Programma van Eisen onderhoud, beheer en doorontwikkeling websites

Datum
27-5-2026

1 Aanvullende eisen

Nummer	Eis
A 1	Opdrachtnemer hanteert Jira (of een functioneel gelijkwaardig systeem, mits vooraf schriftelijk goedgekeurd door ROC Mondriaan) als centraal projectmanagementsysteem voor de volledige uitvoering van de opdracht. Dit omvat minimaal: backlogbeheer, sprintplanning, taakverdeling, voortgangsbewaking en statusrapportage. ROC Mondriaan heeft te allen tijde inzage in het projectbord, inclusief alle actieve en geplande taken, de status van lopende sprints en de inhoud van de backlog. Opdrachtnemer zorgt ervoor dat de projectomgeving actueel en volledig is bijgehouden.
A 2	De Opdrachtnemer verklaart het volledige technisch en functioneel beheer, onderhoud en de doorontwikkeling van alle in Bijlage 7 beschreven onderdelen op zich te nemen. Dit omvat de websites (rocmondriaan.nl, vavohaaglanden.nl, menskracht.rocmondriaan.nl), technische architecturen, functionaliteiten, hosting, infrastructuur, DatoCMS en alle integraties en koppelingen (zoals Sqill, PortalPlus, Ubeeo, Voiceflow, Google Tag Manager, Google Analytics 4, Usercentrics en Google reCAPTCHA). ROC Mondriaan blijft volledig eigenaar van de Azure-tenant. Opdrachtnemer werkt met persoonlijke Azure-accounts die door ROC Mondriaan worden beheerd en verstrekt. ROC Mondriaan (ITO/FUB) behoudt een toezichthoudende rol over de Azure-omgeving, maar de operationele beheertaken liggen volledig bij de Opdrachtnemer.
A 3	De Opdrachtnemer dient proactief te adviseren over nieuwe technologieën, best practices en mogelijkheden om de websites toekomstbestendig te houden (bijv. headless commerce, personalisatie, AI-gedreven chatbots).
A 4	De Opdrachtnemer dient te adviseren over en implementatie van verbeteringen in gebruikerservaring (UX) en interface-design (UI), met aandacht voor toegankelijkheid en conversie-optimalisatie.
A 5	De Opdrachtnemer dient expertise aan te tonen in en te werken met DatoCMS als headless contentmanagementsysteem.
A 6	De Opdrachtnemer dient te coördineren en faciliteren bij de kennisoverdracht, toegang tot systemen, overdracht van credentials, API-tokens, code-repositories en documentatie van de huidige leverancier.
A 7	De Opdrachtnemer dient te zorgen voor een grondige test- en acceptatiefase voorafgaand aan de go-live, om de continuïteit te waarborgen.
A 8	De Opdrachtnemer dient alle werkzaamheden met betrekking tot de kerncompetenties (Nuxt 3, DatoCMS, Azure Container Apps) uit te voeren met eigen personeel. Onderaanneming van deze kerncompetenties is niet toegestaan zonder voorafgaande schriftelijke toestemming van Opdrachtgever.
A 9	Indien de Opdrachtnemer gebruik maakt van onderaannemers voor niet-kern werkzaamheden, dient hij dit vooraf te melden en goedkeuring te verkrijgen van Opdrachtgever. De Opdrachtnemer blijft te allen tijde volledig verantwoordelijk en aansprakelijk.

