Vertrouwelijk

GEMEENTE TILBURG

Cloud Computing

Eisen en Wensen InformatieBeveiliging

v1.71

Cloud Computing Eisen en Wensen InformatieBeveiliging

Cloud Computing Eisen en Wensen InformatieBeveiliging

Versiebeheer

Versie	Datum	Auteur	Status/Wijzigingen
1.50	7/6/16	Marius van Oers	Vastgesteld tijdens het I-managers overleg van de afdeling POI (huidig DAT).
1.51	16/1/17	Marius van Oers	Actualisatie web richtlijnen
1.52	18/7/17	Marius van Oers	Safe Harbor→EU/VS Privacy Shield. TLS/DKIM/DMARC/DANE beveiligingsopties. IBD en NCSC beveiligingsrichtlijnen.
1.53	09/08/18	Marius van Oers	Actualisatie web richtlijnen
1.54	22/08/18	Marius van Oers	TLS vereisten per IBD/NCSC richtlijnen.
1.55	06/02/19	Marius van Oers	WBP→AVG/GDPR
1.56	17/07/19	Marius van Oers	Remote sessie & BIG→BIG/BIO
1.57	24/7/19	Marius van Oers	NCSC Beveiligingsrichtlijnen Webapplicaties
1.58	15/8/19	Marius van Oers	Actualisatie en verwijdering van niet relevante items.
1.59	3/10/19	Marius van Oers	Sync geheimhouding en verwerkersovereenkomst
1.60	6/2/20	Marius van Oers	Actualisatie, Weblinks , SSLLABS
1.61	3/6/20	Marius van Oers	Actualisatie, eisen overgenomen uit B5 meetings.
1.62	3/6/20	Marius van Oers	Flowchart, Full & Mini eisen
1.63	4/6/20	Marius van Oers	Opmerkingen Terence
1.64	8/6/20	Terence van Gestel	Opmerkingen Perry
1.65	21/7/20	Marius van Oers	EU/VS Privacy Shield →SCC
1.66	8/10/20	Marius van Oers	Verduidelijking flowchart
1.67	4/11/21	Marius van Oers	Tilburgse technische veiligheids en inrichtingseisen voor webtoepassingen.
1.68	1/12/21	Marius van Oers	Port forwarding
1.69	23/6/22	Marius van Oers	Web Expertise Team
1.70	10/11/22	Marius van Oers	MS Graph protocol
1.71	28/2/23	Marius van Oers	API Gateway

Cloud Computing Eisen en Wensen InformatieBeveiliging

1.0 - Cloud Computing Eisen en Wensen InformatieBeveiliging

Definitie Cloud Computing: we spreken van Cloud computing als toepassingen ter beschikking worden gesteld door gebruik van internettechnologie.

Cloud Computing raakt alle maatregelen die de gemeente Tilburg zelf moeten nemen in de eigen infrastructuur. Deze maatregelen worden vervolgens gedeeld door de Cloud- leverancier en door de gemeente Tilburg uitgevoerd.

Indien de gemeente Tilburg gebruikt maakt van Cloud-diensten dan blijft de gemeente Tilburg verantwoordelijk voor de juiste beveiliging van haar gegevens.

1.1 Inleiding

Dit document is bedoeld om tijdens trajecten richting Cloud partijen/contractanten (ten behoeve van bijvoorbeeld SAAS, PAAS, IAAS oplossingen etc.) van de gemeente Tilburg Eisen en Wensen m.b.t. Informatiebeveiliging te communiceren.

De antwoorden worden gebruikt om de bestaande beveiligingssituatie te beoordelen en of deze voldoet aan de voor gemeente Tilburg geldende compliancy mbt informatiebeveiliging.

Het beantwoorden van alle vragen en het geven van toelichtingen is verplicht.

Het daadwerkelijk voldoen aan de Eisen is verplicht.
Sommige van de onderstaande eisen zijn afkomstig uit het IBD (Informatie Beveiligingsdienst voor gemeenten) document m.b.t. Cloud Computing.
De eisen zijn realistisch en haalbaar.
Indien er aan een of meerdere eisen niet wordt voldaan dan kan dat gelden als knock-out criteria.
Dit is een algemeen document. Het kan daardoor voorkomen dat een bepaalde eis niet van toepassing is. Geef dit aan met argumentatie.

Aan een eis moet men voldoen, aan een wens mag men voldoen.
Bij de wensen ligt de lat iets hoger dan bij de eisen en kunnen partijen het verschil maken indien zij aantoonbaar kunnen laten zien dat ze aan bepaalde wensen voldoen.
Voor elke niet behaalde wens wordt er 0 punt toegekend.
Voor een behaalde wens worden er de specifiek bepaalde punten toegekend.

De scores geven inzicht in mate van beveiliging en kunnen onder andere dienen als basis voor een objectieve selectie van leveranciers m.b.t. Informatiebeveiligingsaspecten.

