Ref BIO 2021, BIO 1.04 Control
6. Organiseren informatiebeveil
6.1.2 Scheiding van taken
7. Veilig personeel tijdens diens
7.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging

9. Toegangsbeveiliging
9.2.6 Toegangsrechten intrekken of aanpassen
18. Naleving
18.1.4 Privacy en bescherming van persoonsgegevens

Verantwoordingsrichtlijn GeVS 2022

iging6. Organiseren informatiebeveiliging

Criterium BIO:
Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.

Doelstelling:
Ervoor zorgen dat de juiste taken en verantwoordelijkheden binnen de onderkende rollen juist worden uitgevoerd met inachtneming van de juiste functiescheiding voor zover de organisatiegrootte dit toelaat.

Risico:
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.

tverband

Criterium BIO:
Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.

Doelstelling:
Het bewustmaken van gebruikers van Suwinet gegevens

Risico:
Indien gebruikers van Suwinet gegevens zich niet of onvoldoende bewust zijn van de (hoge) vertrouwelijkheid, bestaat het risico dat deze gegevens onvoldoende worden beschermd.

Criterium BIO:
De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast. **Doelstelling:**
Het tijdig beëindigen of wijzigen van de toegangsrechten.

Risico: Als toegangsrechten niet bijtijds worden beëindigd of gewijzigd, bestaat het risico op onbevoegde kennisname van Suwinet gegevens.

Criterium BIO:
Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.

Doelstelling:
Voorkomen van schendingen van wettelijke, statutaire, regelgevende of contractuele verplichtingen betreffende het verwerken van persoonsgegevens.

Risico:
Als de verwerking van Suwinet (persoons)gegevens niet overeenkomstig toepasselijke wet- en regelgeving plaatsvindt, wordt hierdoor de AVG overtreden.

Specifieke overheidsmaatregelen BIO

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.

Deze control kent in de BIO geen maatregel.
NB: voor deze control is een aanvullende maatregel opgesteld in de ENSIA-vragenlijst: 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

18.1.4.1 In overeenstemming met de AVG heeft iedere organisatie een Functionaris Gegevensbescherming (FG) met voldoende mandaat om zijn/haar functie uit te voeren.

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.

conclusie auditor	Verbetermaatregel Suwi Doorstroompunt - Actiehouders en planning
Wij hebben een autorisatiematrix ontvangen. Hierin is niet aangegeven welke specifieke rollen conflicterend zijn. Er is 1 medewerker die per abuis de rol Gebruikersbeheerder en RMC medewerker heeft gehad in 2024 in tegenstelling tot de autorisatiematrix aangeeft.	Suwi-Doorstroompunt: Zodra de vacature van de kwartiermaker Doorstroompunt zal dde kwartiermaker een verbeterde autorisatiematrix opstellen en dit aanleveren. Planning: mei/juni 2025
We hebben vastgesteld dat er binnen de organisatie stedelijke beleidsregels en procedures aanwezig zijn. Wij hebben echter niet kunnen vaststellen dat alle medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten binnen drie maanden na indiensttreding een training I-bewustzijn succesvol hebben gevolgd.	De managers van de medewerkers die nog geen I-bewustzijn training hebben gevolgd of dat nog niet hebben aangetoond zijn aangeschreven met het verzoek dit eind januari 2025 geregeld te hebben. De nieuwe kwartiermaker Doorstroompunt zal hier achteraan gaan en een nieuw overzicht aanleveren van wie de training hebben gevolgd. Planning: me/juni 2025

Zie norm 9.2.1 en 9.2.2. en norm 9.2.5. Wij hebben niet kunnen vaststellen dat bij wijzigingen van autorisatie de aanvraag wordt vastgelegd.	
Wij hebben op basis van de verwerkingsoverzichten en rollen en verantwoordelijkheden vastgesteld dat: - In overeenstemming met de AVG heeft de gemeente Amsterdam een Functionaris Gegevensbescherming (FG) heeft met voldoende mandaat om zijn/haar functie uit te voeren. - Het proces RMC zijn verwerkingen van SUWI gegevens niet herleidbaar heeft opgenomen in een verwerkingen register en daarmee 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 niet heeft gewaarborgd	De nieuwe kwartiermaker Doorstroompunt zal ervoor zorgen dat de gegevens in een verwerkingsregister komen en dit terugkoppelen aan de ACAM. Planning: mei/juni 2025.

Verbetermaatregel Suwi-Inkijk - Actiehouders en planning
Wij zullen er extra op gaan inzetten dat alle gebruikers van Suwinet binnen 3 maanden na indiensttreding de elearning hebben gevolgd. Ook zullen wij eraan werken dat dit aantoonbaar is. Daarnaast zullen wij extra inzetten op het trainen van leidinggevenden. Om dit te realiseren ontbreekt bovendien nog een rol in de organisatie, namelijk de rol van proceseigenaar. De directeur Inkomen verbindt zich aan de afspraak om een proceseigenaar aan te wijzen.

Suwinet-Inkijk, specifiek voor adresonderzoek: autorisatiematrix bijhouden