A 10	Alle nieuwe functionaliteiten en pagina's dienen te voldoen aan WCAG 2.1 niveau AA conform het Besluit digitale toegankelijkheid overheid. Opdrachtnemer levert bij oplevering een toegankelijkheidsrapportage aan.
A 11	Opdrachtnemer garandeert dat de transitie van de huidige leverancier uiterlijk op 10 januari 2027 volledig is afgerond, zonder onderbreking van de dienstverlening.
A 12	Alle door Opdrachtnemer ontwikkelde code, configuraties en documentatie worden opgeslagen in een door ROC Mondriaan toegankelijke Git-repository. ROC Mondriaan heeft te allen tijde volledige toegang tot deze repository. ROC Mondriaan wordt bij oplevering volledig en onvoorwaardelijk eigenaar van alle intellectuele eigendomsrechten op de door Opdrachtnemer ontwikkelde oplossingen (code, configuraties, documentatie, componenten en deliverables). Opdrachtnemer draagt alle auteursrechten, databankrechten en know-how over aan ROC Mondriaan. ROC Mondriaan verkrijgt een onbeperkt, eeuwigdurend, wereldwijd en overdraagbaar gebruiksrecht zonder aanvullende vergoedingen. Deze regeling voorkomt vendor lock-in: ROC Mondriaan kan de oplossing te allen tijde zelfstandig of via derden onderhouden, aanpassen en doorontwikkelen zonder technische, juridische of contractuele belemmeringen van Opdrachtnemer. Opdrachtnemer garandeert dat de oplossing geen inbreuk maakt op rechten van derden en vrijwaart ROC Mondriaan hiervoor.
A 13	Opdrachtnemer houdt een actuele technische documentatie bij van alle architectuurcomponenten, configuraties, koppelingen en customisaties. Deze documentatie is te allen tijde toegankelijk voor ROC Mondriaan.
A 14	Opdrachtnemer levert bij elke opgeleverde doorontwikkeling een bijgewerkte versie van de relevante documentatie aan.
A 15	Opdrachtnemer verzorgt minimaal één keer per jaar een kennissessie voor de relevante medewerkers van ROC Mondriaan over de werking van het platform, nieuwe functionaliteiten en best practices.
A 16	Indien ROC Mondriaan een urgent verzoek indient dat niet kan wachten tot de eerstvolgende reguliere sprint, spant Opdrachtnemer zich in om dit verzoek zo spoedig mogelijk op te pakken, ook indien dit parallel loopt aan de lopende sprint. Opdrachtnemer beoordeelt de haalbaarheid hiervan binnen één (1) werkdag en communiceert de verwachte doorlooptijd en eventuele impact op de lopende sprint aan ROC Mondriaan. Beide partijen stemmen gezamenlijk af over de prioritering. Spoedopdrachten worden geregistreerd en bijgehouden in het projectmanagementsysteem (Jira of gelijkwaardig) en zijn te allen tijde inzichtelijk voor ROC Mondriaan.
A 17	Opdrachtnemer stelt en onderhoudt een acceptatieomgeving die functioneel gelijkwaardig is aan de productieomgeving. Alle updates, patches en aanpassingen met hoge impact worden hier eerst volledig getest. Uitrol naar productie vindt plaats na expliciete goedkeuring van ROC Mondriaan, minimaal drie (3) werkdagen na kennisgeving van Opdrachtnemer (afwijking mogelijk bij kritieke beveiligingsupdates). De acceptatieomgeving dient waar mogelijk gekoppeld te zijn aan de acceptatie- en/of testomgevingen van relevante backofficesystemen (Sqill, PortalPlus, Ubeeo). ROC Mondriaan (ITO/FUB) faciliteert de toegang tot deze externe testomgevingen. Opdrachtnemer is verantwoordelijk voor de technische inrichting en het testen van de

	koppelingen. Bij niet-beschikbaarheid van een externe testomgeving documenteert Opdrachtnemer dit, communiceert de risico's en stemmen partijen de vervolgstappen af.
A 18	Opdrachtnemer hanteert de KPI's parameters voor het registreren, categoriseren en oplossen van incidenten en storingen. Incidenten worden door Opdrachtnemer gecategoriseerd op basis van de impact op de beschikbaarheid en functionaliteit van de websites en de bijbehorende integraties, conform de onderstaande prioriteitsindeling. Opdrachtnemer garandeert de naleving van de hieronder genoemde oplostijden gedurende de gehele looptijd van de raamovereenkomst, inclusief eventuele verlengingen. P1 – Kritiek: Volledige uitval van één of meer websites of kritieke functionaliteiten (zoals de aanmeldflow of de opleidingszoeker) waardoor de website niet of nauwelijks bereikbaar of bruikbaar is voor eindgebruikers. P2 – Hoog: Ernstige verstoring van een belangrijke functionaliteit of integratie (zoals Sqill, PortalPlus, Voiceflow of Usercentrics) met significante impact op de gebruikerservaring, zonder volledige uitval. P3 – Gemiddeld: Beperkte verstoring van een functionaliteit met beperkte impact op de gebruikerservaring. Een tijdelijke workaround is beschikbaar. P4 – Laag: Kleine fouten, cosmetische issues of wensen met minimale impact op de gebruikerservaring.
A 19	Security-updates • De leverancier monitort continu op beveiligingsmeldingen • Security-updates met hoge of kritieke impact worden binnen één werkdag na signalering opgepakt en als fastlane uitgevoerd. • Security-updates met middelhoge impact worden binnen vijf werkdagen ingepland en uitgevoerd. • De leverancier rapporteert maandelijks welke security-updates zijn uitgevoerd en welke nog openstaan, inclusief risico-inschatting.
A 20	Reguliere (niet-security) updates • scans worden wekelijks uitgevoerd. • De leverancier brengt elk kwartaal alle reguliere updates (frameworks, libraries, CMS-componenten, etc.) in kaart en levert een overzicht met impactanalyse en advies. • Reguliere updates worden binnen één kwartaal na akkoord van de opdrachtgever uitgevoerd.
A 21	Planning en communicatie • De leverancier informeert de opdrachtgever binnen twee werkdagen na detectie van een kritieke security-update. • Voor reguliere updates levert de leverancier per kwartaal een overzicht met:

