

Eis	Website	Categorie	Subcategorie	Omschrijving
E8-12	Veilig-website	8. Beheer, dienstverlening en contractafspraken	Onderhoud en rapportages	(Onderhouds)Werkzaamheden aan de aangeboden oplossing mogen de beschikbaarheid én het functioneren van risico- en crisiswebite niet beïnvloeden. M.a.w. onderhoud mag niet leiden tot downtime. Releasematig onderhoud wordt altijd gefaseerd uitgevoerd volgens het OTAP-proces.
E4-11	Beide	4. Techniek, hosting en beveiliging	Informatiebeveiliging en privacy	AI-systemen (zoals bepaald onder de AI Verordening (EU) 2024/1689) die op de websites ingezet worden voldoen aan de eisen van de AI verordening. De inschrijver kan, afhankelijk van diens rol in de AI verordening, aantonen dat voldaan wordt aan de verplichtingen die voor de inschrijver gelden vanuit de AI verordening.
E4-14	Beide	4. Techniek, hosting en beveiliging	Informatiebeveiliging en privacy	Alle door Inschrijver aangeboden diensten vallen binnen een door Inschrijver of zijn onderaannemers gebruikt ISMS (Information Security Management System), dat gecertificeerd is conform de ISO27001.
E1-01	Beide	1. Algemene uitgangspunten	Eigendom en samenwerking	Alle specifiek voor dit project ontwikkelde content, documentatie, databestanden, configuraties, maatwerkfunctionaliteiten en overige projectresultaten worden eigendom van Veiligheidsregio IJsselland, voor zover deze rechten niet aantoonbaar bij derden liggen of onder bestaande licenties vallen.
E1-04	Beide	1. Algemene uitgangspunten	Scope en kaders	Beide websites maken gebruik van hetzelfde contentmanagementsysteem.
E4-22	Beide	4. Techniek, hosting en beveiliging	Technische architectuur en hosting	Beide websites moeten tegelijkertijd IPv6 en IPv4 ondersteunen
E4-15	Beide	4. Techniek, hosting en beveiliging	Informatiebeveiliging en privacy	Bezoekers moeten een kwetsbaarheid kunnen melden. De website biedt een Coordinated Vulnerability Disclosure (CVD)-meldingsroute via een gepubliceerd security.txt-bestand (RFC 9116) met daarin een contactadres, verwijzing naar de CVD-policy en een geldig Expires-veld. De CVD-meldingsroute vereist geen registratie en maakt anonieme melding mogelijk.
E5-01	Veilig-website	5. Meldingsysteem en risico-/crisiscommunicatie	Banners en doorplaatsing	Bij een actief incident wordt de incidentinformatie direct en prominent zichtbaar getoond op de homepage van de Veilig-website. Bezoekers moeten vanaf de homepage duidelijk kunnen zien dat er een actief incident is en direct kunnen doorklikken naar de volledige incidentpagina met actuele informatie, updates en handelingsperspectieven.
E5-06	Veilig-website	5. Meldingsysteem en risico-/crisiscommunicatie	Incidenten en updates	Binnen een incident worden updates in chronologische volgorde weergegeven. De updates zijn herkenbaar als onderdeel van hetzelfde incident met een zichtbare tijdsaanduiding.
E4-10	Beide	4. Techniek, hosting en beveiliging	Informatiebeveiliging en privacy	De aangeboden oplossing beschikt over adequate logging en audittrail. De inschrijver beschikt over een procedure voor beveiligingsincidenten en inbreuken in verband met persoonsgegevens en handelt daarbij overeenkomstig artikel 5 van de Verwerkersovereenkomst Veiligheidsregio IJsselland.
E2-03	Beide	2. Vormgeving, gebruiksvriendelijkheid en toegankelijkheid	Digitale toegankelijkheid	De aangeboden oplossing dient te voldoen aan de eisen van WCAG 2.2, niveau AA. De toegankelijkheidsverklaringen worden door de Inschrijver, na in productie name, geleverd aan VRIJsselland. Inschrijver verplicht zich om, gedurende de looptijd van de overeenkomst de toegankelijkheidsverklaringen kosteloos te leveren, om de aangeboden oplossing continue te laten voldoen aan wet en regelgeving. Op dit moment is de geldigheidsduur van deze verklaring vastgesteld op 3 jaar.
