Informatiebeveiliging – Security-criteria bij ICT-diensten – DIENSTVERLENER ~~COMPACT~~

Security-eisen ten behoeve van informatieveiligheid

Applicatie/ Systeem Beveiliging GOO-locatie(s)

Information Security Management
Gemeente Apeldoorn

[versie 7 januari 2025]

Gewijzigd 15 september 2025, n.a.v. Nvl

1. Alle software (front-end en back-end) behorend tot de (cloud)dienst is volgens relevante standaarden beveiligd, conformeert zich telkens aan de laatst bekende beveiligingsinzichten en is blijvend van voldoende kwaliteit. Richtlijnen van de Autoriteit Persoonsgegevens (AP), Nationaal Cyber Security Centrum (NCSC), Informatiebeveiligingsdienst voor gemeenten (IBD), Forum Standaardisatie en Open Web Application Security Project (OWASP) zijn hierbij normstellend. Systeemprogrammatuur (zijnde non-applicatie programmatuur) dient altijd te kunnen voldoen aan het juiste beveiligingsniveau (patchlevel) aanbevolen door de softwarefabrikant. Alle betrokken softwarecomponenten worden frequent gescand op kwetsbaarheden en gepatcht volgens marktconforme 'best practices'.

2. Opdrachtnemer beveiligt alle gegevens die tot de (cloud)dienst behoren (ook die van niet-productieomgevingen) van Opdrachtgever op adequate wijze, zodanig dat bescherming wordt geboden tegen gegevensverlies als wel toegang tot gegevens door onbevoegden. Met "alle gegevens" wordt bedoeld zowel "data in use", "data in motion" als "data at rest" binnen de ICT Prestatie ~~Oplossing~~. De (cloud)dienst wordt te allen tijde benaderd op basis van een versleutelde verbinding. Bij transport van vertrouwelijke informatie over onvertrouwde netwerken, zoals het internet, wordt te allen tijde gebruikt gemaakt van versleutelde verbindingen en 2-factor authenticatie conform de laatste stand der techniek.

3. De ICT Prestatie ~~Oplossing~~ biedt functionaliteit waarmee Opdrachtgever kan garanderen dat een gebruiker slechts toegang heeft tot de gegevens die voor de uitoefening van zijn/haar functie nodig zijn (least privileged). Wachtwoorden worden bij invoer niet op het scherm getoond en worden versleuteld (gehasht) opgeslagen binnen de ICT Prestatie ~~Oplossing~~ waarbij de versleutelde waarde niet zichtbaar kan worden gemaakt via beheerinterfaces of reverse engineering. Er wordt geen gebruik gemaakt van voorgedefinieerde dan wel hardgecodeerde wachtwoorden. Accounts zonder wachtwoordbeveiliging zijn niet toegestaan.

4. De ICT Prestatie ~~Oplossing~~ biedt de mogelijkheid dat een gebruiker zélf zijn wachtwoord kan wijzigen. Qua constructie-eisen geldt in de basis:
   - Minimaal 12 tekens lang;
   - Bevat tekens uit tenminste 3 van de 4 categorieën:
     - Kleine letters;
     - Eén hoofdletter;
     - Eén leesteken;
     - Eén cijfer;

   Voor beheer- en systeem/service-accounts geldt een minimale lengte van 15 tekens en maximale complexiteit.

5. Activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen worden vastgelegd in audit-logbestanden waarin tenminste wordt opgenomen: de gebeurtenis; de benodigde informatie die nodig is om een beveiligings-incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon; het gebruikte apparaat; het resultaat van de handeling; een datum en tijdstip van de gebeurtenis. Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden.

6. Opdrachtnemer accepteert de maatregelen uit de Baseline Informatiebeveiliging Overheid (BIO) en past de maatregelen die relevant zijn voor Opdrachtgever met betrekking tot onderhavige ICT Prestatie ~~Oplossing~~ toe op de geleverde producten en/of diensten. De ICT Prestatie ~~Oplossing~~ en daarmee samenhangende diensten van Opdrachtnemer stellen Opdrachtgever in staat om te voldoen aan de Baseline Informatiebeveiliging Overheid (oftewel Opdrachtnemer staat Opdrachtgever niet in de weg bij het voldoen aan de BIO). Opdrachtgever heeft het recht om

jaarlijks de beveiligingseisen die van toepassing zijn op de ICT Prestatie ~~Oplossing~~ door een onafhankelijke partij te laten auditen.

~~7. Versie 1.2. Alle data van de oplossing kunnen ontsloten worden via een door de gemeente Apeldoorn geselecteerde BI- of ETL-tool, die lokaal bij de gemeente Apeldoorn draait of extern als SaaS-oplossing wordt gehost.~~

~~De ontsloten data moet geautomatiseerd zonder menselijke tussenkomst (tbv batchverwerking) te benaderen zijn, op veilige wijze, naar de laatste stand der techniek.~~

~~Hierbij kan gedacht worden aan bijv:~~

- ~~Directe connectie met de database of een kopie van deze database (maximaal 24 uur oud) indien er binnen de applicatie een mogelijkheid is wel live data middels een rapport generator te bevragen.~~
- ~~Een kopie van de database in Oracle of MS-SQL formaat die middels SFTP beschikbaar wordt gesteld om te downloaden.~~
- ~~Een dump van alle database tabellen in CSV, JSON of XML formaat om te downloaden.~~
- ~~Geautomatiseerde onbeperkte uitvraag via een api/rest/odata interface. In dit geval moet het mogelijk zijn om grote hoeveelheden te bevragen.~~

~~De volgende voorwaarden zijn van toepassing op deze gegevensuitwisseling;~~

- ~~De oplossing moet in staat zijn om alleen de nieuwe en/of gewijzigde records in bulk aan te leveren. De aangeleverde gegevens moeten per record een unieke sleutel bevatten om gegevensconsistentie te waarborgen.~~
- ~~De ontsloten data dienen een realtime actualiteit te hebben of maximaal 24 uur oud te zijn.~~
- ~~De data dient via een pull functionaliteit (dus Gemeente Apeldoorn haalt op) beschikbaar te zijn.~~

~~Aan de gemeente Apeldoorn dient een volledige beschrijving van de data geleverd te worden. Deze dient aan de volgende voorwaarden te voldoen;~~

- ~~Een beschrijving met definities van alle objecttypen, gegevenstypen en relatietypen, overeenkomend met de structuur waarin de data beschikbaar wordt gesteld in een door mensen leesbaar formaat.~~
- ~~Volledige informatie over de kardinaliteit en objecttypen, gegevenstypen en relatietypen.~~

~~Bij eventuele updates dient er een nieuwe beschrijving geleverd te worden waarin de wijzigingen staan benoemd.~~