Bijlage 6b PvE PPS

Addendum 3RO Informatiebeveiligingsbeleid

(ten behoeve van de aanbesteding voor het nieuwe PPS)

Datum: 27-09-2023
Auteur: Fred van Tol (RN), Sander Spit (LJ&R), Eric Balfour van Burleigh (SVG)
Goedgekeurd stuurgroep PPS :

Addendum 3RO informatiebeveiligingsbeleid

Ten behoeve van het opstellen van security requirements voor het nieuwe PPS is september 2023 een vergelijking gemaakt tussen het informatiebeveiligingsbeleid van de afzonderlijke reclasseringsorganisaties. De verschillen zijn in kaart gebracht en gestroomlijnd. In onderstaande opsomming staan de beleidsmatige aanpassingen die overeengekomen zijn en een addendum vormen op het IB-beleid van de individuele reclasseringsorganisatie. De scope waarop de maatregelen betrekking hebben betreft het (nieuwe) PPS.

Beleidsmatige afspraken:

- De cliëntgegevens in het PPS worden beschouwd als strafrechtelijke persoonsgegevens en vallen onder de van toepassing zijnde wetgeving daarvoor (niet onder de kaders die gelden voor patiëntgegevens);
- Inloggen met MFA/2FA is vereist;
- Voor beveiliging van internetverbindingen is minimaal TLS 1.3 vereist of de geldende markt standaard indien deze hoger ligt;
- Autorisaties zijn gebaseerd op de behandelrelatie en de rol (RBAC). Voor noodsituaties bestaat een maatregel om af te kunnen wijken (inclusief logging en validatie);
- Het plaatsen van cliëntgegevens in de public cloud is toegestaan, mits wordt voldaan aan de voorwaarden uit het Rijkscloudbeleid en werkbaar is voor alle aangesloten organisaties te weten Reclassering Nederland, SVG Reclassering en Leger des Heils Jeugdbescherming en Reclassering.