Continuïteit en beschikbaarheid
De continuïteit van de ICT-dienstverlening is gewaarborgd door het maken van heldere en concrete service level afspraken (SLA's) met de leverancier. Deze SLA's bevatten garanties ten aanzien van beschikbaarheid, herstel bij storingen en calamiteiten, en proactieve monitoring. De gemeente verlangt een planmatige en gecontroleerde transitie en migratie naar de nieuwe omgeving, met nadruk op het mitigeren van continuïteitsrisico's.

Daarnaast is in het Programma van Eisen opgenomen dat:
· Datacenters minimaal TIER-3 geclassificeerd dienen te zijn.
· Datareplicatie altijd versleuteld plaatsvindt (AES256 of vergelijkbaar).
· Er een exitstrategie beschikbaar is, inclusief export van alle data in een open formaat.
· Er periodieke externe beschikbaarheidstesten uitgevoerd kunnen worden.

Hiermee wordt de gemeente te allen tijde in staat gesteld haar dienstverlening aan burgers voort te zetten, ook bij verstoringen of overgang naar een andere leverancier.

Veiligheid en informatiebeveiliging
De veiligheid van de systemen wordt geborgd door een combinatie van technische, organisatorische en procedurele maatregelen:
· De leverancier moet aantoonbaar voldoen aan de eisen van de Baseline Informatiebeveiliging Overheid (BIO).
· Gegevensopslag en -verwerking vindt plaats binnen de Europese Economische Ruimte (EER) of in landen met een gelijkwaardig beschermingsniveau.
· Alle data-at-rest en data-in-transit is versleuteld (minimaal TLS 1.2 / AES256).
· Er is een rolgebaseerd autorisatiemodel (RBAC) voor toegangsbeheer.
· Auditlogging is verplicht, niet-muteerbaar en toegankelijk voor geautoriseerde personen binnen de gemeente.
· De leverancier dient een operationeel proces te hebben voor Coordinated Vulnerability Disclosure (CVD).
· Incidentrespons is strak georganiseerd: bij een datalek of security incident wordt de CISO van de gemeente onmiddellijk geïnformeerd, waarna gezamenlijk een actieplan wordt opgesteld.

Kwaliteits- en beveiligingscertificaten
De gemeente stelt expliciet eisen aan de aanwezigheid van erkende managementsystemen en certificeringen bij de leverancier:
· ISO 27001: verplicht voor informatiebeveiligingsmanagement; processen en procedures moeten aantoonbaar geborgd zijn.
· NEN 2082: verplicht bij de opslag en verwerking van zaakgerichte gegevens.
· GIBIT 2023: de gemeentelijke inkoopvoorwaarden ICT zijn van toepassing op de overeenkomst.
· Privacybeleid conform AVG/GDPR: de leverancier moet een aantoonbaar privacybeleid hanteren.
· Mogelijkheid tot onafhankelijke controle via een right to audit of een Third Party Memorandum (TPM).

Samenvatting
De continuïteit en veiligheid van de systemen bij de gemeente West Maas en Waal zijn gewaarborgd door een combinatie van contractuele SLA-afspraken, technische beveiligingsmaatregelen (encryptie, RBAC, auditlogs, TIER-3 datacenters), en internationale kwaliteitsstandaarden (ISO 27001, NEN 2082, BIO). Daarmee wordt zowel de beschikbaarheid als de compliance met wet- en regelgeving structureel geborgd.