

Bijlage 1 Autorisaties Suwinet

In de onderstaande tabel is aangegeven welke rol tot welke Suwinet-pagina's geautoriseerd is. Dit is conform de Handreiking autorisatie Suwinet-Inkijk van het BKWI.

Rol Suwinet	Rol organisatie	Pagina's Suwinet
GSD GR WerkSaam Westfriesland	▪ Inkomensconsulent ▪ Ontwikkelcoach ▪ Arbeidscoach ▪ Medewerker Uitkeringsadministratie ▪ Kwaliteitsmedewerker	▪ Belastingdienst ▪ Bijstandsregelingen ▪ DUO gegevens ▪ Fraude scorekaart ▪ GBA volledig ▪ Inkomstenverhoudingen ▪ Kadaster ▪ Kostendelerstoets ▪ RDW peildata ▪ Rechtmatigheid+ ▪ SVB gegevens ▪ UWV uitkeringen ▪ SBR Query ▪ UWVWb
Terugvordering & Verhaal	▪ Medewerker terugvordering en verhaal	• Bedrijvenregister • Belastingdienst • Bijstandsregelingen • GBA • GBA volledig • GSD • Fraude-vorderingen • Kadaster • Klant algemeen • Terugvordering en Verhaal
Handhaving	▪ Sociaal rechercheur ▪ Handhaver	▪ Bedrijvenregister ▪ Belastingdienst ▪ Bijstandsregelingen ▪ DUO gegevens ▪ Fraude scorekaart ▪ GBA ▪ GBA volledig ▪ GSD ▪ Handhaving ▪ Inkomstenverhoudingen ▪ Kadaster ▪ Kostendelerstoets ▪ RDW peildata ▪ RDW+ ▪ SVB gegevens ▪ UWV uitkeringen ▪ SBR Query ▪ UWVWb
Functioneel beheerder	▪ Functioneel beheerder	Nvt
Security Officer	▪ Security Officer	▪ Opvragen generieke gebruikersrapportage ▪ Opvragen specifieke gebruikersrapportage

Bijlage 2 Zorgvuldigheidsverklaring

Ondergetekende:

Naam:

Organisatie:

Functie:

Datum:

BELOOFT/VERKLAART:

- op de hoogte te zijn van de inhoud van het algemene informatiebeveiligingsbeleid van de organisatie en het informatiebeveiligingsbeleid Suwinet.
- zich te houden aan het algemene informatiebeveiligingsbeleid van de organisatie en het informatiebeveiligingsbeleid Suwinet.
- zorgvuldig om te gaan met de (persoons)gegevens en de inhoud van de documenten die bij de uitvoering van de werkzaamheden in Suwinet-verband zijn ingezien.
- zich te houden aan de volgende instructies:
 - niet meer of vaker (persoons)gegevens raadplegen dan strikt noodzakelijk is;
 - (persoons)gegevens niet aan onbevoegden te verstrekken;
 - alleen die gegevens raadplegen welke je nodig hebt voor de directe uitoefening van je taken;
 - Bij het (tijdelijk) verlaten van de werkplek de computer vergrendelen of afsluiten.
- het Suwinet-account en wachtwoord zorgvuldig en strikt persoonlijk te gebruiken en niet aan anderen ter beschikking te stellen.
- bekend te zijn dat alle handelingen en verrichtingen in Suwinet-Inkijk worden geregistreerd en vastgelegd. Deze gegevens kunnen steekproefsgewijs worden gecontroleerd.
- gedurende de duur en na beëindiging van de werkzaamheden in Suwinet-verband, alle (persoons)gegevens geheim te houden.
- bekend te zijn dat bij het vermoeden van onrechtmatig gebruik of misbruik van Suwinet-gegevens een onderzoek wordt gestart. Bij vaststelling van onrechtmatig handelen of van misbruik worden passende maatregelen getroffen. Dit kan zelfs leiden tot ontslag.