	○ benodigde updates ○ risico's bij niet-updaten ○ inschatting van doorlooptijd ○ voorgestelde planning • De opdrachtgever geeft binnen vijf werkdagen akkoord; de leverancier verwerkt de updates conform de overeengekomen planning.
A22	De opdrachtnemer is verantwoordelijk voor het inrichten, uitvoeren en monitoren van een volledige back-upstrategie voor de binnen de scope vallende omgevingen. De back-upstrategie omvat minimaal de volgende componenten: De configuratie van DatoCMS, inclusief contentmodellen, contentitems, API-instellingen en gebruikersconfiguraties; De websites en bijbehorende configuraties binnen de Azure-omgeving van ROC Mondriaan, inclusief containerinstellingen, omgevingsvariabelen, netwerkconfiguraties en overige infrastructurele configuraties. De back-upstrategie wordt door de opdrachtnemer vastgelegd in een back-up- en herstelplan, dat vóór aanvang van de dienstverlening ter goedkeuring wordt voorgelegd aan ROC Mondriaan en minimaal jaarlijks wordt geactualiseerd. Het plan beschrijft minimaal: De frequentie van back-ups (minimaal dagelijks voor productieomgevingen); De bewaartermijn van back-ups (minimaal 30 dagen voor dagelijkse back-ups, minimaal 12 maanden voor maandelijkse back-ups); De opslaglocatie van back-ups, waarbij back-ups te allen tijde worden opgeslagen binnen de Europese Economische Ruimte (EER), in overeenstemming met de vereisten van de AVG; De herstelprocedure: hoe en binnen welke termijn kan een volledige of gedeeltelijke restore worden uitgevoerd? De testfrequentie: back-ups worden minimaal twee keer per jaar getest op herstelbaarheid, waarbij de resultaten worden gerapporteerd aan ROC Mondriaan. De opdrachtnemer draagt er zorg voor dat back-ups te allen tijde beschikbaar zijn voor ROC Mondriaan en dat ROC Mondriaan zelfstandig toegang heeft tot de back-upomgeving met lees- en herstelrechten. Bij beëindiging van de overeenkomst worden alle back-ups overgedragen aan ROC Mondriaan of een door ROC Mondriaan aangewezen partij, in een gangbaar en overdraagbaar formaat.
A23	Beheer van externe diensten en integraties • Het monitoren en signaleren van storingen in koppelingen, ook als de oorzaak buiten zijn invloedssfeer ligt; • Het coördineren van de oplossing richting de externe leverancier namens ROC Mondriaan; • Het informeren van ROC Mondriaan conform de SLA-reactietijden.

	De opdrachtnemer is niet aansprakelijk voor de hersteltijd als de oorzaak aantoonbaar en uitsluitend bij een derde partij ligt, mits hij tijdig heeft gesignaleerd en geëscaleerd.
A24	Bereikbaarheid servicedesk De opdrachtnemer stelt een servicedesk beschikbaar als centraal meldpunt voor incidenten, storingen, wijzigingsverzoeken en overige vragen met betrekking tot de dienstverlening. De servicedesk is minimaal bereikbaar op werkdagen (maandag tot en met vrijdag, met uitzondering van officiële Nederlandse feestdagen) tussen 08:00 en 17:00 uur. De servicedesk is bereikbaar via minimaal de volgende kanalen: Telefoon, voor urgente meldingen (minimaal P1 en P2 conform eis A18); E-mail, voor niet-urgente meldingen en vragen; Het projectmanagementsysteem (Jira of functioneel gelijkwaardig conform eis A1), voor het registreren en opvolgen van alle meldingen. Alle meldingen worden door de opdrachtnemer geregistreerd in het projectmanagementsysteem en zijn te allen tijde inzichtelijk voor ROC Mondriaan. De oplostijden zoals vastgelegd in eis A18 en de KPI's zijn onverkort van toepassing op alle via de servicedesk ingediende meldingen. Voor P1-incidenten (kritieke uitval) dient de opdrachtnemer ook buiten de reguliere bereikbaarheidsuren bereikbaar te zijn via een noodcontact (telefonisch), zodat de in eis A18 vastgelegde reactietijd van < 4 uur te allen tijde gewaarborgd kan worden.

2 Algemene eisen

Nummer	Eis
B 1	Opdrachtnemer gaat ermee akkoord dat door in te schrijven expliciet akkoord wordt gegaan met alles opgenomen in dit programma van eisen en overige bijlagen (waaronder de overeenkomsten en voorwaarden) en inschrijver verklaart daarmee automatisch expliciet dat hij voldoet aan de in het beschrijvend document en daarbij behorende bijlage(n) genoemde voorwaarden en eisen die aan de opdracht zijn gesteld.
B 2	Opdrachtnemer staat ervoor in dat hij de dienstverlening zoals omschreven in de aanbestedingsdocumenten, gedurende de looptijd van de (raam)overeenkomst - en de eventueel verlengde looptijd - kan leveren in de soort en kwaliteit zoals in deze aanbesteding is gevraagd.
B 3	Alle door uw organisatie overgelegde gegevens zijn volledig en naar waarheid ingevuld en kunnen door u gestand worden gedaan. U gaat ermee akkoord dat indien u onjuiste en of onvolledige gegevens heeft verstrekt, u wordt uitgesloten van gunning, zonder recht op vergoeding van welke schade of kosten dan ook.
B 4	Bij beëindiging van de overeenkomst dient de Opdrachtnemer zorg te dragen voor een gestructureerde overdracht naar een eventuele opvolgende partij.

B 5	Opdrachtnemer sluit vóór aanvang van de werkzaamheden een verwerkersovereenkomst conform artikel 28 AVG met opdrachtgever. Opdrachtnemer verwerkt persoonsgegevens uitsluitend conform gedocumenteerde instructies van opdrachtgever.

