openbaar

Deze bijlage is een afzonderlijk onderdeel van de Verantwoording informatiebeveiliging Suwinet per 31-12-2025 van de gemeente Amsterdam. Onderwerp van de verantwoording is het gebruik van Suwinet. Deze verantwoording heeft betrekking op de Verantwoordingsrichtlijn GeVS 2025 die is gebaseerd op geselecteerde controls uit de Baseline Informatieveiligheid Overheid (BIO), meer in het bijzonder de in het kader van ENSIA geselecteerde controls.

Suwinet-gegevens worden ten behoeve van de dienstverlening door de gemeente Amsterdam verwerkt. Hierbij is de eventuele aanwezigheid van IT-serviceorganisaties in aanmerking genomen.

Gebruik van Suwinet voor SUWI-taken

Voor de volgende taken wordt Suwinet op de volgende plaatsen gebruikt:

Taak	Organisatie	TPM/AR
Participatiewet (Pw)*	Binnen de gemeente	Nee
Inkomensvoorziening voor Oudere en gedeeltelijk Arbeidsongeschikte Werknemers (IOAW)	Binnen de gemeente	Nee
Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen (IOAZ)	Binnen de gemeente	Nee
Wet gemeentelijke schuldhulpverlening (Wgs)	Niet van toepassing	Niet van toepassing
Uitvoeren bijzondere bijstand	Niet van toepassing	Niet van toepassing
Uitvoeren bezoldiging zelfstandigen	Niet van toepassing	Niet van toepassing
Sociale recherche	Niet van toepassing	Niet van toepassing

*De gemeente Amsterdam gebruikt de inkijkfunctie van Suwinet ook voor enkele gemeentelijke regelingen die buiten de kaders van de Participatiewet vallen; daardoor ontbreekt de wettelijke grondslag.

Gemeente Amsterdam

Gebruik van Suwinet voor niet-SUWI-taken

Voor de volgende niet-SUWI-taken wordt Suwinet op de volgende plaatsen gebruikt:

Taak	Organisatie	TPM/AR
Hulp aan vroegtijdig schoolverlaters door het Doorstroompunt	Doorstroompuntregio Agglomeratie Amsterdam	Niet van toepassing
Onderzoek loonbeslag door Gemeentelijke Belastingdeurwaarders	Binnen de gemeente	Niet van toepassing
Adresonderzoek door Burgerzaken	Binnen de gemeente	Niet van toepassing
Regeling opvang ontheemden Oekraïne	Binnen de gemeente	Niet van toepassing

Gemeente Amsterdam

Naleving BIO-maatregelen voor de Suwi-taken en niet-Suwi-taken

Met uitzondering van de volgende maatregelen voldoen de interne beheersingsmaatregelen voor de SUWI-taken op 31 december 2025 in opzet en bestaan aan de doelstellingen uit de verantwoordingsrichtlijn GeVS 2025:

Organisatie	SUWI-taak	BIO-maatregel	Risico	Applicatie
Binnen de gemeente	Inkijken - Participatiewet (Pw), Inkomensvoorziening voor Oudere en gedeeltelijk Arbeidsongeschikte Werknemers (IOAW), Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen (IOAZ)	5.1.2.1 Het informatiebeveiligingsbeleid wordt periodiek en in aansluiting bij de (bestaande) bestuurs- en P&C-cycli en externe ontwikkelingen beoordeeld en zo nodig bijgesteld. 7.2.2.2 Alle medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten hebben binnen drie maanden na indiensttreding een training I-bewustzijn succesvol gevolgd	De getroffen beveiligingsmaatregelen kunnen ontoereikend zijn in relatie tot aangescherpte wetgeving, verandering van risicoklasse van gegevens en de toegepaste technologieën. Indien gebruikers van Suwinet-gegevens zich niet of onvoldoende bewust zijn van de (hoge) vertrouwelijkheid, bestaat het risico dat deze gegevens onvoldoende worden beschermd.	Suwinet-Inkijk
Binnen de gemeente	Inlezen - Pw, IOAW, IOAZ	5.1.2.1 Het informatiebeveiligingsbeleid wordt periodiek en in aansluiting bij de (bestaande) bestuurs- en P&C-cycli en externe ontwikkelingen beoordeeld en zo nodig bijgesteld. 7.2.2.2 Alle medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten hebben binnen drie maanden na indiensttreding een training I-bewustzijn succesvol gevolgd. 10.1.1 Beleid inzake het gebruik van cryptografische beheers-maatregelen.	De getroffen beveiligingsmaatregelen kunnen ontoereikend zijn in relatie tot aangescherpte wetgeving, verandering van risicoklasse van gegevens en de toegepaste technologieën. Indien gebruikers van Suwinet gegevens zich niet of onvoldoende bewust zijn van de (hoge) vertrouwelijkheid, bestaat het risico dat deze gegevens onvoldoende worden beschermd. Ondanks het besloten karakter van Suwinet bestaat het risico dat de toegang tot gegevens niet adequaat is beschermd.	DKD-Inlezen ZorgNed

Gemeente Amsterdam

Met uitzondering van de volgende normen voldoen de interne beheersingsmaatregelen voor de niet-SUWI-taken in opzet en bestaan aan alle geselecteerde normen:

