Gemeente Sittard-Geleen

Born

UITVRAGEN, AANBESTEDINGEN EN AFSPRAKEN

ICT & SECURITY EISEN

Opgesteld door:	Nabil El Khaldouni
Versienummer:	1.0
Referentie:	SE.CLD.01
Datum:	15-08-2023
Classificatie:	Intern gebruik

LET OP: Dit document beschrijft de stand van eisen op het moment van de laatste datum in versiebeheer. Dit is een dynamisch document en kan na wijziging van ICT beleid, BIO, NCSC richtlijnen en/of forum standaardisatie worden aangepast. Hier dienen zich na aanpassingen opdrachtnemers zich op aan te houden.

1. Algemeen

Referenties en stakeholders

Wie	Referentienummer
Paul Janssen	SE.CLD.01
Theo Derhaag	SE.CLD.01
Nabil El Khaldouni	SE.CLD.01

Reviewer

Naam	Functie	Datum	Versie
Paul Janssen	Adviseur Security & Privacy	15-08-2023	1.0
Theo Derhaag	Security Officer (CISO) | ENSIA Coordinator	15-08-2023	1.0

Versiebeheer

Versie	Datum	Auteur	Omschrijving
0.1	31-06-2023	Nabil El Khaldouni	Initiële opzet.
0.2	02-08-2023	Nabil El Khaldouni	Aanvullen SAAS eisen (alle).
0.3	10-08-2023	Nabil El Khaldouni	Inbreng eisen applicatiebeheer
0.4	10-08-2023	Nabil El Khaldouni	Inbreng eisen serverbeheer
0.5	14-08-2023	Nabil El Khaldouni	Inbreng eisen netwerkbeheer
1.0	15-08-2023	Nabil El Khaldouni	Finaal.

Inhoud

2. Inleiding

Dit document omvat de beveiligingsrichtlijnen en eisen voor alle ICT eisen die buiten en binnen de Gemeente Sittard-Geleen worden gehost, die van toepassing zijn op en gebruikt worden door de Gemeente Sittard-Geleen. Het hoofddoel is ervoor te zorgen dat de inrichting van ICT diensten en middelen voldoen aan de gestelde eisen vanuit beleid.

In samenwerking met de Gemeente Maastricht en de Gemeente Heerlen zijn specifieke eisen vastgelegd voor SAAS-applicaties. De in dit document gespecificeerde eisen zijn een uitbreiding op de vastgelegde eisen en zijn zorgvuldig opgesteld in overeenstemming met ons ICT beleid, informatiebeveiligingsbeleid, dat gebaseerd is op de Baseline Informatiebeveiliging Overheid (BIO) normen, NCSC richtlijnen en de eisen van het forum standaardisatie.

Door deze richtlijnen en vereisten te volgen, streven we naar een goede geborgd, veilig en betrouwbaar gebruik van ICT diensten en middelen om de vertrouwelijkheid en integriteit van onze gegevens en inzet te waarborgen.

Doelstelling

Het doel van dit document is om duidelijke eisen te stellen aan alle ICT diensten en middelen tijdens uitvragen, aanbestedingen en het bijwerken van bestaande verwerkingsovereenkomsten en afsprakendocumenten (Service Level Agreements). Hierbij streven we naar een veilige en betrouwbare werking van ICT diensten en middelen die we gebruiken.

3. ICT security eisen

Algemeen

Deze paragraaf schrijft de toepassing voor van het beleid en de standaarden met betrekking tot de beveiliging van (web)applicaties en diensten binnen onze organisatie. De tabel hieronder, Tabel 1 - Beleid en standaarden, bevat specifieke eisen en richtlijnen waaraan alle te leveren (web)applicaties en diensten dienen te voldoen om een hoog niveau van informatiebeveiliging te waarborgen.

De veiligheid van onze informatiesystemen en de bescherming van gevoelige gegevens zijn van het grootste belang. Om dit te garanderen, dienen alle (web)applicaties en de bijbehorende infrastructuur te voldoen aan de Baseline Informatiebeveiliging Overheid (https://bio-overheid.nl/) en de verplichte standaarden van het Forum Standaardisatie (https://www.forumstandaardisatie.nl/open-standaarden/lijst/verplicht).

Onderstaande tabel biedt een overzicht van de specifieke eisen die van toepassing zijn op het gebied van informatiebeveiliging voor de te leveren (web)applicaties en diensten. Het naleven van deze beleidsregels en standaarden is van essentieel belang voor het waarborgen van de integriteit en vertrouwelijkheid van onze systemen en gegevens.

