Gemeente Amsterdam

Bijlage: Gebruik van Suwinet
Kenmerk: <gemeentelijk kenmerk>
Classificatie: Openbaar

Deze bijlage is een afzonderlijk onderdeel van de collegeverklaring ENSIA Suwinet per 31-12-2024 van de gemeente Amsterdam . Onderwerp van de verantwoording is het gebruik van Suwinet. Deze vertantwoording heeft betrekking op de Verantwoordingsrichtlijn GeVS 2022 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 gemeente Amsterdam verwerkt. Hierbij is de eventuele aanwezigheid van IT-serviceorganisaties in aanmerking genomen.

Het bestuur van de gemeente Amsterdam is als opdrachtgever verantwoordelijk voor de kwaliteit en veiligheid van het gebruik van Suwinet en legt hierover verantwoording af. Gemeente Amsterdam heeft een deel van de Suwinet taken uitbesteed aan Wigo4it. Als gevolg hiervan is een aantal maatregelen belegd bij deze serviceorganisatie. In de navolgende tabellen is opgenomen of het onderzoeken over het al dan niet voldoen aan deze maatregelen is uitgevoerd door de IT-auditor van deze serviceorganisatie. De controls die betrekking hebben op de taken die belegd zijn bij de serviceorganisatie maken geen onderdeel uit van de zelfevaluatie van de gemeente Amsterdam, tenzij sprake is van een gedeelde norm.

De zelfevaluatie ENSIA voor Suwinet is toegepast op dat deel van het gebruik en normenkader dat niet onder uitbesteding aan Wigo4it valt. De overige normen worden afgedekt door onderstaande Third Party Mededeling (TPM) van Wigo4it.

Leverancier	
Naam serviceorganisatie:	Wigo4it
Referentie/rapportnummer:	24090001.01-Suwinet-DKD-Inlezen-Wigo4it
Rapportagedatum:	29 november 2024
Naam RE-auditor:	N.M. (Niels) van der Meij RE
Ondertekend door RE-auditor:	Ja

Gemeente Amsterdam

Gebruik van Suwinet voor SUWI-taken

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

Taak	Organisatie	TPM
Participatiewet (Pw)	Binnen de gemeente en samenwerkingsverband Wigo4it	Ja
Inkomensvoorziening voor Oudere en gedeeltelijk Arbeidsongeschikte Werknemers (IOAW)	Binnen de gemeente en samenwerkingsverband Wigo4it	Ja
Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen (IOAZ)	Binnen de gemeente en samenwerkingsverband Wigo4it	Ja
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

Gebruik van Suwinet voor niet-SUWI-taken

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

Taak	Organisatie	TPM
Hulp aan vroegtijdig schoolverlaters door het Doorstroompunt/Regionaal Meld- en Coördinatiecentrum (RMC)[1]	Doorstroompuntregio Agglomeratie Amsterdam	Niet van toepassing
Onderzoek loonbeslag door Gemeentelijke Belastingdeurwaarders	Binnen de gemeente	Niet van toepassing

[1] Alleen de regiogemeente moet verantwoorden en niet de aangesloten gemeente.

Taak	Organisatie	TPM
Adresonderzoek door Burgerzaken	Binnen de gemeente	Niet van toepassing

Gebruik van Suwinet voor Gemeentelijke Regelingen*

Voor de volgende gemeentelijke regelingen wordt Suwinet op de volgende plaatsen gebruikt:

Taak	Organisatie	TPM
Wet Maatschappelijke Ondersteuning, te weten de Regeling Tegemoetkoming Meerkosten	Binnen de gemeente	Niet van toepassing
Gemeentewet, art. 108, te weten de Stadspas en gratis OV voor ouderen	Binnen de gemeente	Niet van toepassing
Tegemoetkoming aanvullend openbaar vervoer, OV voor mantelzorgers	Binnen de gemeente	Niet van toepassing