E2-04	Beide	2. Vormgeving, gebruiksvriendelijkheid en toegankelijkheid	Digitale toegankelijkheid	De aangeboden oplossing ondersteunt automatische vertaling van websitecontent naar meerdere talen (minimaal Engels, Duits)
E6-01	Beide	6. Vindbaarheid, zoeken en koppelingen	Koppelingen en gegevensuitwisseling	De aangeboden oplossing ondersteunt een automatische koppeling met HR Office voor het tonen van actuele vacatures op de werken-bij pagina. Vacatures die in HR Office worden beheerd, worden automatisch gepubliceerd in een vacatureoverzicht op de website. Het vacatureoverzicht ondersteunt minimaal het tonen van functietitel, afdeling/eigen functiecategorie, sluitingsdatum, dienstverband in uren, salarisindicatie, voor zover deze gegevens vanuit HR Office beschikbaar worden gesteld. De inschrijver is verantwoordelijk voor de technische realisatie van de koppeling binnen de website en stemt met Veiligheidsregio IJsselland en HR Office af welke gegevens beschikbaar zijn en op welke wijze deze worden aangeleverd.
E4-16	Beide	4. Techniek, hosting en beveiliging	Informatiebeveiliging en privacy	De aangeboden oplossing ondersteunt Veiligheidsregio IJsselland bij het tijdig uitvoeren van verzoeken van betrokkenen als bedoeld in artikel 12 tot en met 22 AVG. De inschrijver levert hiervoor de benodigde ondersteuning en functionaliteiten overeenkomstig artikel 4.6 van de Verwerkersovereenkomst.
E4-03	Beide	4. Techniek, hosting en beveiliging	Informatiebeveiliging en privacy	De aangeboden oplossing voldoet aan de AVG en overige toepasselijke privacywetgeving. De Verwerkersovereenkomst Veiligheidsregio IJsselland maakt integraal en onlosmakelijk onderdeel uit van de overeenkomst en prevaleert bij tegenstrijdigheid ten aanzien van de verwerking van persoonsgegevens.
E4-05	Beide	4. Techniek, hosting en beveiliging	Informatiebeveiliging en privacy	De aangeboden oplossing voldoet aantoonbaar aan de BIO 2.0-numering, relevante open standaarden en toepasselijke beveiligingsrichtlijnen voor webapplicaties.
E7-04	Beide	7. Implementatie	Training en documentatie	De aangeboden oplossing wordt geleverd met: - Een functioneel ontwerp/beschrijving, waarin de processen en eventuele workflows beschreven zijn. - Documentatie van hoofdlijnen/keuzen die zijn gemaakt bij inrichting/configuratie van de aangeboden oplossing. - Handleidingen voor beheerders (functioneel en content).

Eis	Website	Categorie	Subcategorie	Omschrijving
E4-07	Beide	4. Techniek, hosting en beveiliging	Informatiebeveiliging en privacy	De authenticatie voor de eigen medewerkers wordt met de Azure AD koppeling verzorgd. Voor gebruikers die bekend zijn in de Active Directory van VRIJsselland die toegang zoeken tot de aangeboden oplossing geldt "single sign-on" (SSO).
E8-13	Veilig-website	8. Beheer, dienstverlening en contractafspraken	SLA, DPA en exit	De calamiteitenregeling beschrijft een plan voor het snel herstellen van functionaliteit na onverwachte gebeurtenissen en is verwerkt in de SLA.
E4-25	Corporate website	4. Techniek, hosting en beveiliging	Beschikbaarheid en continuïteit	De corporate website is minimaal 99,5% beschikbaar per kalendermaand
E4-06	Beide	4. Techniek, hosting en beveiliging	Informatiebeveiliging en privacy	De inschrijver beschrijft de technische en organisatorische beveiligingsmaatregelen waarmee wordt voldaan aan artikel 32 AVG en artikel 4.1 van de Verwerkersovereenkomst, waaronder maatregelen tegen gangbare bedreigingen zoals DDoS-aanvallen. Deze maatregelen worden opgenomen in of als bijlage bij de Verwerkersovereenkomst.
E4-01	Beide	4. Techniek, hosting en beveiliging	Beschikbaarheid en continuïteit	De Inschrijver garandeert d.m.v. backup & restore-procedures dat gegevensverlies maximaal 24 uur bedraagt.
E1-06	Beide	1. Algemene uitgangspunten	Wetgeving en normen	De inschrijver houdt de aangeboden oplossing kosteloos gedurende de looptijd van de overeenkomst in lijn met nieuwe of gewijzigde wet- en regelgeving en toepasselijke overheidsstandaarden.