Tabel 1 – Beleid en standaarden

SE.CLD.01.1	*De te leveren (web)applicatie/dienst voldoet aan de Baseline Informatiebeveiliging Overheid. https://bio-overheid.nl/*
SE.CLD.01.2	*De complete omgeving, dus alle (web)applicaties en onderliggende infrastructuur zijn ingericht conform de verplichte standaarden van het Forum Standaardisatie: zie link. https://www.forumstandaardisatie.nl/open-standaarden/lijst/verplicht*

Beheerorganisatie

De beheerorganisatie van de opdrachtnemer speelt een cruciale rol bij het waarborgen van de veiligheid en integriteit van onze, door hen gehoste systemen. In Tabel 2 - Verklaring omtrent gedrag tegenpartij, worden de vereisten uiteengezet met betrekking tot de medewerkers van de opdrachtnemer (beheerorganisatie). Het is van het grootste belang dat alle betrokken medewerkers beschikken over een recente Verklaring Omtrent Gedrag (VOG) of over een Screening van Justitie, om zo een hoog niveau van betrouwbaarheid en beveiliging te garanderen. Deze maatregelen dragen bij aan het versterken van ons beveiligingsbeleid en het beschermen van vertrouwelijke informatie tegen mogelijke risico's.

Tabel 2 – Verklaring omtrent gedrag tegenpartij

SE.CLD.01.3	*De medewerkers van de opdrachtnemer (beheerorganisatie) hebben een recente Verklaring Omtrent Gedrag (VOG) of beschikken over een Screening van Justitie.*

Authenticatie

Authenticatie is een essentieel aspect van onze beveiligingsmaatregelen om de toegang tot uitbesteedde diensten te waarborgen. In Tabel 3 - Authenticatie op uitbesteedde diensten, worden specifieke eisen en richtlijnen uiteengezet met betrekking tot het gebruik van verschillende authenticatiemethoden. Het doel is om robuuste en veilige digitale toegangscontrole te waarborgen en ervoor te zorgen dat de aangeboden oplossing naadloos aansluit op onze gemeentelijke authenticatiemogelijkheden.

Deze paragraaf behandelt het gebruik van DigiD en eIDAS voor respectievelijk inwoners en bedrijven, waarbij er strikte vereisten zijn voor de aansluiting en jaarlijkse verantwoording aan Logius doormiddel van strikte audits en pentesten. Daarnaast wordt het gebruik van Azure AD door ons benadrukt als eis voor accountsynchronisatie en centralisatie voor accountbeheer. Ook wordt de mogelijkheid van implementatie van MFA (Multi-Factor Authentication) op de doelapplicatie benadrukt als vereiste, wat bijdraagt aan een verhoogd beveiligingsniveau.

Het naleven van deze eisen is van essentieel belang om een hoog niveau van authenticatiebeveiliging te waarborgen en de vertrouwelijkheid van gegevens te beschermen bij het gebruik van uitbesteedde diensten.

Tabel 3 – Authenticatie op uitbesteedde diensten

SE.CLD.01.4	*De aangeboden oplossing maakt geen gebruik van lokale gebruikers, maar sluit aan op de gemeentelijke authenticatiemogelijkheden, LDAPS of Azure AD Connect. Het is niet toegestaan andere authenticatiemethodes te gebruiken of een eigen systeem in het netwerk van de Gemeente Sittard-Geleen te plaatsen.*
SE.CLD.01.5	*Ten behoeve van accountsynchronisatie wordt gebruik gemaakt van Azure AD Connect, SSO / SAML.*
SE.CLD.01.6	*Authenticatie voor burgers vindt plaats middels DigiD en eIDAS. Indien de DigiD aansluiting via Gemeente Sittard-Geleen wordt aangevraagd, dient de opdrachtnemer jaarlijks een TPM-verklaring opgesteld door een RE aan te leveren ten behoeve van de ENSIA-verantwoording aan Logius. De jaarlijkse kosten van deze TPM worden meegenomen in de totale kosten van de aangeboden webapplicatie. Ook de kosten van de TPM-verklaring ten behoeve van de aansluitaudit worden meegenomen.*
SE.CLD.01.7	*Wordt een gemeentelijke DigiD aansluiting gebruikt, dan dient de opdrachtnemer alle info aan te leveren inclusief het gebruikte publieke certificaat en metadata (XML), beide aangeleverd als bestand.*
SE.CLD.01.8	*Authenticatie voor bedrijven vindt plaats middels eHerkenning. De Gemeente Sittard-Geleen stelt het minimale betrouwbaarheidsniveau vast.*
SE.CLD.01.9	*Implementatie van MFA op de doel applicatie is verplicht.*
SE.CLD.01.10	*Alle accounts dienen persoonsgebonden te zijn.*