*Het gebruik van deze inkijkfunctie van Suwinet is geen onderdeel van de Participatiewet of valt niet strikt binnen de kaders van de Participatiewet; daardoor ontbreekt de wettelijke grondslag

Gemeente Amsterdam

Naleving BIO-maatregelen

Met uitzondering van de volgende maatregelen voldoen de interne beheersingsmaatregelen voor de SUWI-taken op 31 december 2024 in opzet en bestaan aan de doelstellingen uit de verantwoordingsrichtlijn GeVS 2022:

Organisatie	SUWI-taak	BIO-maatregel	Applicatie
Binnen de gemeente	Taken vallend onder de Participatiewet (Pw), Inkomensvoorziening voor Oudere en gedeeltelijk Arbeidsongeschikte Werknemers (IOAW), Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen (IOAZ)	7.2.2.1 Alle medewerkers hebben de verantwoordelijkheid bedrijfsinformatie te beschermen. Iedereen kent de regels en verplichtingen met betrekking tot informatiebeveiliging en daar waar relevant de speciale eisen voor gerubriceerde omgevingen. 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. 7.2.2.3 Het management benadrukt bij aanstelling en interne overplaatsing en bijvoorbeeld in werkoverleggen of in personeelsgesprekken bij zijn medewerkers en contractanten het belang van opleiding en training op het gebied van informatiebeveiliging en stimuleert hen actief deze periodiek te volgen.	Suwinet-Inkijk
Binnen de gemeente		6.1.2.1 Er zijn maatregelen getroffen die onbedoelde of ongeautoriseerde toegang tot bedrijfsmiddelen waarnemen of voorkomen. 7.2.2.1 Alle medewerkers hebben de verantwoordelijkheid bedrijfsinformatie te beschermen. Iedereen kent de regels en verplichtingen met betrekking tot informatiebeveiliging en daar waar relevant de speciale eisen voor gerubriceerde omgevingen. 7.2.2.2 Alle medewerkers en contractanten die gebruikmaken van de	DKD-Inlezen

		informatiesystemen en -diensten hebben binnen drie maanden na indiensttreding een training I-bewustzijn succesvol gevolgd. 7.2.2.3 Het management benadrukt bij aanstelling en interne overplaatsing en bijvoorbeeld in werkoverleggen of in personeelsgesprekken bij zijn medewerkers en contractanten het belang van opleiding en training op het gebied van informatiebeveiliging en stimuleert hen actief deze periodiek te volgen. 9.2.1.1 Er is een sluitende formele registratie- en afmeldprocedure voor het beheren van gebruikersidentificaties. 9.2.1.2 Het gebruiken van groepsaccounts is niet toegestaan, tenzij dit wordt gemotiveerd en vastgelegd door de proceseigenaar. 9.2.2.1 Er is uitsluitend toegang verleend tot informatiesystemen na autorisatie door een bevoegde functionaris. 9.2.2.3 Er is een actueel mandaatregister of er zijn functieprofielen waaruit blijkt welke personen bevoegdheden hebben voor het verlenen van toegangsrechten. 9.2.5.2 De opvolging van bevindingen is gedocumenteerd en wordt behandeld als beveiligingsincident. 9.2.5.3 Alle uitgegeven toegangsrechten worden minimaal eenmaal per halfjaar beoordeeld. 9.2.6 Toegangsrechten intrekken of aanpassen. 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 10.1.1.1 In het cryptografiebeleid zijn minimaal de volgende onderwerpen uitgewerkt: a) Wanneer cryptografie ingezet wordt. b) Wie verantwoordelijk is voor de implementatie. c) Wie verantwoordelijk is voor het sleutelbeheer. d) Welke normen als basis dienen voor cryptografie en de wijze waarop de normen van het Forum worden toegepast. e) De wijze waarop het beschermingsniveau vastgesteld wordt. f) Bij communicatie tussen organisaties wordt het beleid onderling vastgesteld. 10.1.1.2 Cryptografische toepassingen voldoen aan passende standaarden. 12.1.1 Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben. 12.4.1.1 Een logregel bevat minimaal: a) de gebeurtenis; b) de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon; c) het gebruikte apparaat; d) het resultaat van de handeling; e) een datum en tijdstip van de gebeurtenis. 12.4.1.2 Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden. 12.4.1.3 De informatieverwerkende omgeving wordt gemonitord door een SIEM en/ of SOC middels detectie-voorzieningen, zoals het Nationaal	

