

Informatiebeveiliging – MINIMALE Security-criteria bij ICT-diensten

Minimale set van security-criteria ten behoeve van Klein Onderhoud Rioleringen (software ondersteuning)

Information Security Management
Gemeente Apeldoorn

[versie 6 juni 2024]

1. Alle software (front-end en back-end) behorend tot Oplossing 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.
2. Opdrachtnemer beveiligt alle gegevens die tot Oplossing 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 Oplossing.
3. Oplossing 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.
4. Indien Opdrachtnemer niet kan aansluiten op de authenticatiedienst van Opdrachtgever (Entra ID), biedt Opdrachtnemer zelf een sterke, in de markt gangbare, methode voor 2-factor authenticatie waarbij de 2^{de} factor wordt gebaseerd op iets dat de gebruiker heeft en bij voorkeur in de vorm van een authenticator-app.
5. Oplossing biedt de mogelijkheid dat een gebruiker zelf zijn wachtwoord kan wijzigen waarbij eisen aan constructie, geldigheidsduur en toepassing zijn gebaseerd op het vigerende wachtwoordbeleid van Opdrachtgever. 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;
 - Minimaal een dag geldig;
 - Maximaal een half jaar geldig;
 - Niet herhalend of opeenvolgend.Voor beheer- en systeem/service-accounts geldt een minimale lengte van 15 tekens en maximale complexiteit.
6. Wachtwoorden worden bij invoer niet op het scherm getoond en worden versleuteld (gehasht) opgeslagen binnen 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 in het algemeen en in het bijzonder bij standaard accounts. Accounts zonder wachtwoordbeveiliging zijn niet toegestaan.
7. 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 (need to know / least privilege).
8. 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.
9. Als Oplossing kan worden benaderd door een browser geldt dat Oplossing op basis van een gangbare en ondersteunde browser (als Chrome, Edge, Firefox en Safari), juist, volledig en optimaal kan worden gebruikt, onafhankelijk van de onderliggende hardware en zonder toevoeging van extra plug-ins of add-ons.
10. Opdrachtnemer past de maatregelen uit de Baseline Informatiebeveiliging Overheid (BIO), die relevant zijn voor Opdrachtgever met betrekking tot de Oplossing, toe op de geleverde producten

en/of diensten. Oplossing en daarmee samenhangende diensten van Opdrachtnemer stellen Opdrachtgever in staat om te voldoen aan de Baseline Informatiebeveiliging Overheid (BIO).

11. Opdrachtgever heeft het recht om de beveiligingseisen die van toepassing zijn op Oplossing door een onafhankelijke partij te laten auditen. Opdrachtnemer stelt Opdrachtgever in staat om periodiek toe te zien of de dienstaanbieder zijn verplichting tot adequate beveiliging nakomt.
12. Alle betrokken softwarecomponenten worden frequent gescand op kwetsbaarheden en gepatcht volgens marktconforme 'best practices' en zijn ontworpen en getest op het voorkomen van inbreuken op beschikbaarheid, integriteit en vertrouwelijkheid.
13. Opdrachtnemer heeft een back-up en recovery beleid dat voldoet aan de eisen uit de BIO en waarbij minimaal de volgende eisen van toepassing zijn op de back-up en restorevoorzieningen van Oplossing:
 - De 3-2-1 regel wordt toegepast.
 - Een incident op de ene locatie kan niet leiden tot schade op de andere locatie (ook niet in het geval van ransomware).
 - Bedrijfskritische systemen worden bij calamiteiten binnen 1 week hersteld.
 - Gegevensverlies bedraagt maximaal 28 uur.
 - Hersteltijd in geval van incidenten is maximaal 16 werkuren (twee dagen van 8 uur) in 85% van de gevallen.
 - Het herstellen van back-ups wordt minimaal jaarlijks of na een grote wijziging getest waarbij recovery-procedures voortdurend worden bijgewerkt.
 - Er is sprake van een reconstructiemechanisme als geen data verloren mag gaan.
 - Back-ups worden beschermd tegen onbevoegde toegang.
 - In het geval van ketensoftware is data-integriteit van de keten gewaarborgd.
 - Opdrachtnemer zorgt voor adequate afspraken over back-up en recovery en voldoet aantoonbaar aan relevante punten uit het beleid.
 - In het geval van noodscenario's is toegang tot Oplossing geborgd door de inzet van zogenaamde "break glass accounts".
14. Indien (een deel van) Oplossing zich bij Opdrachtgever on-premises bevindt, dient Opdrachtnemer zich te conformeren aan on-premises inrichtingseisen van Opdrachtgever waarbij Oplossing geschikt is om samen te werken met on-premises technieken zoals hieronder beschreven:
 - a. Internetfacing systemen worden ontsloten via een firewall waarbij segmentatie / zonering (DMZ) wordt toegepast om vertrouwde en onvertrouwde verkeersstromen zoveel mogelijk te scheiden en te beperken tot het hoogstnoodzakelijke.
 - b. Alle netwerkverkeer (ingress, egress, lokaal) dient door Opdrachtgever te kunnen worden geïnspecteerd. Versleuteld verkeer dient daartoe via een SSL-Offloader te kunnen worden ontsleuteld ten behoeve van inspectie door het IPS.
 - c. Opdrachtnemer garandeert dat Oplossing in zijn totaliteit succesvol kan worden gecombineerd met standaard technieken van SSL-Offloaders, Reverse Proxy's, Poort Filtering, Reputation Filtering en Web Application Firewalls die Opdrachtgever in huis heeft.
15. Indien koppeling met internetfacing systemen van Opdrachtgever noodzakelijk is, geldt dat interne systemen van Opdrachtgever gegevens met Opdrachtnemer, ketenpartners en / of klanten uitwisselen via een centrale interne zone (DMZ) en een vertrouwde externe zone. Voor de uitwisseling van gegevens met derden (niet openbare gegevens) worden besloten externe zones (vertrouwde derden) gebruikt. In een DMZ worden alleen openbare gegevens van een organisatie opgeslagen die in het uiterste geval verloren mogen gaan.
16. Emailverkeer dat namens Opdrachtgever (@apeldoorn.nl) plaatsvindt (intern dan wel extern) voldoet blijvend aan aanvullende beveiligingsmaatregelen als DNSSEC, SPF, DKIM, DMARC, STARTTLS en DANE. Opdrachtnemer definieert en valideert de SPF-, DKIM- en DMARC-records van het domein van Opdrachtgever conform de actuele configuratie van Opdrachtgever. Opdrachtnemer zorgt ervoor dat de partijen, die emailberichten ontvangen van Opdrachtgever, kunnen valideren dat deze emailberichten inderdaad van Opdrachtgever afkomstig zijn. Opdrachtnemer deelt daartoe tenminste de publieke sleutel van het DKIM sleutelpaar én de "selector" in de vorm van een TXT-record (voorkeur) of CNAME-record met Opdrachtgever zodat Opdrachtgever deze aan haar DNS-dienst kan koppelen.