3 Technische eisen

Nummer	Eis

Eis C1	Ontwerp en ketenafhankelijkheden De opdrachtnemer waarborgt dat de toepassing zodanig is ontworpen dat ketenafhankelijkheden inzichtelijk zijn en uitval tijdig wordt gesignaleerd. Als minimumeis geldt: Inzicht in ketenafhankelijkheden — De opdrachtnemer brengt bij aanvang van de opdracht de afhankelijkheden van aanpalende systemen (zowel intern als extern, zoals hosting, DNS, leveranciers en ketenpartners) in kaart en stelt deze documentatie beschikbaar aan de opdrachtgever. Notificatie bij uitval — De toepassing en infrastructuur zijn ingericht om bij uitval van een component automatisch een kennisgeving te genereren richting de verantwoordelijke beheerder. Redundantie — De infrastructuur beschikt minimaal over: Active-passive inrichting van applicatieonderdelen; Een passieve backup netwerkverbinding; Een redundante aansluiting op de voeding. Periodieke heranalyse — De ketenafhankelijkheden worden minimaal jaarlijks opnieuw geanalyseerd en gedocumenteerd. Contractuele borging — Afspraken over redundantie, notificatie bij uitval en periodieke heranalyse van ketenafhankelijkheden worden contractueel vastgelegd met de hosting- en beheerpartij.
Eis C2	Capaciteitsbeheer De opdrachtnemer waarborgt dat de capaciteit van de toepassing en infrastructuur toereikend is voor de verwachte en piekbelasting. Als minimumeis geldt: Capaciteitsmonitoring — De opdrachtnemer monitort actief het gebruik van systeemcapaciteit (CPU, geheugen, opslag, bandbreedte) en signaleert tijdig wanneer capaciteitsgrenzen worden benaderd. Proactief capaciteitsbeheer — Bij verwachte groei in gebruikersaantallen of activiteiten neemt de opdrachtnemer proactief maatregelen om de benodigde capaciteit tijdig beschikbaar te stellen. Rapportage — De opdrachtnemer rapporteert minimaal per kwartaal over de capaciteitsbenutting en verwachte ontwikkelingen.
Eis C3	Testen van releases en performance De opdrachtnemer waarborgt de kwaliteit en beschikbaarheid van de toepassing door middel van gestructureerd testen. Als minimumeis geldt: Regressietesten na elke release — Na elke release voert de opdrachtnemer direct een regressietest uit om te verifiëren dat de beschikbaarheid en performance van de toepassing niet zijn afgenomen. De resultaten worden gedocumenteerd. Loadtesten bij significante wijzigingen — Bij grotere wijzigingen in het ontwerp of bij een verwachte significante verandering in het gebruikersverkeer voert de opdrachtnemer voorafgaand aan productiegang een loadtest uit met de verwachte gebruikersaantallen en activiteiten. Deze loadtest wordt niet tijdens gebruikersuren op de productieomgeving uitgevoerd. Testomgeving — De opdrachtnemer beschikt over een testomgeving die representatief is voor de productieomgeving. Rapportage — De opdrachtnemer rapporteert minimaal per kwartaal over uitgevoerde tests, bevindingen en eventuele verbeteracties.

Eis C4	Continue monitoring en incident management De opdrachtnemer waarborgt de continue beschikbaarheid van de toepassing door middel van monitoring en gestructureerd incident management. Als minimumeis geldt: Continue monitoring — De opdrachtnemer monitort 24/7 de beschikbaarheid van de toepassing en kritieke aanpalende systemen, inclusief responstijden en performance-indicatoren. Gestructureerd incident management — Bij geconstateerde uitval of degradatie start de opdrachtnemer onmiddellijk een gestructureerd proces voor notificatie van de opdrachtgever en herstel van de dienstverlening, conform de in de SLA overeengekomen escalatieprocedure. Incident logging en rapportage — Alle incidenten worden geregistreerd. De opdrachtnemer levert minimaal per kwartaal een rapportage met een overzicht van incidenten, oorzaakanalyses en genomen maatregelen. Proactieve signalering — De opdrachtnemer signaleert proactief afwijkingen van normale waarden in monitoring-indicatoren, ook wanneer dit nog niet tot daadwerkelijke uitval heeft geleid.
Eis C5	Herstel en disaster recovery De opdrachtnemer waarborgt tijdig herstel van de dienstverlening bij calamiteiten. Als minimumeis geldt: Warm Standby — De opdrachtnemer beschikt over een Warm Standby oplossing waarbij nieuwe fysieke of virtuele infrastructuur direct in gebruik kan worden genomen, met dien verstande dat enkele handelingen (zoals het overzetten van recente gegevens) nog noodzakelijk kunnen zijn. Maximale hersteltijd (RTO) — Herstel van de dienstverlening bedraagt niet langer dan 24 uur gerekend vanaf het moment van constatering van de calamiteit. Beperkt sessieverlies toegestaan — Verlies van enkele lopende sessies en transacties is toegestaan bij herstel, mits dit verlies beperkt blijft tot de periode na de laatste succesvolle back-up of synchronisatie. Jaarlijkse recovery test — De opdrachtnemer voert minimaal eenmaal per jaar een recovery test uit en documenteert de resultaten. Deze worden gedeeld met de opdrachtgever. Disaster Recovery Plan — De opdrachtnemer levert bij aanvang van de opdracht een gedocumenteerd Disaster Recovery Plan aan, dat minimaal de herstelprocedure, rollen en verantwoordelijkheden, escalatieprocedure, RTO en RPO bevat. Het plan wordt minimaal jaarlijks geactualiseerd.