E4-17	Beide	4. Techniek, hosting en beveiliging	Informatiebeveiliging en privacy	De inschrijver houdt een verwerkingsregister bij waarin de verwerkingsactiviteiten op basis van doeleinde zijn opgenomen die plaatsvinden op de websites.
E8-02	Beide	8. Beheer, dienstverlening en contractafspraken	Onderhoud en rapportages	De inschrijver informeert Veiligheidsregio IJsselland proactief over ontwikkelingen, wijzigingen en risico's die invloed kunnen hebben op de werking, veiligheid, beschikbaarheid, beheerbaarheid en doorontwikkeling van de websites en het CMS.
E4-02	Beide	4. Techniek, hosting en beveiliging	Informatiebeveiliging en privacy	De inschrijver is verantwoordelijk voor de verwerking van persoonsgegevens door door hem ingeschakelde subverwerkers en voldoet daarbij aan de verplichtingen uit artikel 28 lid 2 en 4 AVG en artikel 4.5 van de Verwerkersovereenkomst Veiligheidsregio IJsselland
E8-01	Beide	8. Beheer, dienstverlening en contractafspraken	Onderhoud en rapportages	De inschrijver is verantwoordelijk voor technisch beheer, onderhoud, beveiligingsupdates, beschikbaarheid en continuïteit van het CMS.
E7-03	Beide	7. Implementatie	Migratie en testen	De Inschrijver levert en beheert gedurende de implementatie en de contractduur, naast de productieomgeving, een acceptatie-omgeving en stelt deze beschikbaar aan de VRIJsselland. Dit volgens het OTAP-proces. De acceptatie-omgeving is een omgeving die zo dicht mogelijk bij de productieomgeving staat. Het OTAP-proces zorgt ervoor dat wijzigingen in de software gecontroleerd en stapsgewijs worden doorgevoerd, waardoor risico's worden beperkt en de kwaliteit van de software wordt gewaarborgd voordat deze in de productieomgeving wordt uitgerold.
E8-03	Beide	8. Beheer, dienstverlening en contractafspraken	Onderhoud en rapportages	De inschrijver levert maandelijks een SLA rapportage aan voor de functioneel beheerder. Deze rapportage bevat minimaal informatie over beschikbaarheid, uitgevoerd en gepland onderhoud, performance, verstoringen, oplostijden en afwijkingen ten opzichte van de afgesproken serviceniveaus.
E7-01	Beide	7. Implementatie	Migratie en testen	De inschrijver ondersteunt en begeleidt bij de contentmigratie naar de nieuwe websites.
E4-12	Beide	4. Techniek, hosting en beveiliging	Informatiebeveiliging en privacy	De inschrijver ondersteunt Veiligheidsregio IJsselland gedurende de contractperiode bij het uitvoeren en actualiseren van DPIA's en andere privacybeoordelingen, overeenkomstig artikel 4.7 van de Verwerkersovereenkomst
E7-02	Beide	7. Implementatie	Migratie en testen	De inschrijver stelt voorafgaand aan de migratie een SEO migratieplan op en voert dit uit, met als doel de bestaande vindbaarheid van de website in zoekmachines zoveel mogelijk te behouden. Dit plan bevat minimaal maatregelen voor URL behoud of redirects, metadata, paginatitels, headings, sitemaps, indexeerbaarheid en controle op gebroken links.
E8-11	Veilig-website	8. Beheer, dienstverlening en contractafspraken	Helpdesk en storingen	De Inschrijver verzorgt een helpdesk, welke als 'single point of contact' dienst doet voor het stellen van vragen, melden van incidenten en indienen van wijzigingsvoorstellen, als ook voor informatie over de afhandeling daarvan. De helpdesk is telefonisch bereikbaar van 8.00 uur tot 18.00 uur op werkdagen. Buiten deze tijden wordt een calamiteitenregeling door Inschrijver beschikbaar gesteld.
E7-05	Beide	7. Implementatie	Training en documentatie	De inschrijver verzorgt passende trainingen voor minimaal drie gebruikersgroepen: functioneel beheerders, contentgebruikers en Crisisfunctionarissen. De trainingen sluiten aan op de taken, rechten en verantwoordelijkheden van de betreffende gebruikersgroep.
E4-09	Beide	4. Techniek, hosting en beveiliging	Informatiebeveiliging en privacy	De inschrijver voert periodiek beveiligingstesten uit, waaronder minimaal jaarlijks een pentest en kwetsbaarhedenscan, en herstelt bevindingen tijdig.
