

Beveiligingsaspecten SCOL, ESIS en BurgerschapMeten

1. Rovict is gehouden aan de FENIT-voorwaarden; dit is overeengekomen in de Hostingovereenkomst met de klant.
2. Alleen de school registreert gegevens en heeft met Rovict een overeenkomst gesloten voor het beheren van de data. Rovict registreert geen gegevens.
3. In de handleiding van SCOL, ESIS en BurgerschapMeten (BSM) is uitgebreid beschreven op welke wijze het invoeren, opslaan en bewaren van gegevens is geregeld:
 - a. alleen leerlinggegevens die relevant zijn voor het doel van SCOL, ESIS en BSM worden geregistreerd.
 - b. de toegang tot de SCOL-, ESIS- en BSM-website is door middel van een autorisatieproces (gebruikersnaam, wachtwoord) geregeld.
 - c. de toegang is alleen via beveiligde verbindingen te benaderen door de klant.
 - d. de database is *alleen* via de website (vanaf de beheerde webserver) te benaderen en *niet* rechtstreeks.
4. De database wordt door Rovict beheerd. Dit betekent onvermijdelijk dat een beperkte groep van medewerkers van Rovict, met naam en autorisaties vastgesteld, toegang heeft tot de gegevens om bij storingen een reparatie te kunnen uitvoeren. Binnen de organisatie van Rovict is dit aan strikte regels gekoppeld. In het personeelsreglement van Rovict zijn clausules opgenomen die er voor zorg dragen dat (een medewerker van) Rovict niets mag doen met persoonlijke gegevens van klanten.
5. Binnen de werkprocessen van Rovict is continu aandacht voor de beveiliging van de klantgegevens. Mocht daar aanleiding toe zijn, dan worden verbeteringen aangebracht in de organisatorische aspecten, de functionaliteit van SCOL, ESIS en BSM of in de technische infrastructuur.
6. De database staat in een datacentrum. De infrastructuur van dit datacentrum voldoet aan de vereiste gecertificeerde beveiligingsvoorwaarden. Het gebouw van het datacentrum beschikt over een klasse B2 beveiliging m.b.t. hang- en sluitwerk (fysieke toegang). Voor wat betreft de elektronische beveiliging (toegang) beschikt de locatie over beveiligingsklasse 4. Ongeautoriseerde toegang van de gegevens is daarmee zo goed als onmogelijk.
7. Als een contract beëindigd wordt, dan is per direct de toegang tot de website en tot de gegevens geblokkeerd. De gegevens zelf worden na een termijn van 3 maanden definitief verwijderd (lees: vernietigd).