Web Services

Deze paragraaf omvat de technische eisen voor SAAS en bij ons gehoste web services, uiteengezet in Tabel 4. Het belangrijkste doel van deze eisen is om ervoor te zorgen dat onze web services op een veilige en betrouwbare manier functioneren, met specifieke aandacht voor de bescherming van gegevens en het voorkomen van mogelijke beveiligingsrisico's.

De eisen omvatten onder andere het gebruik van secure verbindingen (https) voor alle webverkeer, de implementatie van security headers in response headers, en de bescherming tegen OWASP top 10 aanvallen. Daarnaast wordt er gekeken naar de beveiliging van mobiele apps, het beheer van cookies en de ondersteuning van verschillende browsers.

Het naleven van deze technische eisen is van essentieel belang om een hoog niveau van beveiliging te waarborgen bij het gebruik van de SAAS of bij ons gehoste web services. Door deze maatregelen te implementeren, kunnen we de vertrouwelijkheid, integriteit en beschikbaarheid van onze diensten en gegevens effectief waarborgen.

Tabel 4 – Technische eisen voor de web services

SE.CLD.01.11	*In de response headers wordt de versie van de webserver of service niet meegestuurd.*
SE.CLD.01.12	*Foutmeldingen geven geen details weer die misbruik mogelijk maken.*
SE.CLD.01.13	*Al het webverkeer wordt middels TLS getransporteerd (https). Zie hiervoor ook de eisen voor TLS.*
SE.CLD.01.14	*Alleen de benodigde HTTP-request methoden worden gebruikt.* *(B.v. GET, POST, PUT, DELETE)*
SE.CLD.01.15	*Connecties via http worden automatisch doorverwezen naar https middels een http response status code 3xx.*
SE.CLD.01.16	*De webserver stuurt securityheaders mee in de response headers. Voor een actueel overzicht van mee te sturen securityheaders zie: https://owasp.org/www-project-secure-headers/* *Voor de Content Security Policy (CSP) geldt de volgende aanscherping: Onveilige configuraties zoals het gebruik van 'unsafe-inline' en 'unsafe-eval' zijn niet toegestaan. Het whitelisten van bronnen kan uitsluitend via een secure verbinding (https).* *De website heeft een A+ rating op https://securityheaders.com/*
SE.CLD.01.17	*De webapplicatie is minimaal beschermd tegen OWASP top 10 aanvallen.* *https://owasp.org/www-project-top-ten/*
SE.CLD.01.18	*De webapplicatie is conform de ict-beveiligingsrichtlijnen voor webapplicaties van het NCSC gebouwd. https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties*

SE.CLD.01.19	*Voor mobiele apps, dient de inschrijver aan de ICT-beveiligingsrichtlijnen voor mobiele apps te voldoen.* *https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-mobiele-apps. Zie ook richtlijnen document MDM van de gemeente Sittard-Geleen.* *Ook zijn de apps altijd beschikbaar in Apple of Android store, geen sideloaded apps toegestaan.*
SE.CLD.01.20	*Een webbased userinterface is zonder beperking van functionaliteit benaderbaar door de laatste twee versies van de meest gangbare en ondersteunde browsers Microsoft Edge is een vereiste (aanvullend Google Chrome, Apple Safari en Mozilla Firefox) zonder gebruik te maken van NPAPI plug-ins (zoals Flash, Silverlight, ActiveX, etc.)*
SE.CLD.01.21	*Gebruikte Cookies zijn voorzien van de attributen 'Secure' en 'HttpOnly'. Cookies met gevoelige informatie hebben een korte levensduur en maken gebruik van het 'SameSite' attribuut met als waarde 'Strict' of 'Lax'.*

E-mail

Deze paragraaf heeft betrekking op de beveiliging van mailcommunicatie binnen de Gemeente Sittard-Geleen en omvat Tabel 5 met specifieke eisen en standaarden voor de opdrachtnemer. Het doel is om de veiligheid en betrouwbaarheid van e-mailverzending te waarborgen, vanuit domeinen van de Gemeente Sittard-Geleen.

