Informatiebeveiliging – Security-criteria bij ICT-diensten – DIENSTVERLENER

Security-eisen ten behoeve van informatieveiligheid

All-in beheer hoofdgemalen en randvoorzieningen

PLC software

Information Security Management
Gemeente Apeldoorn

[versie 7 januari 2025]

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 garandeert te allen tijde expliciet compliance van onderaannemers, hostingpartijen en gelieerde partners aan de overeengekomen afspraken met Opdrachtgever en is daarbij zelf volledig verantwoordelijk.

3. Indien een securitypatch beschikbaar is voor een applicatie/software dan wel voor onderliggende componenten zoals systeemprogrammatuur en middleware dient deze zo spoedig mogelijk te kunnen worden geïnstalleerd. Componenten mogen hierbij onderling geen verhinderende factor vormen.

4. 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. 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.

5. De ICT Prestatie 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 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.

6. Wachtwoordconstructie-eisen zijn 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.

7. 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.

8. 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 toe op de geleverde producten en/of diensten. De ICT Prestatie 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 door een onafhankelijke partij te laten auditen.

9. Kaders
    a. Toegang wordt alleen verleend op basis van persoonlijke (dus herleidbare) accounts.
    b. Toegangsrechten zijn zoveel mogelijk ingericht conform “need-to-know” en “least privilege” principes.
    c. Het gebruik van (verhoogde) bevoegdheden wordt toegekend op basis van PIM (toegang geven, wanneer het nodig is en intrekken wanneer de werkzaamheden zijn verricht).

10. Spelregels
    a. Leverancier voert geen werkzaamheden uit zonder voorafgaande afstemming.
    b. Zorg voor vastlegging van uitgevoerde werkzaamheden. Maak afspraken over hoe en met welke frequentie dat met ons wordt gedeeld.
    c. Gebruik je gezonde verstand, in het bijzonder als het om een *prod-only-omgeving* gaat.
    d. Voorkom een configuratie die andere uitrol of doorontwikkeling in de weg staat.
    e. Zorg voor adequate naamgeving, conform vigerende standaarden en stem af waar nodig.
    f. Werk waar mogelijk volgens het OTAP-principe.
    g. Stem maatregelen en/of inrichting die informatiebeveiliging raken af met Security Management (en uiteraard IT-specialisten). Leg grotere vraagstukken altijd voor.