E8-06	Beide	8. Beheer, dienstverlening en contractafspraken	SLA, DPA en exit	De inschrijver zorgt dat alle content en data van de website op elk moment exporteerbaar is in een open en volledig formaat.
E3-08	Beide	3. CMS en contentbeheer	Gebruikers, rollen en rechten	De opdrachtgever (functioneel beheerder) kan gebruikers, rollen, rechten, basisinstellingen en contentstructuren beheren zonder tussenkomst van de inschrijver.

Eis	Website	Categorie	Subcategorie	Omschrijving
E4-27	Veilig-website	4. Techniek, hosting en beveiliging	Informatiebeveiliging en privacy	De opdrachtnemer voorziet in een veilige fallback voorziening voor authenticatie, zodat bevoegde gebruikers toegang kunnen krijgen tot het CMS wanneer single sign on via Microsoft Entra ID tijdelijk niet beschikbaar is. De opdrachtnemer is verantwoordelijk voor de inrichting, het beheer, de beveiliging en het testen van deze fallback voorziening. De fallback voorziening mag alleen gebruikt worden door daartoe bevoegde gebruikers en moet voorzien zijn van passende beveiligingsmaatregelen, waaronder minimaal sterke authenticatie en logging.
E1-07	Beide	1. Algemene uitgangspunten	Wetgeving en normen	De Rijksoverheid hanteert verplicht toe te passen richtlijnen. Deze zijn vooral gericht op veiligheid, bescherming persoonsgegevens, toegankelijkheid en transparantie. De Inschrijver hanteert deze richtlijnen bij de ontwikkeling van de websites en gedurende de hele looptijd van de overeenkomst. Zie: https://www.communicatierijk.nl/vakkennis/rijkswebsites/verplichte-richtlijnen
E5-05	Veilig-website	5. Meldingssysteem en risico-/crisiscommunicatie	Incidenten en updates	De Veilig-website beschikt over een meldingssysteem waarmee bevoegde gebruikers tijdens incidenten snel incidentinformatie en updates kunnen aanmaken, bewerken en publiceren.
E5-10	Veilig-website	5. Meldingssysteem en risico-/crisiscommunicatie	Templates en contentelementen	De Veilig-website beschikt over templates voor thematische risicopagina's. Binnen dit template staan handelingsperspectieven voor inwoners centraal.
E4-26	Veilig-website	4. Techniek, hosting en beveiliging	Beschikbaarheid en continuïteit	De Veilig-website is 24 uur per dag, 7 dagen per week beschikbaar met een minimale beschikbaarheid van 99,99% per kalendermaand. Alle perioden waarin de Veilig-website niet beschikbaar is, ongeacht de oorzaak, worden aangemerkt als onbeschikbaarheid en tellen mee bij het bepalen van het beschikbaarheidspercentage. Onderhoud, updates, technische verstoringen, piekbelasting en incident- of crisissituaties vormen hierop geen uitzondering.
E2-05	Beide	2. Vormgeving, gebruiksvriendelijkheid en toegankelijkheid	Digitale toegankelijkheid	De websites beschikken over een digitaal toegankelijke videospeler die voldoet aan de geldende toegankelijkheidseisen. De videospeler werkt op desktop, tablet en mobiel.
E6-04	Beide	6. Vindbaarheid, zoeken en koppelingen	Zoekfunctie	De websites beschikken over een gebruiksvriendelijke zoekfunctie met relevante resultaten, inclusief filter en sorteermogelijkheden. De zoekfunctie doorzoekt paginatitels, intro's, bodytekst, metadata, taxonomie en doorzoekbare documenten, zoals PDF bestanden. De zoekfunctie ondersteunt synoniemen, veelgebruikte zoektermen en spellingsvarianten, bijvoorbeeld stroomstoring, stroomuitval en elektriciteitsuitval. Ook toont de zoekfunctie suggesties bij typfouten of wanneer er geen resultaten worden gevonden. De opdrachtgever kan content opnemen in of uitsluiten van zoekresultaten en de prioriteit van belangrijke zoekresultaten beïnvloeden.
E2-02	Beide	2. Vormgeving, gebruiksvriendelijkheid en toegankelijkheid	Devices	De websites inclusief alle pagina's en onderdelen moeten probleemloos functioneren op desktops, mobiele devices zoals tablets en smartphones en zijn zowel responsive als adaptive. De aangeboden oplossing is webbased en volgt de W3C-standaarden. Het design van de aangeboden oplossing is responsive.