De vastgelegde eisen vereisen dat gebruik wordt gemaakt van standaarden zoals SPF, DKIM, STARTTLS en DANE bij het verzenden van e-mails vanuit de domeinen van de Gemeente Sittard-Geleen. Bovendien moet het versturen van mails verlopen via een sub-domein van de Gemeente Sittard-Geleen via het platform van onze gemeente, waarbij de criteria van forum standaardisatie en internet.nl wordt gehandhaafd.

Door te voldoen aan deze beveiligingsstandaarden kan een veilige en betrouwbare mailcommunicatie worden gegarandeerd, waarbij de privacy en vertrouwelijkheid van de e-mailcorrespondentie en ontvangt door tegenpartijen, zoals inwoners binnen de Gemeente Sittard-Geleen worden gewaarborgd.

Tabel 5 - Beveiliging van mailcommunicatie

SE.CLD.01.22	*Binnen de Gemeente Sittard-Geleen verloopt mailverkeer met een (sub)domein uitsluitend via onze exchange server. Hierdoor kunnen we het serviceaccount en het mailverkeer beter beheren en controleren. De volgende standaarden worden toegepast: SPF, DKIM, DMARC, STARTTLS, DANE.*
SE.CLD.01.23	*De opdrachtnemer maakt geen gebruik van een eigen mailservice.*
SE.CLD.01.24	*Veilig verzenden of mailen met zorgmail moet een ondersteunende functie zijn voor de applicatie.* *https://enovationgroup.com/nl/aanbod/producten/enovation-zorgmail/*

File Transfer Services

Deze paragraaf behandelt de beveiliging van grote bestandsoverdrachten vanuit de service(s) van opdrachtnemer. Tabel 6 omvat specifieke eisen voor deze overdrachten. Het doel is om ervoor te zorgen dat bestandsoverdrachten op een veilige manier plaatsvinden, met nadruk op het gebruik van beveiligde file transfer services.

Voor de overdracht van grote bestanden is het vereist om uitsluitend gebruik te maken van SFTP (bij voorkeur) of Explicit FTPS (TLS-handhaving). Bovendien moeten deze services verlopen via onze secure gateway (reverse proxy) of via een encrypted tunnel (VPN). Het naleven van deze beveiligingseisen waarborgt de bescherming van gegevens tijdens de overdracht en minimaliseert de risico's van ongeoorloofde datadiefstal.

Tabel 6 - Beveiliging van grote bestandsoverdrachten vanuit de service(s).

SE.CLD.01.25	*Bij handmatige bestandsoverdrachten dient gebruik gemaakt te worden van Doczend (via de gemeente Sittard-Geleen). Indien een file transfer service noodzakelijk is, kan alleen gebruik gemaakt worden van SFTP of Explicit FTPS (TLS enforcement). Dit gaat alleen via onze secure gateway (reverse proxy).*

Domain Name System (DNS)

Deze paragraaf behandelt de beveiliging van domainnamen en omvat Tabel 7 met specifieke eisen en maatregelen voor de opdrachtnemer. Het doel is om de veiligheid en integriteit van domainnamen te waarborgen, vooral wanneer de opdrachtnemer gebruikmaakt van een 'eigen' domein.

De vastgelegde eisen benadrukken het belang van het toepassen van DNSSEC (Domain Name System Security Extensions) wanneer een opdrachtnemer een eigen domein gebruikt. Tevens dienen domeinen waarvoor certificaten zijn uitgegeven, CAA records (DNS Certification Authority Authorization) te publiceren.

Voor controle op de naleving van deze technische eisen via forum standaardisatie en basisbeveiliging.nl van het 'eigen' domein en services die hier achter draaien, moet de gemeente een CNAME aanmaken met het bijbehorende overheidscertificaat dat in de applicatie moet worden toegevoegd.

Het voldoen aan deze beveiligingseisen is essentieel om de betrouwbaarheid en veiligheid van domainnamen te waarborgen, waardoor de kans op potentiële beveiligingsincidenten wordt geminimaliseerd. Door deze maatregelen te implementeren, kunnen we de integriteit van onze domainnamen waarborgen en onze systemen beschermen tegen mogelijke bedreigingen.

