ICT Eisen	Programma van ICT Eisen voor de levering van Bedrijfsafvalverwerking
ICT1	**Bedrijfsafvalverwerkingssportaal**
1	De opdrachtnemer levert een bedrijfsafvalverwerkingsportaal
2	Op 01-01-2027 moet de door opdrachtnemer aangeboden oplossing in productie zijn.
3	De opdrachtnemer garandeert dat gedurende de contractperiode de aangeboden oplossing wordt onderhouden, ondersteund en doorontwikkeld
4	IPv4 en IPv6 dienen ondersteund te worden en in staat te zijn om te kunnen communiceren via IPv4-only, via IPv6-only en via dual-stack netwerken. Als de software netwerkparameters in haar lokale of remote server-instellingen bevat, dan moet de software ook de configuratie van IPv6-parameters ondersteunen. Alle functies die via IPv4 worden aangeboden moeten ook via IPv6 beschikbaar zijn. De opdrachtgever/eindgebruiker mag geen verschil ervaren wanneer de software via IPv4 of IPv6 communiceert, tenzij dit een expliciet voordeel voor de gebruiker oplevert.
4.1	Het is niet toegestaan om vaste IPv6 adressen in de softwarecode op te nemen.
5	De voorziening is een webbased oplossing en het front-end voor de medewerkers van de opdrachtgever bestaat uit een webapplicatie.
6	De voorziening is volledig in het Nederlands in woord en geschrift.
ICT2	**Doelgroep gebruikers**
1	De door de opdrachtnemer geleverde oplossing geeft het recht tot gebruik van de voorziening door alle medewerkers van de opdrachtgever en uitvoeringsorganisaties voor zover deze taken uitvoeren voor de opdrachtgever.
ICT3	**Beschikbaarheid**
1	De oplossing is 96,0% beschikbaar: Bij beschikbaarheid laag: De voorziening mag incidenteel uitvallen voor langer dan 1 dag (ook in piekperiodes) en de maximale hersteltijd (RTO) in geval van incidenten is binnen 40 werkuren (5 werkdagen van 8 uur). Dus maximaal totaal 14 dagen p.j. uitval en herstel is maximaal 40 uur (> 96%). Dataverlies mag maximaal 24 uur bedragen.
	- binnen de werktijden van de opdrachtgever van maandag tot en met vrijdag tussen 07:00 uur tot 18:00 uur
	- buiten de werktijden van de opdrachtgever uitgezonderd ICT3.3
2	Onderhoudswerkzaamheden van opdrachtnemer vinden plaats na werktijden (ICT3.1) in de avonden, weekenden en op nationale feestdagen.
3	Een uitzondering op punten ICT3.1 en ICT3.2 zijn calamiteiten met een hoge prioriteit zoals onvoorziene zaken waarbij de integriteit van de gegevens in gevaar zijn, informatiebeveiligingsincidenten en rampen.
ICT4	**Performance**
1	De opdrachtnemer draagt zorgt voor een oplossing met voldoende (in praktijk gangbare en acceptabele) prestaties voor de eindgebruiker, hierbij moet worden uitgegaan van circa 5 concurrent eindgebruikers.
ICT5	**Technische beveiliging**
1	De opdrachtnemer hanteert een degelijk patchschema om alle componenten (zoals firmware, operating systems, applicaties) van de oplossing actueel te houden om verbeteringen door te voeren en bekende fouten op te lossen.
2	De opdrachtnemer geeft hoge prioriteit aan het snel installeren van de laatste beveiligingspatches.
3	De opdrachtnemer maakt gebruik van een hardeningsproces zodat alle ICT-componenten zijn gehard tegen aanvallen. Het realiseren hiervan leidt tot een beter beveiligd systeem dat moeilijker door kwaadwillenden is te misbruiken.
4	De toegang tot de webapplicatie maakt gebruik van een versleutelde (HTTPS) verbinding.
5	Bij het sturen en ontvangen van e-mails wordt gebruik gemaakt van alle hiervoor relevante, voor overheden verplichte, beveiligingsstandaarden en behaald het maildomein een 100% score op internet.nl.