E2-01	Beide	2. Vormgeving, gebruiksvriendelijkheid en toegankelijkheid	Design	De websites sluiten qua look and feel aan bij de huisstijl en huisstijlrichtlijnen van Veiligheidsregio IJselland. De inschrijver vertaalt de huisstijl naar een toegankelijk, gebruiksvriendelijk en herkenbaar webdesign.
E4-23	Beide	4. Techniek, hosting en beveiliging	Technische architectuur en hosting	De websites zijn geoptimaliseerd voor snelle laadtijden en goede prestaties. De inschrijver past hiervoor passende maatregelen toe, zoals optimalisatie van afbeeldingen, code, caching en hostingprestaties.
E6-03	Beide	6. Vindbaarheid, zoeken en koppelingen	SEO en GEO	De websites zijn goed vindbaar en indexeerbaar voor zoekmachines en AI gedreven zoekassistenten. Het CMS ondersteunt een zoekmachinevriendelijke en machineleesbare inrichting van content, waaronder het beheren van metadata, URL structuren, redirects, sitemaps, taxonomieën en onderlinge relaties tussen content.
E4-13	Beide	4. Techniek, hosting en beveiliging	Informatiebeveiliging en privacy	De websites, webapplicaties en onderliggende hostingomgeving zijn passend beveiligd tegen ongeautoriseerde toegang, datalekken, hackeraanvallen en kwaadaardige software. Dataverkeer is versleuteld met geldige SSL/TLS-certificaten en minimaal TLS 1.2. De inschrijver treft minimaal maatregelen op het gebied van firewalling, antivirus/antimalware, IDS/IPS, hardening, encryptie, monitoring en tijdig patchmanagement. De aangeboden webapplicaties zijn ingericht conform de relevante richtlijnen van het Nationaal Cyber Security Centrum, waaronder de ICT-Beveiligingsrichtlijnen voor Webapplicaties
E8-04	Beide	8. Beheer, dienstverlening en contractafspraken	SLA, DPA en exit	Een DAP maakt onderdeel uit van de overeenkomst en wordt na gunning door beide partijen opgesteld.
E8-05	Beide	8. Beheer, dienstverlening en contractafspraken	SLA, DPA en exit	Een SLA maakt deel uit van de overeenkomst en wordt na gunning door beide partijen opgesteld. Een voorbeeld SLA wordt in de aanbesteding opgevraagd als beoordelingscriterium.
E4-21	Beide	4. Techniek, hosting en beveiliging	Technische architectuur en hosting	Gegevens worden uitsluitend binnen Europese Economische Ruimte (EER) gehost en worden alleen doorgegeven naar buiten de EER onder uitdrukkelijke toestemming van Veiligheidsregio IJselland.
E3-15	Beide	3. CMS en contentbeheer	Media en formulieren	Het CMS beschikt over een overzichtelijke mediabibliotheek voor het beheren van mediabestanden. De mediabibliotheek ondersteunt minimaal een mappenstructuur, metadata- en tagbeheer, zoekfunctionaliteit en het identificeren van ongebruikte bestanden.



Eis	Website	Categorie	Subcategorie	Omschrijving
E3-07	Beide	3. CMS en contentbeheer	Contentbeheer en kwaliteit	Het CMS biedt bij het plakken van tekst vanuit tekstverwerkingsprogramma's, zoals Microsoft Word, de mogelijkheid om overbodige opmaak en ongewenste code te verwijderen (opmaak verwijderen). Redacteurs kunnen geplakte tekst eenvoudig opschonen, zodat de tekst consistent, toegankelijk en passend binnen de huisstijl wordt gepubliceerd.
E3-03	Beide	3. CMS en contentbeheer	Content en pagina's	Het CMS biedt vaste templates voorspecifieke contenttypen, zoals incidentenpagina's, zodat veelvoorkomende content op een consistente en herkenbare manier wordt opgebouwd en beheerd.
E3-09	Beide	3. CMS en contentbeheer	Gebruikers, rollen en rechten	Het CMS is in te richten met rollen en rechten, waarmee bepaald wordt wat de gebruiker in het CMS kan. Er moet voor aparte gedeeltes van de site apart lees- en/of schrijfrechten kunnen worden toegekend aan individuele (en groepen) gebruikers. Rechten moeten toegekend kunnen worden aan mensen binnen en buiten de organisatie. Denk hierbij aan medewerkers van gemeenten of partnerorganisaties.