Tabel 7 – Beveiliging van domainnamen

SE.CLD.01.26	*Wordt door opdrachtnemer een ‘eigen’ domein gebruikt, dan moet DNSSEC (Domain Name System Security Extensions) worden toegepast.*
SE.CLD.01.27	*Domeinen waarvoor certificaten zijn uitgegeven dienen CAA records (DNS Certification Authority Authorization) te publiceren.*

SE.CLD.01.28	*Voor controle slagen via forum standaardisatie van het 'eigen' domein n.a.v. deze technische eisen moet de gemeente een CNAME op het eigen domein aanmaken met bijhorend overheidscertificaat die in de applicatie toegevoegd dient te worden.*

Transport Layer Security (TLS)

Deze paragraaf behandelt de beveiliging van SSL/TLS certificaten en configuratie, en omvat Tabel 8 met specifieke eisen en richtlijnen. Het belangrijkste doel is om ervoor te zorgen dat de transport layer security (TLS) op een veilige en conformerende manier wordt geïmplementeerd, met speciale aandacht voor het gebruik van erkende certificaten en sterke cipher suites.

Wanneer een domeinnaam wordt gebruikt die niet eigendom is van de Gemeente Sittard-Geleen, moet de opdrachtnemer een officieel erkend certificaat gebruiken dat voldoet aan de eisen van forum standaardisatie en dat alleen voldoende of sterke cipher suites gebruikt. TLS moet worden ingericht volgens de richtlijnen van het NCSC, en de server moet zo worden geconfigureerd en onderhouden dat deze een A+ rating behaalt op SSL Labs.

Het naleven van deze beveiligingseisen waarborgt de integriteit en vertrouwelijkheid van datatransmissie en versterkt de beveiliging van onze systemen tegen mogelijke aanvallen en inbreuken. Door de implementatie van erkende certificaten en de naleving van TLS-richtlijnen kunnen we een hoog niveau van transport layer security waarborgen en onze organisatie beschermen tegen beveiligingsrisico's.

Tabel 8 - Beveiliging van SSL/TLS certificaten en configuratie

SE.CLD.01.29	*Indien een domeinnaam wordt gebruikt die niet eigendom is van Gemeente Sittard-Geleen, dient de opdrachtnemer een officieel erkend certificaat te gebruiken. Die voldoet aan de eisen van forum standaardisatie en die alleen voldoende of sterke cipher suites gebruikt.https://www.ncsc.nl/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1*
SE.CLD.01.30	*TLS is volgens de richtlijnen van het NCSC ingericht. https://www.ncsc.nl/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1*
SE.CLD.01.31	*De server is zo ingericht en onderhouden dat deze een A+ rating behaalt op SSL Labs.* *https://www.ssllabs.com/ssltest/index.html*

Governance

Deze paragraaf behandelt governance en omvat Tabel 9 met specifieke eisen voor beleidsuitvoering en controle. De inschrijver en eventuele onderaannemers moeten voldoen aan ISO27001/2-certificering of ISAE3402 SOC2 assurance rapportage. Verder moet de opdrachtnemer jaarlijks een TPM-verklaring indienen, en de opdrachtnemer moet instemmen met pentesten en meewerken aan audits door de Gemeente Sittard-Geleen.

Tabel 9 – Uitvoeren van beleid, controle en principes

SE.CLD.01.32	*De inschrijver en eventuele onderaannemers zijn ISO27001/2 (Informatiebeveiliging) gecertificeerd en/of is in het bezit van een geldige ISAE3402 SOC2 assurance rapportage en/of levert ten tijde van de inschrijving jaarlijks een TPM-verklaring over de gehele dienstverlening inclusief onderaannemers, uitgegeven door een IT Auditor (RE en/of CISA), waarmee assurance wordt afgegeven over de kwaliteitsaspecten integriteit, beschikbaarheid en vertrouwelijkheid in opzet, bestaan en werking. De jaarlijkse kosten van de TPM worden meegenomen in de totale kosten van de aangeboden dienstverlening.*
SE.CLD.01.33	*De opdrachtnemer ondertekent bij gunning en vooraf aan de POC de vrijwaringsverklaring waardoor de Gemeente Sittard-Geleen pentesten kan (laten) uitvoeren op de aangeboden oplossing. De template van deze vrijwaringsverklaring kan bij de Gemeente Sittard-Geleen worden opgevraagd.*
SE.CLD.01.34	*De opdrachtnemer werkt kosteloos mee aan audits uitgevoerd door of in opdracht van de aanbesteder. Deze audits worden uitgevoerd door of onder verantwoordelijkheid van een RE of CISA.*

Cloud

Deze paragraaf behandelt de eisen voor de locaties van het aanbod van de SAAS services en omvat Tabel 10 met specifieke eisen. De geboden oplossing vereist dat de volledige ICT-infrastructuur in een datacenter binnen de EER (Europese Economische Ruimte) is ondergebracht.