		Detectie Netwerk (alleen voor rijksoverheidsorganisaties). Deze worden ingezet op basis van een risicoinschatting, mede aan de hand van de aard van de te beschermen gegevensen informatiesystemen, zodat aanvallen kunnen worden gedetecteerd. 12.4.1.4 Bij ontdekte nieuwe dreigingen (aanvallen) via 12.4.1.3 worden deze binnen geldende juridische kaders verplicht gedeeld binnen de overheid, waaronder met het NCSC (alleen voor rijksoverheidsorganisaties) of via de sectorale CERT (voor andere overheidsorganisaties), middels (bij voorkeur geautomatiseerde) threat intelligence sharing mechanismen. 12.4.1.5 De SIEM en/of SOC hebben heldere regels over wanneer een incident moet worden gerapporteerd aan het verantwoordelijk management. 12.4.2.1 Er is een overzicht van logbestanden die worden gegenereerd. 12.4.2.2 Ten behoeve van de loganalyse is op basis van een expliciete risicoafweging de bewaarperiode van de logging bepaald. Binnen deze periode is de beschikbaarheid van de loginformatie gewaarborgd. 12.4.2.3 Er is een (onafhankelijke) interne audit procedure die minimaal half jaarlijks toetst op het ongewijzigd bestaan van logbestanden. 12.4.2.4 Oneigenlijk wijzigen of verwijderen van loggegevens of pogingen daartoe worden zo snel mogelijk gemeld als beveiligingsincident via de procedure voor informatiebeveiligingsincidenten conform BIO hoofdstuk 16.	

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	Applicatie
Binnen de gemeente	Hulp aan vroegtijdig schoolverlaters door Regionaal Meld- en Coördinatiecentrum (RMC)	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. 7.2.2.1 Alle medewerkers hebben de verantwoordelijkheid bedrijfsinformatie te beschermen. Iedereen kent de regels en verplichtingen met betrekking tot informatiebeveiliging en daar waar relevant de speciale eisen voor gerubriceerde omgevingen. 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. 7.2.2.3 Het management benadrukt bij aanstelling en interne overplaatsing en bijvoorbeeld in werkoverleggen of in personeelsgesprekken bij zijn medewerkers en contractanten het belang van opleiding en training op het gebied van informatiebeveiliging en stimuleert hen actief deze periodiek te volgen. 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.	Suwinet-Inkijk RMC
Binnen de gemeente	Adresonderzoek door Burgerzaken	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.	Suwinet-Inkijk adresonderzoek

Gemeente Amsterdam

Organisatie	Niet-SUWI-taak	BIO-maatregel	Applicatie
		7.2.2.1 Alle medewerkers hebben de verantwoordelijkheid bedrijfsinformatie te beschermen. Iedereen kent de regels en verplichtingen met betrekking tot informatiebeveiliging en daar waar relevant de speciale eisen voor gerubriceerde omgevingen. 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. 7.2.2.3 Het management benadrukt bij aanstelling en interne overplaatsing en bijvoorbeeld in werkoverleggen of in personeelsgesprekken bij zijn medewerkers en contractanten het belang van opleiding en training op het gebied van informatiebeveiliging en stimuleert hen actief deze periodiek te volgen. 9.2.6 Toegangsrechten intrekken of aanpassen. 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.	