E4-20	Beide	4. Techniek, hosting en beveiliging	Technische architectuur en hosting	Het CMS moet aantoonbaar ondersteund/onderhouden worden door een organisatie zoals een community of een associatie.
E3-04	Beide	3. CMS en contentbeheer	Content en pagina's	Het CMS ondersteunt flexibele paginaopbouw binnen vaste templates en huisstijlregels. Redacteurs kunnen pagina's gedeeltelijk zelfstandig opbouwen met beschikbare contentblokken, zoals tekst, afbeeldingen, video's, knoppen, formulieren, quotes, uitgelichte content, tegels, overzichten en downloads. Redacteurs kunnen deze contentblokken zelf toevoegen, verwijderen, verplaatsen, dupliceren en aanpassen, zonder tussenkomst van de inschrijver of de ontwikkeling van een nieuw template. De oplossing waarborgt daarbij toegankelijkheid en werking op verschillende schermformaten.
E3-05	Beide	3. CMS en contentbeheer	Contentbeheer en kwaliteit	Het CMS ondersteunt het aanmaken en beheren van interne links, deeplinks en ankers. Bij het wijzigen, verplaatsen of verwijderen van content, zoals pagina's, media en bestanden, signaleert het CMS mogelijke gebroken links en ondersteunt het herstellen of doorverwijzen van deze links.
E3-02	Beide	3. CMS en contentbeheer	Content en pagina's	Het CMS ondersteunt het aanmaken, bewerken, opslaan als concept, plannen, publiceren, depubliceren, archiveren en verwijderen van content. Het CMS beschikt over versiebeheer en een wijzigingslog. Per wijziging wordt vastgelegd welke gebruiker de wijziging heeft gedaan, wanneer deze wijziging is gedaan en welke content is aangepast. Eerdere versies van content kunnen worden ingezien en, indien nodig, worden hersteld.
E3-06	Beide	3. CMS en contentbeheer	Contentbeheer en kwaliteit	Het CMS ondersteunt het beheren van redirects. Bevoegde gebruikers kunnen redirects aanmaken, wijzigen en verwijderen, zodat bezoekers en zoekmachines automatisch worden doorgestuurd wanneer URL's wijzigen, pagina's worden verplaatst of content wordt verwijderd.
E3-12	Beide	3. CMS en contentbeheer	Media en formulieren	Het CMS ondersteunt het bewerken en optimaliseren van geüploade afbeeldingen. Redacteurs kunnen afbeeldingen minimaal bijsnijden, schalen, spiegelen en draaien. Geüploade afbeeldingen worden automatisch geoptimaliseerd voor webgebruik, waaronder bestandsgrootte, formaat en weergave op desktop, tablet en mobiel. Redacteurs kunnen per afbeelding alternatieve tekst toevoegen of aanpassen en, indien nodig, automatische optimalisatie uitschakelen.
E3-13	Beide	3. CMS en contentbeheer	Media en formulieren	Het CMS ondersteunt het maken en beheren van gebruiksvriendelijke en digitaal toegankelijke formulieren. Bevoegde gebruikers kunnen formulieren zelfstandig aanmaken, aanpassen en publiceren. Gepubliceerde formulieren sluiten qua vormgeving aan bij de huisstijl en het ontwerp van de website. Formulieren voldoen aan de geldende eisen voor privacy, beveiliging en digitale toegankelijkheid en zijn voorzien van passende anti-spam maatregelen.
E3-11	Beide	3. CMS en contentbeheer	Media en formulieren	Het CMS ondersteunt het uploaden, beheren en publiceren van gangbare bestandsformaten, waaronder PDF bestanden, Office documenten, afbeeldingen, audio bestanden en videobestanden. Daarnaast ondersteunt het CMS het embedden van externe content, zoals video's, kaarten, formulieren, socialmediaberichten of andere toegestane externe bronnen. Embedded content moet veilig, toegankelijk en responsive worden weergegeven.
E3-10	Veilig-website	3. CMS en contentbeheer	Gebruikers, rollen en rechten	Het CMS ondersteunt rollen en rechten waarmee Crisisfunctionarissen alleen toegang krijgen tot het meldingssysteem van de veilig website. Bevoegde beheerders van Veiligheidsregio Ijsselland kunnen deze toegang zelfstandig inrichten, wijzigen en beheren zonder tussenkomst van de inschrijver.