Eis C6	Herleidbaarheid van gegevenswijzigingen door gebruikers De opdrachtnemer waarborgt dat wijzigingen in de content van de toepassing herleidbaar zijn tot individuele gebruikers. Als minimumeis geldt: Logging van gegevenswijzigingen — De toepassing registreert automatisch welke gegevens zijn gewijzigd, door welk gebruikersaccount en op welk tijdstip, binnen het CMS en de beheeromgeving. Mogelijkheid tot terugdraaien — De toepassing biedt de mogelijkheid om doorgevoerde wijzigingen in content terug te draaien naar een eerdere versie. Verbod op naamloze gebruikersaccounts — Naamloze of gedeelde gebruikersaccounts zijn niet toegestaan. Elk account dat wijzigingen kan doorvoeren is herleidbaar tot een individuele gebruiker of geïdentificeerd systeem. Rolgebaseerd rechtenbeheer — Gebruikersrechten worden ingericht volgens het principe van least privilege. Beheerdersrechten worden uitsluitend toegekend aan daartoe aangewezen functionarissen. Periodieke controle op autorisaties — De opdrachtnemer voert minimaal jaarlijks een controle uit op de toegekende gebruikersrechten en rapporteert de bevindingen aan de opdrachtgever.
Eis C7	Back-up van gegevens en integriteitscontrole De opdrachtnemer waarborgt dat gegevens periodiek worden geback-upt en dat de herstelbaarheid aantoonbaar is. Als minimumeis geldt: Minimale back-upfrequentie — Back-ups worden minimaal wekelijks uitgevoerd, bij voorkeur via een geautomatiseerd proces. Herstelbaarheid — De back-upoplossing is zodanig ingericht dat de content van de toepassing aantoonbaar herstelbaar is vanuit de gemaakte back-ups. Jaarlijkse integriteitscontrole — De integriteit van de back-ups wordt minimaal eenmaal per jaar gecontroleerd door middel van een hersteltest. De resultaten worden gedocumenteerd en op verzoek beschikbaar gesteld aan de opdrachtgever. Bewaartermijn — Back-ups worden minimaal 4 weken bewaard, tenzij schriftelijk een andere termijn is overeengekomen. Contractuele vastlegging — Back-upafspraken worden contractueel vastgelegd in de SLA met de hosting- en beheerpartij en zijn transparant voor de opdrachtgever.
Eis C8	Application controls — invoer- en uitvoercontroles De opdrachtnemer waarborgt dat de toepassing beschikt over adequate controles op de invoer en uitvoer van gegevens. Als minimumeis geldt: Invoervalidatie — De toepassing controleert alle invoer op minimaal syntaxcontrole, verplichte velden en, bij uploadfunctionaliteit, bestandstype en -inhoud (inclusief controle op malware). Uitvoersanering — Gegevens die worden doorgegeven aan andere systemen worden opgeschoond tot veilige waarden op basis van syntaxcontrole of whitelisting. Beperkte foutmeldingen — Foutmeldingen die zichtbaar zijn voor eindgebruikers bevatten uitsluitend de voor de gebruiker noodzakelijke informatie. Technische details en systeeminformatie worden niet getoond aan eindgebruikers.

Eis C9	Onweerlegbaarheid — logging van gebruikersactiviteit De opdrachtnemer waarborgt dat inlogactiviteit van gebruikers wordt gelogd en adequaat wordt beheerd. Als minimumeis geldt: Logging van inlogactiviteit — De toepassing registreert automatisch alle inlogactiviteit van gebruikers, inclusief minimaal tijdstip, gebruikersaccount en (indien beschikbaar) IP-adres. Doelbinding — Loggegevens worden uitsluitend gebruikt voor controle en ondersteuning, conform de AVG. Gebruik voor andere doeleinden is niet toegestaan zonder expliciete schriftelijke afspraak. Bewaartermijn — Loggegevens worden minimaal 13 maanden bewaard, tenzij schriftelijk een andere termijn is overeengekomen. Kwaliteit van logging — De opdrachtnemer past bij de inrichting van de logging best practices toe, met de OWASP Logging Cheat Sheet als referentiekader. Controle op logging — Loggegevens worden minimaal ad hoc gecontroleerd, in ieder geval bij incidenten of beveiligingsonderzoeken.
Eis C10	Herleidbaarheid van technische beheerwijzigingen De opdrachtnemer waarborgt dat technische wijzigingen aan de toepassing en configuratie herleidbaar zijn. Als minimumeis geldt: Logging van beheerwijzigingen — Alle technische wijzigingen aan de toepassing, configuratie en infrastructuur worden geregistreerd via beheeraccounts en een change-managementproces, met minimaal registratie van wat is gewijzigd, door welk account en op welk tijdstip. Mogelijkheid tot terugdraaien — Technische wijzigingen kunnen worden teruggedraaid naar een vorige stabiele toestand. Beperking van verhoogde rechten — Toegang met verhoogde rechten (systeemaccounts, root-accounts) is beperkt tot daartoe geautoriseerde functionarissen. Gebruik van root-accounts is uitsluitend toegestaan wanneer technisch noodzakelijk. Organisatorische functiescheiding — Volledige technische functiescheiding is niet in alle gevallen vereist, maar wordt minimaal organisatorisch geborgd door middel van procedures, autorisatiebeheer en periodieke controles. Jaarlijkse controle — De opdrachtnemer voert minimaal jaarlijks een controle uit op toegekende beheerrechten en naleving van het change-managementproces en rapporteert de bevindingen aan de opdrachtgever.
Eis C11	Controle op integriteit van de toepassing De opdrachtnemer waarborgt dat de integriteit van de toepassing, configuratie en software actief wordt bewaakt. Als minimumeis geldt: Patchmanagement — De status van patches en updates van firmware en software wordt actief beheerd en minimaal ad hoc gecontroleerd door de opdrachtnemer. Integriteitscontroles — De integriteit van configuratie en software wordt periodiek gecontroleerd, bij voorkeur via geautomatiseerde hash-checks. Waar automatisering niet beschikbaar is, worden handmatige controles uitgevoerd. Malwarebescherming — Op alle relevante lagen van de toepassing en infrastructuur zijn maatregelen tegen malware getroffen en actief in werking. Secure coding — De opdrachtnemer past secure coding guidelines toe bij ontwikkeling en onderhoud van de toepassing, conform erkende standaarden zoals de OWASP Secure Coding Practices. Veilige configuratie — De toepassing en infrastructuur worden geconfigureerd volgens het principe van security by default: onnodige functionaliteit, poorten en services zijn uitgeschakeld.