6	Oplossing voldoet aan de vereisten van forum standaardisatie gedurende de looptijd van het contract. Daarbij geldt dat opdrachtgever behoort tot een overheidsorganisatie en daardoor alle normen gezien moeten worden als 'pas toe'
7	De opdrachtnemer zorgt ervoor dat netwerkverkeer tussen verschillende omgevingen niet kan worden onderschept door andere klanten die actief zijn binnen de systeemomgeving van opdrachtnemer.
8	De opdrachtnemer voert actief controles uit op systeemlogging.

9	Situaties waarin meer dan normale kwetsbaarheden of risico's aanwezig zijn, worden onmiddellijk gemeld aan en besproken met de opdrachtgever.
10	IT-voorzieningen en apparatuur bij opdrachtnemer zijn fysiek beschermd tegen toegang door onbevoegden en tegen schade en storingen.
11	Het gebruik van indirecte toegangsvormen (RDP, Citrix) om niet-webgebaseerde functionaliteit van de voorziening aan te bieden wordt als niet compliant beschouwd en is derhalve niet toegestaan.
ICT6	**Informatieveiligheid**
1	Leverancier laat minimaal jaarlijks en na significante wijzigingen een onafhankelijke, handmatige penetratietest uitvoeren op de geleverde dienst, gebaseerd op erkende standaarden (o.a. OWASP). Kwetsbaarheden worden binnen een termijn opgelost die passend is bij het vastgestelde risiconiveau, waarbij kritieke kwetsbaarheden met hoogste prioriteit worden verholpen en middels hertest worden gevalideerd.
2	De opdrachtnemer garandeert dat ongeautoriseerde personen geen toegang hebben tot gegevens of gegevensdragers (zoals harde schijven en back-upmedia) die tussentijds of na beëindiging van de overeenkomst worden verwijderd c.q. worden vervangen.
3	De opdrachtnemer zal indien hij (pogingen tot) ongeautoriseerde toegang tot de systeemomgeving signaleert, alle noodzakelijke maatregelen nemen teneinde de eventuele schade tot een minimum te beperken en herhaling te voorkomen. De (poging tot) ongeautoriseerde toegang alsmede alle getroffen maatregelen zullen direct aan de opdrachtgever worden gerapporteerd.
4	De opdrachtnemer verleent medewerking aan het uitoefenen van controle door of namens opdrachtgever op bewaring en gebruik van data en naleving van procedures.
5	De opdrachtnemer garandeert adequate back-up- en restorevoorzieningen van de oplossing waarbij in geval van een gebeurtenis buiten de invloedsfeer van de opdrachtnemer (bijvoorbeeld een ramp of incident) de afgesproken dienstverlening binnen 48 uur kan worden gecontinueerd en waarbij het verlies van gegevens maximaal 1 werkdag kan bedragen. De back-up retentie tijd voldoet aan de vereisten die de diverse wetgevingen stellen over processen die worden ondersteund middels de voorziening.
6	Het systeem dwingt 2 factor af voor inloggen vanaf buiten het netwerk. Hierbij wordt gebruikt gemaakt van Microsoft Authenticator.
6.1	Het systeem ondersteunt het afdwingen van een maximale gebruiksduur van een wachtwoord. Indien opdrachtnemer hier niet aan kan voldoen kan van deze eis, na goedkeuring van bevoegd ICT-manager van opdrachtgever, worden afgeweken.
6.2	De applicatie moet een functie hebben waarmee time-outs op het aantal foutieve inlogpogingen worden ondersteund. Onderscheid moet gemaakt kunnen worden tussen het inloggen vanaf het lokale netwerk of vanaf het internet. Indien opdrachtnemer hier niet aan kan voldoen kan van deze eis, na goedkeuring van bevoegd ICT-manager van opdrachtgever, worden afgeweken.
6.3	Wachtwoorden in de voorziening worden nooit in plaintext opgeslagen of verstuurd. Basic Authentication is niet toegestaan.
