Informatiebeveiliging – Security-criteria bij ICT-diensten

Set van security-eisen ten behoeve van informatieveiligheid

Marktconsultatie Rittenregistratie

Information Security Management
Gemeente Apeldoorn

[versie 1 december 2025]

Security-eisen:

	Relatie met normering:	Site: C=cloud P=onprem

1. Algemeen

1.1 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.

2. Applicatie

2.1 Mobiele applicaties (apps) dienen via de officiële Appstores (Apple, Google, Microsoft) dan wel via de interne Enterprise App store te kunnen worden geïnstalleerd. Distributie en beheer van apps is mogelijk via gangbare voorzieningen op basis van Unified Endpoint Management.

2.2 Applicatieprogrammatuur dient *backward* en *forward compatible* te zijn met alle door de fabrikant ondersteunde versies van het onderliggende besturingssysteem en met andere vereiste systeemprogrammatuur. [P]

2.3 Als de ICT Prestatie wordt geleverd als een *virtual* of *software appliance* en als zodanig één geheel vormt met het onderliggende besturingssysteem en andere componenten is Opdrachtnemer verantwoordelijk voor het up-to-date houden van de gehele de ICT Prestatie. [P]

2.4 Indien er sprake is van interne dan wel externe koppelingen tussen verschillende applicatiediensten (denk aan berichtenverkeer of gegevensoverdracht) wordt uit principe de gemeentelijke integratievoorziening ingezet, zéker als het uitwisseling van privacygevoelige of vertrouwelijke gegevens betreft. Daarbij gaat het primair om de inzet van een API-gateway en een Enterprise Service Bus (ESB).

3. Auditing

3.1 Opdrachtgever heeft het recht om de beveiligingseisen die van toepassing zijn op de ICT Prestatie 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. Gecertificeerde security-specialisten van het SOC van Opdrachtgever voeren daartoe tenminste bij de initiële oplevering van de ICT Prestatie een security-check uit (altijd in afstemming met Opdrachtnemer). Een TPM is verplicht indien de ICT Prestatie onderdeel uitmaakt van de jaarrekeningcontrole / ENSIA-verantwoording.

3.2 Activiteiten van gebruikers (denk aan raadpleging en mutatie), beheerders (denk aan autorisatiewijzigingen), uitzonderingen en informatiebeveiligingsgebeurtenissen worden vastgelegd in audit-logbestanden die vanuit een applicatie-interface, en bij voorkeur via een standaard koppelvlak naar het SIEM-systeem van

Opdrachtgever, te allen tijde door Opdrachtgever kunnen worden geraadpleegd voor nadere analyse.

3.3 In audit-logbestanden wordt tenminste 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.

3.4 De beveiligingsorganisatie van Opdrachtnemer werkt volgens een algemeen geaccepteerd kwaliteitssysteem zoals ISO 27001. Daarbij heeft Opdrachtnemer technische en organisatorische maatregelen op een systematische manier doorgevoerd, zodanig dat deze door een onafhankelijke auditor kunnen worden beoordeeld.

4. Autorisatie

4.1 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 (need to know / least privilege).

5. Eigendom

5.1 Opdrachtgever behoudt te allen tijde het (intellectuele) eigendom van de gegevens die voor deze dienst worden ingevoerd. Opdrachtnemer behoudt geen rechten voor om de gegevens te gebruiken, te ontsluiten of publiek te maken. Opdrachtnemer verplicht zich om geen andere handelingen met de (persoons)gegevens te verrichten dan in het contract is omschreven.

6. Gegevensbescherming

6.1 Opdrachtnemer beveiligt alle gegevens die tot de ICT Prestatie 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.

6.2 Bij *multi-tenancy* zijn afdoende maatregelen getroffen om te voorkomen dat gegevens van Opdrachtgever bedoeld of onbedoeld worden gedeeld met derden, dan wel worden gecombineerd met gegevens van andere klanten door aggregatie of interferentie. De ICT Prestatie kan onafhankelijk van met andere klanten gedeelde infrastructuur en/of virtuele componenten worden ingericht en onderhouden.

6.3 De ICT Prestatie 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. Dit geldt ook indien er sprake is van toegang op afstand vanuit Opdrachtnemer, bijvoorbeeld voor ondersteunende werkzaamheden.

6.4 Indien (een deel van) de ICT Prestatie zich bij Opdrachtgever *on premises* bevindt, dient Opdrachtnemer zich te conformeren aan

inrichtingseisen van Opdrachtgever waarbij de ICT Prestatie geschikt is om samen te werken met *on premises* technieken zoals hieronder beschreven:

- 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.
- 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.
- Opdrachtnemer garandeert dat de ICT Prestatie 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.

7. Identificatie & authenticatie

7.1 De authenticatiedienst van Opdrachtnemer kan worden gekoppeld aan de authenticatiedienst van Opdrachtgever, gehost bij Opdrachtgever. De ICT Prestatie biedt een federatief koppelvlak voor uitwisseling van rollen en rechten. De verplichte standaard hiervoor is SAML 2.0. In de praktijk beperkt zich dat tot Microsoft Entra ID. Opdrachtgever stelt praktische inrichtingseisen bij implementatie.

Indien Opdrachtnemer niet kan aansluiten op het federatief koppelvlak van Opdrachtgever, biedt Opdrachtnemer zélf een sterke, in de markt gangbare, methode voor 2-factor authenticatie waarbij de 2de factor wordt gebaseerd op iets dat de gebruiker heeft, in de vorm van een authenticator-app. Authenticatie via onvertrouwde netwerken vindt te allen tijde plaats op basis van tenminste 2-factor authenticatie.

7.2 Opdrachtgever maakt gebruik van Conditional Access policies in Entra ID om de toegang tot de ICT Prestatie, in de breedste zin van het woord, te beperken tot door Opdrachtgever beheerde apparatuur. Opdrachtnemer waarborgt dat er geen alternatieve toegangspaden zijn, zoals een interne gebruikersadministratie, die dat mechanisme kunnen omzeilen.

8. Informatieveiligheid

9. Servicevoorwaarden

9.1 Opdrachtnemer heeft een common vulnerabilities disclosure (responsible disclosure) regeling die in lijn is met die van Opdrachtgever en draagt maximaal bij aan de gezamenlijke zorgplicht om te streven naar het voldoen aan de vigerende CVD-regeling van Opdrachtgever, tenminste qua reactie- en oplostijden. Er is een security.txt voorhanden conform de bijbehorende RFC en de inhoud verwijst naar Opdrachtgever als het om een subdomein van Opdrachtgever gaat. Er worden werkafspraken vastgelegd.