Eis C12	Onweerlegbaarheid van technisch beheer en tijdssynchronisatie De opdrachtnemer waarborgt dat activiteiten van technisch beheer worden gelogd en dat de tijdsregistratie consistent en betrouwbaar is. Als minimumeis geldt: Logging van beheeractiviteiten — Alle activiteiten van technisch beheer worden gelogd, inclusief configuratiewijzigingen, beheeracties en toegang met verhoogde rechten, met minimaal registratie van actie, account en tijdstip. Kwaliteit van logging — De opdrachtnemer past best practices toe bij de inrichting van beheerlogging, met de OWASP Logging Cheat Sheet als referentiekader. Tijdssynchronisatie — De systeemtijd van de toepassing wordt gesynchroniseerd met één centrale referentietijdbron binnen de hostingomgeving, die op haar beurt is gesynchroniseerd met een publieke tijdsbron (zoals NTP). Consistentie met aanpalende systemen — De tijdsbron is afgestemd op aanpalende systemen, zodat loggegevens uit verschillende systemen betrouwbaar gecorreleerd kunnen worden. Bescherming van loggegevens — Loggegevens zijn beschermd tegen manipulatie en ongeautoriseerde toegang. Beheerders hebben geen mogelijkheid hun eigen loggegevens te verwijderen of aan te passen. Bewaartermijn — Loggegevens van technisch beheer worden minimaal 13 maanden bewaard, tenzij schriftelijk een andere termijn is overeengekomen.
Eis C13	Levenscyclus van gegevens De opdrachtnemer waarborgt dat persoonsgegevens en andere gegevens worden beheerd conform wettelijke bewaartermijnen en het recht op verwijdering. Als minimumeis geldt: Naleving van bewaartermijnen — De toepassing ondersteunt de naleving van wettelijke bewaartermijnen voor persoonsgegevens, logging en overige relevante gegevenscategorieën. Recht op verwijdering — De toepassing biedt de mogelijkheid om persoonsgegevens te verwijderen, zowel op verzoek van de betrokkene als bij het verstrijken van de bewaartermijn. Veilige verwijdering van media — Op media en apparatuur die niet meer worden gebruikt of voor andere doeleinden worden hergebruikt, worden gegevens veilig gewist conform erkende standaarden.
Eis C14	Logische toegangsbeveiliging De opdrachtnemer waarborgt adequate beveiliging van de toegang tot de toepassing. Minimumeisen zijn: Authenticatie: Toegang tot de toepassing vereist minimaal authenticatie via gebruikersnaam en wachtwoord, conform NIST-richtlijnen. Toegang tot beheersystemen (DatoCMS, Azure, projectmanagementsysteem) is verplicht beveiligd met Multifactorauthenticatie (MFA). Waar mogelijk wordt Single Sign-On (SSO) via het Mondriaan-account (Azure AD/Entra ID) gebruikt voor gecentraliseerd toegangsbeheer. Toegangsbeleid: Een beleid voor logische toegang is geïmplementeerd voor supportmedewerkers, beheerders en ontwikkelaars. Periodieke controle: Het beleid omvat periodieke controle van actieve accounts ten opzichte van actieve medewerkers, zodat accounts van vertrokken medewerkers tijdig worden ingetrokken.