Handtekening medewerker:

.....

Bijlage 3 Autorisatieprocedure Suwinet

Deze procedure maakt deel uit van het Informatiebeveiligingsbeleid Suwinet. Deze procedure beschrijft de stappen die noodzakelijk zijn voor het autoriseren van personen tot Suwinet. Hiermee wordt de logische toegangsbeveiliging en de vertrouwelijkheid.

De procedure bestaat uit afzonderlijke deelprocedures die gescheiden kunnen worden uitgevoerd:

- Autorisatie tot Suwinet-Inkijk.
- Functiewijziging of einde dienstverband/opdracht.
- Controle op autorisaties en raadplegen.

Uitgangspunten:

- Toegang is verleend op basis van de uit te voeren functie / rol.
- Het uniek identificeren van elke gebruiker tot één persoon.
- De aanvraag voor toegangsrechten is gedaan door de leidinggevende of HRM (voor een nieuwe medewerker).
- Bij functiewijziging of vertrek is de autorisatie direct aangepast.
- Suwinet-account en wachtwoord zijn herleidbaar naar één persoon en worden niet aan anderen/meerdere ter beschikking gesteld.
- De manager is eindverantwoordelijk voor het gebruik en de beveiliging van Suwinet Inkijk.
- Functioneel beheerders Suwinet hebben een Suwinet beheeraccount.

Autorisatieprocedure:

1. De leidinggevende dient via TopDesk een verzoek in voor een medewerker (vast, tijdelijk of inhuur) voor een autorisatie in Suwinet. De taakhoud/functie van de medewerker is hierin verwoord.
2. De functioneel beheerder Suwinet stelt vast of de medewerker in het personeelsbestand voorkomt en of de gevraagde rol passend is bij de functie.
3. De functioneel beheerder zorgt voor ondertekening van de zorgvuldigheidsverklaring door de medewerker. Een afschrift van deze verklaring wordt vastgelegd in het personeelsdossier.
4. De functioneel beheerder Suwinet informeert de medewerker over het gebruik van Suwinet en over de onderwerpen genoemd in het informatiebeveiligingsbeleid Suwinet.
5. De functioneel beheerder archiveert het autorisatieverzoek in TopDesk.
6. Als de functioneel beheerder een melding krijgt via TopDesk over een vergeten wachtwoord of geblokkeerde account, deblokkeert de functioneel beheerder het account en verstuurt de medewerker via TopDesk een mail hierover. De functioneel beheerder stuurt via outlook een aparte mail met het nieuwe wachtwoord.

Functiewijziging of einde dienstverband/opdracht

1. De leidinggevende is verantwoordelijk voor het doorgeven van een functiewijziging of einde dienstverband/opdracht aan de servicedesk via een melding in TopDesk en/of de HR-adviseurs.
2. De functioneel beheerder Suwinet beëindigt de autorisatie per de opgegeven einddatum.
3. De servicedesk archiveert de melding tot beëindigen autorisatie.

Controle op autorisaties

1. Minimaal 1x per jaar controleert de Security Officer zichtbaar of:
 - Degenen die toegang hebben tot Suwinet werkzaam zijn (vast, tijdelijk of extern) binnen de organisatie.
 - Degenen die toegang hebben tot Suwinet een rol hebben die past bij de functie.
 - Suwinet gebruikt wordt door gebruikers die gedurende een lange periode niet zijn ingelogd, terwijl dit wel verwacht mag worden gezien de functie van de gebruiker. Er wordt dan nagegaan waarom niet is ingelogd. Dit kan duiden op gebruik van een ander zijn autorisatie.
2. De Security Officer rapporteert eventuele bevindingen aan de manager. Misbruik of oneigenlijk gebruik van Suwinet wordt direct gerapporteerd aan het hogste management.
3. De controle, bevindingen en rapportage wordt digitaal gearchiveerd.