Tabel 10 - Eisen voor locaties van het aanbod van de SAAS services

SE.CLD.01.35	*De ICT-infrastructuur van de geboden oplossing is in zijn geheel ondergebracht in een datacenter binnen de EER. (Niet van toepassing bij On Premise installatie).*

Koppelingen

Deze paragraaf gaat over de beveiliging van netwerkinfrastructuur en integraties, met Tabel 11 voor specifieke eisen. De oplossing moet ondersteuning bieden voor zowel IPv4 als IPv6, en koppelingen moeten inzichtelijk worden gemaakt in een protocol/firewall matrix. Alle koppelingen naar derden moeten via de integratielaag van de Gemeente Sittard-Geleen lopen, met specifieke beveiligingsniveaus. Het gebruik van RDP-koppelingen en Remote Desktop Gateway is niet toegestaan.

Tabel 11 - Beveiliging van netwerkinfrastructuur en integraties

SE.CLD.01.36	*De geboden oplossing ondersteunt zowel IPv4 als IPv6. Voor Cloud oplossingen dienen beide actief te zijn.*
SE.CLD.01.37	*Koppelingen/verbindingen tussen systemen en/of services (ook als deze op hetzelfde systeem draaien) worden door opdrachtnemer bij inschrijving inzichtelijk gemaakt in een protocol matrix, waarin de verkeerstromen zijn opgenomen. Deze matrix bestaat minimaal uit de volgende velden:* • *Source IPv(4/6)* • *Source Port* • *Destination IPv(4/6)* • *Destination Port* • *Layer 4 protocol (bijv. TCP/UDP/...)* • *Application protocol (bijv.: http/https/smtp/dns/...).*
SE.CLD.01.38	*Koppelingen vanuit de SaaS omgeving van de opdrachtnemer naar derden (bv andere SaaS omgevingen) lopen ten allen tijden via de integratie laag (reverse proxy) van de Gemeente Sittard-Geleen. Rechtstreekse koppelingen zijn dus niet toegestaan.*
SE.CLD.01.39	*Koppelingen vanuit de SaaS omgeving van de opdrachtnemer naar derden (bv andere SaaS omgevingen) lopen te allen tijde via de integratie laag van de Gemeente Sittard-Geleen. Rechtstreekse koppelingen zijn dus niet toegestaan.*
SE.CLD.01.40	*Koppelingen met onze integratie laag hebben minimaal het onderstaande beveiligingsniveau:* *REST architectuur: TLS & API Key* *SOAP / StUF architectuur: TLS Mutual Authentication*
SE.CLD.01.41	*Het aanbieden van RDP-koppelingen (of vergelijkbaar) evenals het gebruik van Remote Desktop Gateway is niet toegestaan.*

Versiebeheer

Alle webapplicaties en onderliggende ICT-componenten moeten altijd up-to-date zijn. De opdrachtnemer mag maximaal 1 stabiele versie aan het einde van de train achterlopen, maar alleen als deze versie nog volledig wordt ondersteund door de leverancier.

Tabel 12 – Patchmanagement en updates

SE.CLD.01.42	*De webapplicatie en onderliggende ICT-componenten zijn altijd up-to-date. Opdrachtnemer mag maximaal 1 stabiele patch aan het einde van de train (bijv 1.0.0.**1**)achterlopen, mits deze versie nog volledig wordt ondersteund door de betreffende leverancier van dat component en geen kwetsbaarheden bevat.*

Security incidenten

Deze paragraaf gaat over ICT security incidenten en CVE's (Common Vulnerabilities and Exposures), met Tabel 13 voor specifieke eisen. Bij security incidenten moet de opdrachtnemer deze onverwijld (binnen 4 uur) melden bij de Gemeente Sittard-Geleen, zowel per telefoon als per e-mail.

In het geval van security incidenten moeten de gevolgen zo snel mogelijk worden hersteld of beperkt, zodat het incident onder controle wordt gebracht. De Gemeente Sittard-Geleen moet op de hoogte worden gesteld van de genomen maatregelen. Dit waarborgt een snelle en effectieve reactie op security incidenten, waardoor de beveiliging van de systemen en gegevens wordt versterkt.