Eis C15	Netwerktoegangsbeveiliging De opdrachtnemer waarborgt dat de netwerktoegang tot de toepassing adequaat is beveiligd. Als minimumeis geldt: Netwerksegmentatie — De infrastructuur is ingericht met gescheiden netwerken, minimaal onderscheiden naar type (zoals WAN, LAN en wifi). Firewalling — Toegang vanuit andere netwerksegmenten is beschermd door een firewall die onnodige poorten en services afsluit. Beveiligde externe toegang — Externe toegang voor medewerkers en beheerders is uitsluitend mogelijk via een beveiligde verbinding met authenticatie en encryptie.
Eis C16	Transport- en opslagbeveiliging De opdrachtnemer waarborgt dat gegevens tijdens transport adequaat zijn versleuteld. Als minimumeis geldt: Encryptie van extern verkeer — Alle extern verkeer van en naar de toepassing is versleuteld conform de meest recente versie van de Uniforme Beveiligingsvoorschriften (UBV) TLS van Edustandaard, inclusief koppelingen, cloud-verbindingen en back-ups. Gebruik van erkende standaarden — Voor de inrichting van encryptie worden erkende richtlijnen en best practices gehanteerd, zoals die van het NCSC, ENISA of NIST. Intern verkeer — Encryptie van intern verkeer is niet verplicht, maar wordt aanbevolen waar gevoelige gegevens worden verwerkt.

4 Levering en personeel

Nummer	Eis
D 1	De benodigde werkzaamheden ten behoeve van beheer, onderhoud en ontwikkelen websites vinden plaats op de met Opdrachtgever overeengekomen dag(en) en tijdstip(pen).
D 2	Opdrachtnemer staat ervoor in dat zijn werknemers dan wel door hem in te schakelen derden desgevraagd kunnen beschikken van een geldige Verklaring Omtrent het Gedrag (VOG).
D 3	Opdrachtnemer garandeert dat zijn werknemers of door hem in te schakelen derden bij uitvoering van de werkzaamheden vertrouwelijkheid en geheimhouding betrachten wat ten aanzien van wat hen bij de uitvoering van de werkzaamheden bekend wordt.
D 4	Opdrachtnemer instrueert het door hem in te zetten personeel over arbo, veiligheid en milieu.
D 5	Het personeel dient zich te houden aan de in het betreffende gebouw van toepassing zijnde huisregels.
D 6	In te zetten personeel dient zich te kunnen identificeren bij het verkrijgen van toegang tot de panden van ROC Mondriaan.
D 7	Opdrachtnemer zal indien ROC Mondriaan hier om vraagt een account/projectmanager bij opdrachtgever inzetten.

4 Communicatie

Nummer	Eis

E 1	Opdrachtnemer stelt gedurende de duur van de (raam)overeenkomst voor ROC Mondriaan een vaste contactpersoon beschikbaar. Bovendien draagt Opdrachtnemer zorg voor vaste plaatsvervangers bij afwezigheid. De contactpersoon van Opdrachtnemer is in ieder geval telefonisch bereikbaar tussen 08:30 en 17:00 uur op werkdagen en reageert binnen één (1) werkdag op e-mail.
E 2	De contactpersonen van Opdrachtnemer en het personeel van Opdrachtnemer dat op de opdracht van ROC Mondriaan wordt ingezet dienen de Nederlandse taal in woord en geschrift machtig te zijn.
E 3	De communicatie met betrekking tot operationele zaken, vindt plaats tussen opdrachtnemer en de verantwoordelijke namens de contactpersoon bij de dienst communicatie van ROC Mondriaan.
E 4	Opdrachtnemer organiseert tweewekelijks een vast overlegmoment met de contactpersoon van ROC Mondriaan. In dit overleg worden minimaal de volgende onderwerpen besproken: de voortgang van de lopende sprint, de inhoud en prioritering van de komende sprint(s), openstaande incidenten en wijzigingsverzoeken, en eventuele knelpunten of risico's. Opdrachtnemer stelt minimaal twee (2) werkdagen voor aanvang van het overleg een agenda op en deelt deze met ROC Mondriaan. Verslaglegging van het overleg vindt plaats binnen twee (2) werkdagen na het overleg en wordt gedeeld via het overeengekomen projectmanagementsysteem.

5 Commerciële eisen

Nummer	Eis
F 1	Opdrachtnemer garandeert dat gedurende de gehele looptijd aan Opdrachtgever geleverd wordt tegen marktconforme tarieven. Onder marktconform wordt verstaan wat voor de invulling van een bepaalde behoefte een gangbare prijs is die in de markt wordt aangeboden. U gaat ermee akkoord dat ROC Mondriaan een prijscontrole kan uitoefenen door bij derde partijen een offerte op te vragen om de marktconformiteit te toetsen. Indien uit andere offertes blijkt dat prijzen voor de in te kopen dienstverlening meer dan 5 % hoger zijn dan bij minimaal twee (2) andere aanbieders verkregen kan worden dan gaat Opdrachtnemer ermee akkoord dat – als deze niet instemt om ook voor dezelfde prijs te leveren – ROC Mondriaan gerechtigd is om de dienstverlening bij een derde af te nemen.
F 2	De door Opdrachtnemer aangeboden prijzen en tarieven voor onderhoud, beheer en doorontwikkeling websites dienen te zijn gesteld exclusief BTW en inclusief overige belastingen, heffingen, verzekeringen, parkeerkosten en/of overige verblijfskosten te zijn en alle overige denkbare kosten. De prijzen dienen gesteld te zijn in euro's. De door Opdrachtnemer opgegeven tarieven dienen all-in tarieven te zijn.
F 3	Overige kosten buiten de opgegeven tarieven om worden tijdens de contractduur niet geaccepteerd.