E4-19	Beide	4. Techniek, hosting en beveiliging	Technische architectuur en hosting	Het CMS wordt aangeboden als cloudoplossing en wordt niet geïnstalleerd binnen de ICT omgeving van Veiligheidsregio Ijsselland. Het CMS is bereikbaar via moderne webbrowsers, waaronder minimaal Edge, Chrome, Firefox en Safari, zonder aanvullende software installatie.
E4-18	Beide	4. Techniek, hosting en beveiliging	Technische architectuur en hosting	Het CMS wordt breed in de markt ondersteund en mag niet leiden tot ongewenste afhankelijkheid van één leverancier. Meerdere marktpartijen moeten aantoonbaar in staat zijn om diensten te leveren voor implementatie, beheer, onderhoud en doorontwikkeling van het aangeboden CMS.
E1-02	Beide	1. Algemene uitgangspunten	Scope en kaders	Het eindresultaat bestaat uit gebruiksvriendelijke websites, waarvan één met een meldingssysteem, die voldoen aan onze eisen en waarvan toepassing wensen zoals opgesteld in dit programma van eisen en begeleidend document in deze aanbesteding.
E8-07	Beide	8. Beheer, dienstverlening en contractafspraken	SLA, DPA en exit	Het exitplan maakt onderdeel uit van de overeenkomst en wordt uiterlijk binnen drie maanden na ondertekening gezamenlijk opgesteld door de inschrijver en Veiligheidsregio Ijsselland. De exitplan borgt minimaal de overdracht van beheer, content, data, configuraties, documentatie, koppelingen en eventuele maatwerkfunctionaliteiten.



Eis	Website	Categorie	Subcategorie	Omschrijving
E5-02	Veilig-website	5. Meldingssysteem en risico-/crisiscommunicatie	Banners en doorplaatsing	Het meldingssysteem biedt de mogelijkheid om bij een actief incident een goed zichtbare, maar niet overheersende banner te tonen op vrijsselland.nl . De banner verwijst naar de incidentpagina op de Veilig-website, waar actuele informatie, updates en handelingsperspectieven worden gepubliceerd.
E5-08	Veilig-website	5. Meldingssysteem en risico-/crisiscommunicatie	Incidenten en updates	Het meldingssysteem biedt de mogelijkheid om bovenaan een incidentpagina een basisbericht te plaatsen. Dit bericht blijft bovenaan zichtbaar, ook wanneer nieuwe updates worden gepubliceerd, en bevat bijvoorbeeld een korte samenvatting van het incident en het belangrijkste handelingsperspectief.
E5-04	Veilig-website	5. Meldingssysteem en risico-/crisiscommunicatie	Incidenten en updates	Het meldingssysteem maakt duidelijk zichtbaar of een incident actueel/open of gesloten is. Deze status is zichtbaar op de incidentpagina en in overzichten.
E5-09	Veilig-website	5. Meldingssysteem en risico-/crisiscommunicatie	Templates en contentelementen	Het meldingssysteem ondersteunt het koppelen van bestaande handelingsperspectieven aan incidenten en incidentupdates. Bevoegde Crisisfunctionarissen kunnen vanuit het meldingssysteem eenvoudig een relevant handelingsperspectief(f)(ven) selecteren en toevoegen aan een incident of liveblogupdate.
E5-03	Veilig-website	5. Meldingssysteem en risico-/crisiscommunicatie	Banners en doorplaatsing	Het meldingssysteem ondersteunt het tonen van een melding of banner op de website van de betreffende gemeente(s) bij een actief incident. Bevoegde Crisisfunctionarissen kunnen in het meldingssysteem instellen of de melding automatisch of handmatig wordt doorgezet naar de betreffende gemeentewebsite(s). De melding of banner verwijst naar de incidentpagina op de Veilig-website. Bij het sluiten van het incident wordt de banner automatisch gedeactiveerd.
E4-04	Beide	4. Techniek, hosting en beveiliging	Informatiebeveiliging en privacy	Indien cookies of vergelijkbare technieken worden gebruikt, ondersteunt de aangeboden oplossing een functionaliteit in de vorm van een cookiebanner en toestemmingsinrichting waar nodig conform de Telecommunicatiewet (artikel 11.7a Telecommunicatiewet) en AVG (artikel 5, 6 en 7 AVG).
E6-02	Beide	6. Vindbaarheid, zoeken en koppelingen	Koppelingen en gegevensuitwisseling	Indien in toekomst wordt gekozen voor een ander recruitmentstelsel dient de oplossing hiermee gekoppeld te kunnen worden.