6.4	De voorziening forceert een verandering van wachtwoord bij het eerste gebruik (ingebruikname) van het systeem door individuele gebruikers. Indien opdrachtnemer hier niet aan kan voldoen kan van deze eis, na goedkeuring van bevoegd ICT-manager van opdrachtgever, worden afgeweken.
7	De voorziening voldoet aan de actuele vereisten gesteld in de NCSC beveiligingsrichtlijnen voor webapplicaties.
8	De voorziening voldoet aan de actuele vereisten gesteld in de NCSC ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS). Daarbij gaat opdrachtgever op dit moment uit van TLS 1.2.
9	Voor websites en publieke diensten wordt gebruikgemaakt van publiek vertrouwde certificaten, uitgegeven door een publiek erkende Certificate Authority (CA). Het gebruik van Self Signed certificaten is niet toegestaan.
9.1	Indien opdrachtnemer eigenaar is van een domein is opdrachtnemer verantwoordelijk voor aanschaf en beheer van het SSL-certificaat, inclusief het tijdig leveren en vervangen van het certificaat. Indien opdrachtgever eigenaar is van een domein, dan is dit belegd bij opdrachtgever.
9.2	De maximale geldigheidsduur van certificaten is 1 jaar, tenzij wetgeving of standaarden een kortere termijn voorschrijven.
9.3	SAN multidomain of wildcard-certificaten zijn, naar aanleiding van een expliciete risicoanalyse, toegestaan indien het beheer en de uitgifte aantoonbaar goed zijn geborgd (bijvoorbeeld via een centraal certificaatbeheerplatform).

9.4	Wildcard-certificaten worden uitsluitend toegepast binnen de grenzen van één webapplicatie of platformcomponent, en alleen wanneer alle subdomeinen onder het wildcard-domein binnen dezelfde security-zone en met hetzelfde beheerdomein vallen.
9.5	SAN multidomain certificaten zijn toegestaan, mits alle domein en-identiteiten binnen het certificaat behoren tot dezelfde webapplicatie, dezelfde security-zone en dezelfde beheerverantwoordelijkheid.
10	Opdrachtnemer maakt voor de uitwisseling van e-mail en bestanden met opdrachtgever gebruik van de door opdrachtgever aangeboden oplossing voor veilig mailen, welke voldoet aan de eisen uit NTA 7516:2019 (thans: Zivver). Indien leverancier een oplossing ter beschikking heeft kan dit na goedkeuring van bevoegd ICT-manager van de opdrachtgever als alternatief dienen.
11	Het systeem voldoet aan de vereisten die de AVG en de Archiefwet stellen.
12	Indien de leverancier werkzaamheden op afstand dient te verrichten kan via Teamviewer toegang tot het domein van Purmerend worden verkregen. Ondersteuning is hierbij op een afgesproken moment waarbij de werkzaamheden onder supervisie van opdrachtgever worden uitgevoerd.
ICT7	**Technisch beheer**
1	Systeem en Technisch beheer wordt geheel verzorgd door opdrachtnemer.
2	Opdrachtnemer conformeert zich aan de de definitie dat onder Technisch beheer de werkzaamheden worden verstaan die nodig zijn voor het waarborgen van de ononderbroken goede werking van de oplossing.
3	Opdrachtnemer conformeert zich aan de definitie dat onder Technisch beheer tevens de werkzaamheden worden verstaan van het continu en actief monitoren van o.a. de beschikbaarheid, capaciteit, continuïteit, back-up, beveiliging en data-integriteit.
4	Gebruikers van opdrachtgever worden enkel aangemaakt door opdrachtnemer na opdracht van een bevoegd ambtenaar van de opdrachtgever.
5	Eindgebruikers hebben geen lokale administrator rechten nodig.
ICT8	**Toegang voorziening via webapplicatie**
1	De webapplicatie is bruikbaar op apparaten met het Windows 11/2022 en hoger operating system, ook als het Windows operating systeem is gevirtualiseerd (SBC of VDI).