Organisatie	Niet-SUWI-taak	BIO-maatregel	Risico	Appli-catie
Binnen de gemeente, agglomera-tie Amsterdam	Hulp aan vroegtijdig schoolverlaters door Doorstroompunt	5.1.2.1 Het informatiebeveiligingsbeleid wordt periodiek en in aansluiting bij de (bestaande) bestuurs- en P&C-cycli en externe ontwikkelingen beoordeeld en zo nodig bijgesteld. 9.2.5.2 De opvolging van bevindingen is gedocumenteerd en wordt behandeld als beveiligingsincident.	De getroffen beveiligingsmaatregelen kunnen ontoereikend zijn in relatie tot aangescherpte wetgeving, verandering van risicoklasse van gegevens en de toegepaste technologieën. Bij het ontbreken controles op het gebruik van autorisaties wordt misbruik niet gesignaleerd.	Suwinet-Inkijk Door-stroom-punt
Binnen de gemeente	Onderzoek loonbeslag door gemeentelijke Belastingdeurwaarders	5.1.2.1 Het informatiebeveiligingsbeleid wordt periodiek en in aansluiting bij de (bestaande) bestuurs- en P&C-cycli en externe ontwikkelingen beoordeeld en zo nodig bijgesteld.	De getroffen beveiligingsmaatregelen kunnen ontoereikend zijn in relatie tot aangescherpte wetgeving, verandering van risicoklasse van gegevens en de toegepaste technologieën.	Suwinet-Inkijk Belasting deurwaarders
Binnen de gemeente	Adresonderzoek door Burgerzaken	5.1.2.1 Het informatiebeveiligingsbeleid wordt periodiek en in aansluiting bij de (bestaande) bestuurs- en P&C-cycli en externe ontwikkelingen beoordeeld en zo nodig bijgesteld. 6.1.2.1 Er zijn maatregelen getroffen die onbedoelde of ongeautoriseerde toegang tot bedrijfsmiddelen* waarnemen of voorkomen. * Onder bedrijfsmiddelen worden in dit verband de Suwinet gegevens (mede) begrepen. 7.2.2.2 Alle medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten hebben binnen drie maanden na indiensttreding een training I-bewustzijn succesvol gevolgd.. 9.2.5.2 De opvolging van bevindingen is gedocumenteerd en wordt behandeld als beveiligings-incident.	De getroffen beveiligingsmaatregelen kunnen ontoereikend zijn in relatie tot aangescherpte wetgeving, verandering van risicoklasse van gegevens en de toegepaste technologieën. Onduidelijke taken en verantwoordelijkheden en het ontbreken van juiste functie-scheiding kunnen leiden tot misbruik van bevoegdheden, te ruim toegekende bevoegdheden, over het hoofd zien van en/of tot implementatie van tegenstrijdige beveiligingsmaatregelen. Indien gebruikers van Suwinet gegevens zich niet of onvoldoende bewust zijn van de (hoge) vertrouwelijkheid, bestaat het risico dat deze gegevens onvoldoende worden beschermd. Bij het ontbreken controles op het gebruik van autorisaties wordt misbruik niet gesignaleerd. Als toegangsrechten niet bijtijds worden beëindigd of gewijzigd,	Suwinet-Inkijk Adres-onder-zoek

Organisatie	Niet-SUWI-taak	BIO-maatregel	Risico	Appli-catie
		9.2.5.3 Alle uitgegeven toegangsrechten worden minimaal eenmaal per halfjaar beoordeeld. 9.2.6 Aanvullende maatregel: Het lijnmanagement heeft een procedure vastgesteld en geïmplementeerd voor verandering van functie binnen de organisatie, waarin minimaal aandacht besteed wordt aan het intrekken van toegangsrechten en innemen van bedrijfsmiddelen die niet meer nodig zijn na het beëindigen van de oude functie 18.1.4.2 Organisaties controleren regelmatig de naleving van de privacyregels en informatieverwerking en -procedures binnen hun verantwoordelijkheidsgebied aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	bestaat het risico op onbevoegde kennisname van Suwinet gegevens. Als de verwerking van Suwinet (persoons)gegevens niet overeenkomstig toepasselijke wet- en regelgeving plaatsvindt, wordt hierdoor de AVG overtreden.	

Gemeente Amsterdam

Organisatie	Niet-SUWI-taak	BIO-maatregel	Risico	Appli-catie
Binnen de gemeente	Regeling opvang ontheemden Oekraïne	5.1.2.1 Het informatiebeveiligingsbeleid wordt periodiek en in aansluiting bij de (bestaande) bestuurs- en P&C-cycli en externe ontwikkelingen beoordeeld en zo nodig bijgesteld.	De getroffen beveiligingsmaatregelen kunnen ontoereikend zijn in relatie tot aangescherpte wetgeving, verandering van risicoklasse van gegevens en de toegepaste technologieën.	Suwinet-Inkijk RooO
		6.1.1.1 De leiding van de organisatie heeft vastgelegd wat de verantwoordelijkheden en rollen zijn op het gebied van informatiebeveiliging binnen haar organisatie.	Het risico bestaat dat door gebrek aan coördinatie van activiteiten niet op beveiligingsincidenten wordt geacteerd en dat door wijzigingen nieuwe kwetsbaarheden ontstaan.	
		6.1.2.1 Er zijn maatregelen getroffen die onbedoelde of ongeautoriseerde toegang tot bedrijfsmiddelen* waarnemen of voorkomen. * Onder bedrijfsmiddelen worden in dit verband de Suwinet gegevens (mede) begrepen.	Onduidelijke taken en verantwoordelijkheden en het ontbreken van juiste functiescheiding kunnen leiden tot misbruik van bevoegdheden, te ruim toegekende bevoegdheden, over het hoofd zien van en/of tot implementatie van tegenstrijdige beveiligingsmaatregelen.	
		7.2.2.2 Alle medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten hebben binnen drie maanden na indiensttreding een training I-bewustzijn succesvol gevolgd.	Indien gebruikers van Suwinet gegevens zich niet of onvoldoende bewust zijn van de (hoge) vertrouwelijkheid, bestaat het risico dat deze gegevens onvoldoende worden beschermd.	