Tabel 13 – ICT security incidenten en CVE's.

SE.CLD.01.43	*Security incidenten worden onverwijld (binnen 4 uur), na hiervan op de hoogte te zijn, gemeld bij de Gemeente Sittard-Geleen. (Per telefoon +31464778999 en per e-mail aan: soc@sittard-geleen.nl en sd-ict@sittard-geleen.nl)*
SE.CLD.01.44	*Bij security incidenten worden de gevolgen zo snel mogelijk ongedaan gemaakt dan wel beperkt, waardoor het incident onder controle wordt gebracht. Over de genomen maatregelen wordt de Gemeente Sittard-Geleen geïnformeerd.*

Logging

Logging is essentieel voor het vastleggen van belangrijke gebeurtenissen en handelingen binnen de oplossing. De oplossing moet een niet-muteerbare audit-trail bevatten met informatie zoals de gebeurtenis, gebruikersidentificatie, apparaatgebruik, handelingsresultaat, en tijdstip. Logregels mogen geen gegevens bevatten die de beveiliging kunnen compromitteren. De logging moet ten minste 6 maanden worden bewaard en indien nodig moet de Gemeente Sittard-Geleen toegang krijgen tot logfiles op de omgeving van de opdrachtnemer.

Tabel 14 – Loggingscriteria

SE.CLD.01.45	*De oplossing beschikt voor alle mutaties over een niet-muteerbare audit-trail met daarin minimaal:* • *de gebeurtenis;* • *de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een gebruiker;* • *het gebruikte apparaat;* • *het resultaat van de handeling;* • *een datum en tijdstip van de gebeurtenis.*
SE.CLD.01.46	*Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden.*
SE.CLD.01.47	*Ten behoeve van de loganalyse is de bewaarperiode van de logging bepaald op 6 maanden. Binnen deze periode is de beschikbaarheid van de loginformatie gewaarborgd.*
SE.CLD.01.48	*Indien logging bij de Gemeente Sittard-Geleen niet kan, wordt voor de Gemeente Sittard-Geleen toegang geregeld tot de logfiles op de omgeving van de opdrachtnemer.*
SE.CLD.01.49	*Accounting van wijzigingen door specifieke accounts dient aan te staan en mogelijk te zijn binnen de gehoste service.*

OTAP

De aangeboden oplossing moet een OTA-omgeving bevatten.

Tabel 15 – Volledige OTAP-straat

SE.CLD.01.50	*In de aangeboden oplossing wordt tevens de OTA-inrichting meegenomen.*

Back-ups

Deze paragraaf beschrijft essentiële eisen voor het veiligstellen, bewaren en beschermen van kritieke gegevens, zoals vastgelegd in Tabel 16. Van regelmatige back-ups tot veilige verwijdering, deze voorschriften vormen de opzet van onze gegevensbescherming en recovery strategie.

Tabel 16 - Eisen voor back-ups en bijhorende retentie

SE.CLD.01.51	*Regelmatige, geautomatiseerde back-ups van kritieke systemen en gegevens.* *Minimaal dagelijkse back-up.*
SE.CLD.01.52	*Validatie van back-up gegevens voor integriteit.* *Mechanismen voor authenticatie van back-up gegevens.*
SE.CLD.01.53	*Fysiek gescheiden opslaglocatie.* *Beveiligde opslaglocaties tegen fysieke schade en ongeoorloofde toegang.*
SE.CLD.01.54	*Versleuteling van back-up gegevens tijdens opslag en transport.*
SE.CLD.01.55	*Gedocumenteerde en geteste herstelprocedure.* *Gedefinieerde hersteltijden volgens organisatiebehoeften.*
SE.CLD.01.56	*Periodieke hersteltests voor effectiviteit.*
SE.CLD.01.57	*Bewaartijd gebaseerd op beleidsvereisten, zie hieronder:* *Reguliere back-up 30 dagen bewaartijd.*
SE.CLD.01.58	*Veilige en permanente verwijdering van verouderde back-ups.* *Gedetailleerde logboeken van bewaar- en verwijderacties. Zie ook logging eisen.*
SE.CLD.01.59	*Gedocumenteerde rechtvaardiging voor uitzonderingen*

Bijlagen

Lijst met alle tabellen.