E3-16	Beide	3. CMS en contentbeheer	Webstatistieken en optimalisatie	Inschrijver biedt de mogelijkheid op de websites om bezoekersaantallen, paginaweergaven, herkomst van bezoekers (vanuit welke website de bezoeker komt) op een privacyvriendelijke manier te kunnen weergeven via een cookiefunctionaliteit. De cookies is/zijn beperkt analytische cookies zoals bepaald in artikel 11.7a lid 3 onder b Telecommunicatiewet.
E1-05	Beide	1. Algemene uitgangspunten	Wetgeving en normen	Inschrijver conformeert zich aan de eisen van de GIBIT 2025 en de daarbij behorende ICT-kwaliteitsnormen
E8-09	Corporate website	8. Beheer, dienstverlening en contractafspraken	Helpdesk en storingen	Inschrijver conformeert zich bij het afhandelen van storingen voor de website en het CMS aan onderstaande bepalingen: Prio 1: responsetijd: 30 minuten Oplostermijn: Work-around binnen 4 uur Prio 2: responsetijd: 2 uur Oplostermijn: Work-around binnen 8 uur Prio 3: responsetijd: 1 werkweek Oplostermijn: Work-around binnen 8 uur Servicewindow: maandag tm vrijdag 7u00-18u00
E8-10	Veilig-website	8. Beheer, dienstverlening en contractafspraken	Helpdesk en storingen	Inschrijver conformeert zich bij het afhandelen van storingen voor het meldingssysteem en crisiscommunicatie aan onderstaande bepalingen: Prio 1: Servicewindow: 24/7 Prio 2: responsetijd: 2 uur; Oplostermijn: Work-around binnen 1 werkdag; Servicewindow: maandag tm vrijdag 7u00-18u00 Prio 3: responsetijd: 1 werkweek; Oplostermijn: Work-around binnen 2 werkdagen; Servicewindow: 24/7
E8-08	Beide	8. Beheer, dienstverlening en contractafspraken	SLA, DPA en exit	Inschrijver verzorgt jaarlijks een (kosteloze) kennisbijeenkomst waarbij minimaal 3 collega's van VRIJSS aan kunnen deelnemen. Doel is om essentiële vernieuwingen door te nemen en advies om het gebruik van de websites (op basis van de statistieken) en daarmee de beleving van de bezoekers te optimaliseren
E4-24	Beide	4. Techniek, hosting en beveiliging	Technische architectuur en hosting	Inschrijver voldoet en blijft voldoen aan de eisen zoals geformuleerd door https://www.forumstandaardisatie.nl/open-standaarden waaronder het gebruik van HTTPS en HSTS voor webverkeer.
E3-14	Beide	3. CMS en contentbeheer	Media en formulieren	Inzendingen via formulieren kunnen worden verzonden naar één of meerdere vooraf ingestelde e-mailadressen en zijn door bevoegde gebruikers exporteerbaar in een gangbaar bestandsformaat, zoals CSV of Excel. Indien een e-mailadres is ingevuld, ontvangt de inzender automatisch een ontvangstbevestiging in een opmaak die aansluit bij de huisstijl. De opslag, verzending en export van formuliergegevens voldoen aan de geldende eisen voor privacy en informatiebeveiliging.
E5-07	Veilig-website	5. Meldingssysteem en risico-/crisiscommunicatie	Incidenten en updates	Per incidentupdate kunnen tekst, foto's, video's en links naar achterliggende informatie of documentatie worden toegevoegd.
E3-01	Beide	3. CMS en contentbeheer	Content en pagina's	Redacteuren kunnen websitecontent en pagina's eenvoudig aanmaken, bewerken, publiceren en beheren, ook wanneer zij beperkte CMS ervaring hebben.
E1-03	Beide	1. Algemene uitgangspunten	Scope en kaders	Tijdens de uitvoering van het contract zullen alle gesprekken en correspondentie in de Nederlandse taal plaatsvinden.

Eis	Website	Categorie	Subcategorie	Omschrijving
E4-08	Beide	4. Techniek, hosting en beveiliging	Informatiebeveiliging en privacy	Voor het verwerken van (formulier)data bevatten de websites de nodige functionaliteiten om te kunnen voldoen aan de beginselen van de AVG, waaronder ook het inrichten van een toestemmingsvraag en het apart inrichten van een bewaartermijn per formulier. (Formulier)data wordt automatisch verwijderd indien de ingestelde bewaartermijn is verstreken