2	De webapplicatie is device aware en past de weergave (o.a. schaalbaarheid) aan het soort apparaat aan.
3	De webapplicatie is toegankelijk en compatible met de meest recente versie (en twee versies lager) van onderstaande webbrowsers: a. Microsoft Edge Chromium b. Mozilla Firefox c. Google Chrome d. Safari
4	Voor een webbased applicatie gelden de onderstaande eisen: a. Volledig HTML5 ondersteuning b. Het gebruik van JAVA is niet toegestaan. c. Het gebruik van plug-ins en extensions is niet toegestaan. d. Het gebruik van OpenGL of DirectX is niet toegestaan.
4.1	De webapplicatie controleert voor elk http-verzoek of de initiator geauthenticeerd is en de juiste autorisaties heeft.
ICT9	**Support SLA**
1	Medewerkers van opdrachtnemer bieden ondersteuning in de Nederlandse taal in woord en geschrift.
2	Opdrachtnemer levert voor de oplevering in de productieomgeving een Nederlandstalige handleiding voor de medewerkers van de opdrachtgever en houdt deze gedurende de looptijd van de voorziening c.q. overeenkomst actueel.
3	Opdrachtnemer beschikt over een helpdesk welke medewerkers van de opdrachtgever van maandag tot en met vrijdag van 8:00 tot 17:00 per telefoon te woord kan staan.
ICT10	**Opleiding**
1	De opdrachtnemer biedt een gebruikerstraining aan voor eindgebruikers.
2	Trainingen worden in het Nederlands gegeven; documentatie is in het Nederlands beschikbaar.
ICT17	**Overdracht gegevens/data bij beëindiging overeenkomst**

1	Alle gegevens in de voorziening zijn en blijven te allen tijde eigendom van opdrachtgever en mogen door opdrachtnemer niet voor andere dan de overeengekomen doeleinden worden gebruikt. Bij beëindiging van de overeenkomst worden alle gegevens, naar keuze van opdrachtgever, overgedragen aan de opdrachtgever in een standaard uitwisselformaat dan wel vernietigd/gewist. Hiervan wordt een bewijs van vernietiging door opdrachtnemer aangeleverd.
2	De geheimhoudingsplicht van de opdrachtnemer blijft ook na beëindiging overeenkomst bestaan.
3	Niettegenstaande het voorgaande mag de opdrachtnemer en haar vertegenwoordigers vertrouwelijke informatie bewaren voor zover dit nodig is om te voldoen aan wettelijke, regelgevende of nalevingsverplichtingen dan wel als overeenkomstig een bonafide beleid inzake het bewaren van documenten is opgesteld. De opdrachtnemer blijft de informatie vertrouwelijk behandelen, maakt geen gebruik van de informatie die niet voor andere dan de overeengekomen doeleinden worden gebruikt, noch maakt de opdrachtnemer deze niet openbaar zonder voorafgaande schriftelijke toestemming van de opdrachtgever.
4	De opdrachtnemer blijft na de beëindiging overeenkomst aansprakelijk voor een datalek, beveiligingsincidenten en beschikbaar blijven voor het oplossen van beveiligingsincidenten (datalekken) die voortkomen uit tekortkomingen, fouten of kwetsbaarheden die zijn ontstaan tijdens de uitvoering van de dienstverlening, maar die zich na beëindiging overeenkomst manifesteren. U kunt denken aan bijvoorbeeld back-up tapes. De opdrachtnemer is verplicht om deze incidenten kosteloos op te lossen en te mitigeren.

In ICT eisen genoemde producten	Huidige versie welke ondersteund moet worden binnen de aangeboden oplossing
Windows server	2022
Citrix Virtual Apps en Desktop	7 2209
Cognos BI	11
Microsoft 365 Apps for enterprise	Semi-annual
Oracle Server	19
Microsoft SQL Server	2022
NCSC ICT Beveiligingsrichtlijnen voor webapplicaties	Juli 2024
Azure MTA Oauth	2.0
NCSC ICT Beveiligingsrichtlijnen voor mobiele apps	December 2017