F 4	De opgegeven tarieven mogen éénmaal per jaar, per 1 januari, worden bijgesteld voor het eerst 1 januari 2028. De prijzen en tarieven worden geïndexeerd met een percentage te berekenen op basis van het Consumentenprijsindex (CPI) alle huishoudens, 2015=100, alle categorieën volgens de volgende prijsherziening formule: Prijs nieuw = Prijs oud * (L1/ L0) Prijs oud: Prijzen conform uw inschrijving Prijs nieuw: Nieuw overeen te komen prijzen L0: CPI, augustus 2026 * L1: CPI, augustus 2027 * Prijs nieuw wordt afgerond op 2 cijfers achter de komma. **: Het aangegeven jaar wordt gedurende de looptijd van de overeenkomst telkens met 1 verhoogd.* Ook in het geval van een negatieve indexering wordt de herziening van de tarieven doorgevoerd. *Indien Opdrachtnemer de prijzen wenst aan te passen aan deze indexering legt hij een schriftelijk voorstel met een onderbouwing minimaal 60 dagen tot uiterlijk 28 dagen voor het doorvoeren van de prijsverhoging voor aan ROC Mondriaan.* *Wanneer ROC Mondriaan vaststelt dat het voorstel overeenstemt met de hiervoor genoemde indexering, geeft zij schriftelijke goedkeuring voor de tariefaanpassing, zodat deze geldt voor de volgende contractperiode.* ***Ook als er géén indexering plaats vindt, moet dit schriftelijk kenbaar worden gemaakt minimaal 60 dagen tot uiterlijk 28 dagen van tevoren.***
F 5	Gepland onderhoud dat leidt tot downtime wordt minimaal 5 werkdagen van tevoren aangekondigd aan ROC Mondriaan en vindt uitsluitend plaats buiten kantooruren (maandag t/m vrijdag 08:00–18:00 uur), tenzij anders overeengekomen.

6 Administratieve Eisen

Nummer	Eis
G 1	Bij iedere opdracht krijgt de Opdrachtnemer een inkoopordernummer. Voor iedere inkooporder stuurt de Opdrachtnemer een aparte factuur waarop het inkoopordernummer vermeld moet staan.
G 2	Op de factuur vermeldt de Opdrachtnemer in ieder geval (voor zover van toepassing) de volgende zaken: o Factuuradres o Factuurnummer en datum o Kostenplaats o Afleveradres o Naam tekenbevoegde o Beschrijving van geleverde artikelen / abonnementen o Afzonderlijke bedragen, alsmede het totaalbedrag o Naam en het volledige adres van de leverancier en de afnemer o IBAN rekeningnummer

	o Het BTW percentage o Het BTW bedrag o BTW-nummer o KvK nummer Opdrachtnemer dient op de factuur een gedetailleerde specificatie van de uitgevoerde werkzaamheden op te nemen. Deze specificatie omvat minimaal: Per opdracht/project: Unieke opdrachtbenaming of projectnaam Inkooporder nummer Kostenplaats Per werkzaamheid/story binnen de opdracht: Duidelijke omschrijving van de uitgevoerde werkzaamheid/story (conform sprint-indeling indien van toepassing) Aantal bestede uren per werkzaamheid/story Uurtarief Subtotaal per werkzaamheid (uren × tarief) Totaaloverzicht: Totaal aantal uren per opdracht/project Totaalbedrag per opdracht/project Eindtotaal van de factuur Deze gedetailleerde specificatie stelt Opdrachtgever in staat om de gefactureerde werkzaamheden te relateren aan de overeengekomen opdrachten en kostenplaatsen, en om de voortgang en kosten per project transparant te bewaken. Facturen die niet voldoen aan deze specificatie-eisen worden geretourneerd conform eis [verwijzing naar bestaande eis over retourneren facturen] en dienen opnieuw te worden ingediend met aangepaste factuurdatum.
G 3	Facturen dienen als XML bestand met daaraan toegevoegd een PDF per e-mail gestuurd te worden naar: crediteuren.fc@rocmondriaan.nl
G 4	Voor aanvullende facturen en creditnota's gelden dezelfde voorschriften als voor facturen. Op creditnota's moeten bovendien de datum, het nummer en het eindbedrag worden vermeld van de factuur waarop de creditnota betrekking heeft.
G 5	U gaat ermee akkoord dat betaling door aanbestedende dienst plaatsvindt binnen 30 kalenderdagen na ontvangst van een juiste en op het juiste moment ingediende factuur.
G 6	Facturatie geschiedt per maand en vindt achteraf plaats, behalve als daarover andere afspraken zijn gemaakt.
G 7	Voor specifieke opdrachten of additionele diensten zal ROC Mondriaan een prijsopgave vragen.

	Deze prijsopgave dient te worden gebaseerd op de geoffreerde c.q. overeengekomen (uur)tarieven. ROC Mondriaan zal deze prijsopgave desgewenst toetsen op marktconformiteit en behoudt zich het recht voor de opdracht elders te verstrekken.
G 8	Indien de factuur niet in overeenstemming is met het bepaalde in eis G1 t/m G5 zal de Opdrachtgever deze factuur niet verder behandelen en retourneren aan Opdrachtnemer. Indien dit gebeurt, stuurt Opdrachtnemer een nieuwe factuur met aangepaste datum aan Opdrachtgever.