

Bijlage 17: ICT-kwaliteitscriteria Gemeente Tilburg

EU-aanbesteding
Vervoercentrale Regio Midden-Brabant.



Datum: 1 mei 2024

Kenmerk: BRMB/AANB/REGIE/2024

Tendernummer: TN 462142

Versie: 5.0

In opdracht van:

Gemeente Tilburg, namens de Stuurgroep Regiovervoer Midden-Brabant.

Een IT-gerelateerde inkoop door een overheidsorganisatie zoals een gemeente is in sommige gevallen complex. Een gemeente is gebonden aan wetgeving en regels om te zorgen dat een gemeente een verantwoorde inkoop doet. Denk aan aanbestedingsregels, informatiebescherming, privacy en cybersecurity. Deze aspecten worden met de dag belangrijker in de zo veranderlijke wereld.

Dit is natuurlijk belangrijk om te waarborgen: aan de andere kant kan dit soms zorgen voor een langdurig en complex inkoopproces.

Om dit proces zo goed en efficiënt mogelijk te laten verlopen heeft onze organisatie geprobeerd om de informatie die wij binnen dit traject vragen en verstrekken in dit document samengevat.

Op deze manier willen wij zorgen dat beide partijen inzicht hebben in de stappen die genomen moeten worden en vooral ook waarom deze genomen moeten worden bij het aankopen van het product of dienst.

Op de volgende pagina's vindt u de stappen en bijbehorende documenten die wij voor dit specifieke inkoopproces nodig hebben om tot een verantwoorde aankoop te komen.

Bij iedere stap vindt u terug waarom deze stap nodig is en wat wij aan informatie van u vragen en welke actie vanuit ons kunt verwachten en wat wij vanuit de leverancier verwachten.

Daarnaast worden eventueel benodigde documenten toegevoegd aan dit document.

Mocht u naar aanleiding van dit document nog vragen of opmerkingen hebben dan horen wij dit uiteraard graag van u.

Inhoudsopgave

1.	DIGITALE TOEGANKELIJKHEID.....	4
2.	ARCHIVERINGSEISEN	5
3.	CYBERSECURITY	6

1. DIGITALE TOEGANKELIJKHEID

4. Digitale toegankelijkheid	
Achtergrondinformatie (wat en waarom) Vanuit de wet voor digitale toegankelijkheid worden overheidsinstanties verplicht om hun websites en apps toegankelijk te maken en te houden. Dit moet ervoor zorgen dat ieder mensen, ongeacht de belemmeringen, mee kunnen doen in de digitale wereld en daarmee dus ook in de samenleving. Daarom is het belangrijk dat websites en apps toegankelijk zijn. Want als dat zo is, kan écht iedereen ze gebruiken.	
Wanneer van toepassing	De wet geldt voor alle webtoepassingen (alles met http(s), websites, webapplicaties en apps) van de overheid. Het gaat hierbij ook over webtoepassingen waarvan de overheid gebruik maakt in haar dienstverlening naar inwoners, ondernemers, recreanten en eigen medewerkers Daar vallen ook intranetten, extranetten en cloudapplicaties onder. Ook alle mobiele applicaties vallen onder de wet. Dat zijn dus zowel native, web- als hybride apps voor mobiele apparaten.
Benodigde informatie	Bevestiging d.m.v. de verklaring en de rapportage van de toets dat de betreffende webtoepassing voldoende digitoegankelijk is volgens de richtlijnen die door het besluit 'Digitale toegankelijkheid overheid' voorgeschreven wordt. Wanneer een webtoepassing nog niet volledig toegankelijk is graag een roadmap toevoegen aan welke onderdelen de komende periode gewerkt wordt om toegankelijker te worden.
Actie Tilburg	Uitvoeren van de digi-toegankelijke toets met bijbehorend rapportage.
Actie Leverancier	Aanleveren rapportage rondom toegankelijkheid in de WCAG-EM standaard.
Document	N.v.t.

2. ARCHIVERINGSEISEN

Archiveringseisen	
Achtergrondinformatie (wat en waarom) Iedere gemeente heeft een archief. Hiervoor geldt de Archiefwet. Deze wet schrijft voor dat de overheid haar informatie op een goede manier bewaart. Dat is van belang voor de bedrijfsvoering van de overheid zelf, maar ook voor publieke verantwoording, rechtsvinding en vanuit cultuur-historisch perspectief. Voor websites van de gemeente is de archiefwet ook van toepassing. Een website die wordt gelanceerd dient ook gearchiveerd en vervolgens publiekelijk ontsloten te worden zodat deze archieven kunnen worden gebruikt als bewijsvoering dat iets wel/niet op een bepaald moment online heeft gestaan. Op basis van de richtlijnen van deze wet is een gemeente verplicht om zorg te dragen dat een toepassing archiefwaardig is. Archiefwaardig betekent dat er in de software een archiefmodule of -optie aanwezig is.	
Wanneer van toepassing	Dit is altijd van toepassing als er gegevens verwerkt en opgeslagen worden.
Benodigde informatie	Duidelijkheid rondom de vragen, eisen en wensen die gesteld worden in bijlage A.
Actie Tilburg	Bijlage A wordt beschikbaar gesteld aan de leverancier.
Actie Leverancier	Bijlage A invullen en ondertekend retourneren aan de gemeente.
Document	Zie bijlage 'A bij opdrachtdocument ICT kwaliteitscriteria'

3. CYBERSECURITY

Advies Cybersecurity	
Achtergrondinformatie (wat en waarom) Een overheidsorganisatie is verplicht om aan wettelijke eisen te voldoen m.b.t. cyber security. (<i>Wet beveiliging netwerk- en informatiesystemen</i>). In het beleid van de gemeente Tilburg is vastgelegd dat onze leveranciers aan dezelfde eisen moet voldoen. Er worden technische controles uitgevoerd m.b.t. cybersecurity. Dit komt erop neer dat de toetsen die gedaan worden gericht zijn op het risico in welke mate er wel of niet 'binnengedrongen' kan worden in de webtoepassing die evt. aangeschaft gaat worden. Concreet houdt dit in dat er getoetst wordt of de webtoepassing voldoet aan de wettelijke eisen en richtlijnen die opgesteld zijn door Nationaal Cyber Security centrum (NCSC) en Informatiebeveiligingsdienst (IBD).	
Wanneer van toepassing	Alleen als het een webtoepassing betreft (alles met http, intranet, extranet, websites, webapplic. en apps).
Benodigde informatie	• Relevante linken beschikbaar stellen die gecontroleerd moeten worden • Representatieve link: voor live gang ook de productie URL aanleveren t.b.v. de controles.
Actie Tilburg	Afhankelijk van de situatie: • Testen van de beschikbaar gestelde link op mogelijkheid tot ongewenst binnendringen van de toepassing en terugkoppeling bevindingen d.m.v. rapportage. • Pentest (laten) uitvoeren (vrijwaring opvragen bij leverancier)
Actie Leverancier	• Beschikbaar stellen van de link die gecontroleerd moet worden en aanpassen van de issues die gevonden worden. Afhankelijk van de situatie: • Aanleveren recente onafhankelijke pentestrapportage • Op verzoek vrijwaring t.b.v. pentest ondertekend retourneren.
Document	Zie bijlage 'A bij opdrachtdocument ICT kwaliteitscriteria'