2.0 Algemene zakelijke informatie van de Contractant

- Leverancier:
- Product/dienst naam:
- Korte functionele beschrijving van de dienst:
- Contactpersoon:
  Adres:
  Telefoon:
  E-mail:
- Websites/weblinks die mogelijk gebruikt gaan worden. Waar loggen eindgebruikers en beheerders op in. En indien er koppelingen worden gelegd ten behoeve van system/service accounts/api koppelingen etc geef deze ook aan.

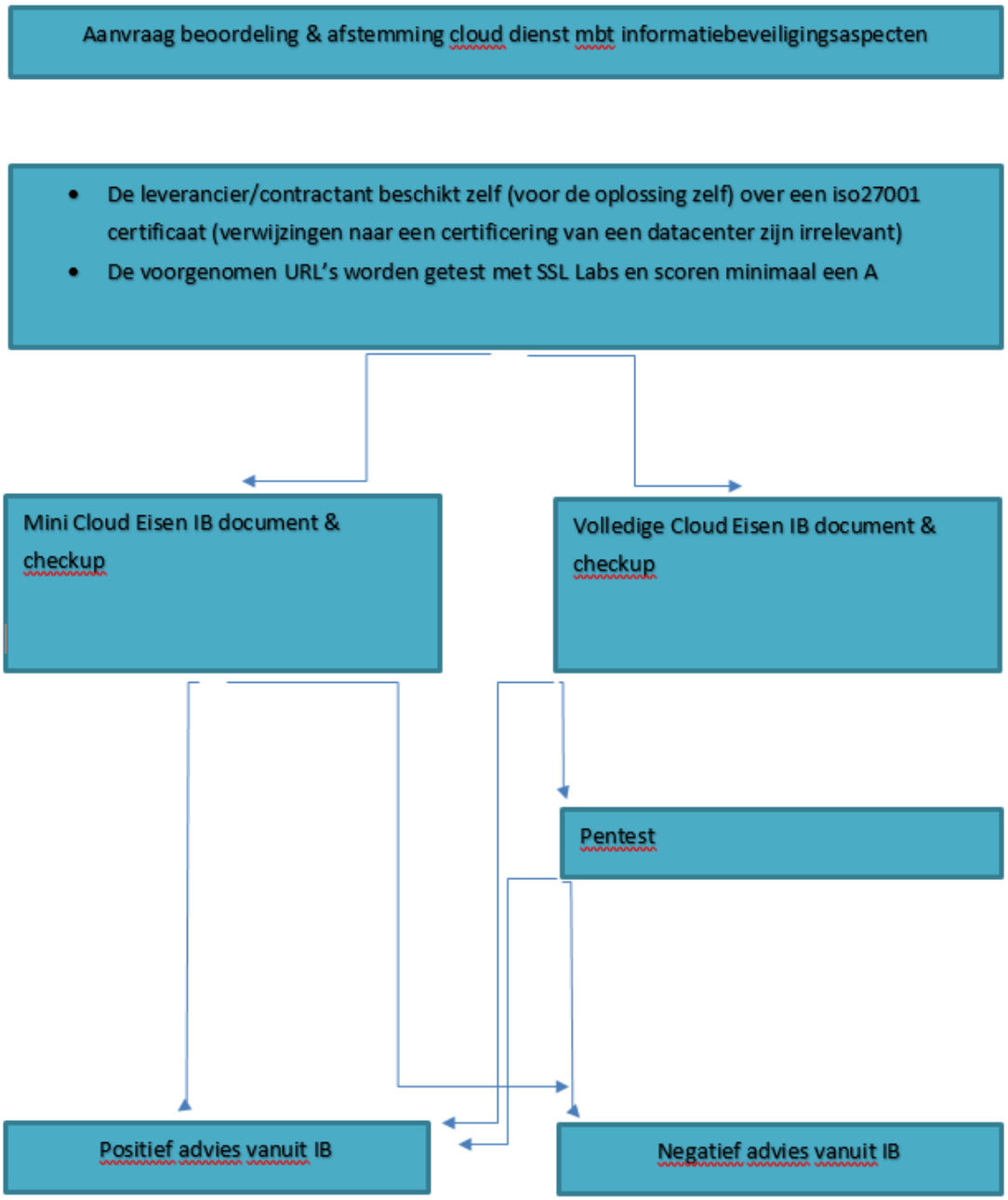
    1. Weblink voor Eindgebruikers :
    2. Weblink voor Beheerders :
    3. Weblink voor System/Service accounts/api koppelingen etc :

- Heeft uw organisatie een ISO 27001/27002 verklaring van uw informatiebeveiliging?
  De onafhankelijk auditor dient te verklaren dat het systeem en de achterliggende processen voldoen. De verklaring dient te zijn verstrekt door een derde partij die zich houdt aan de norm voor auditors (in NL: Norea). De verklaring dient recent te zijn en is maximaal 2 jaar oud. Indien ja, dan ontvangen we graag een kopie hiervan.

2.1 Flowchart

Standaard worden de volledige eisen gesteld aan de Contractant (C – Full)
Als een leverancier zelf beschikt over een iso27001 certificaat en de voorgenomen url's een A score hebben op ssllabs dan hanteren we de mini eisen. (C-Mini)

We hanteren de volgende flowchart:



2.2 Eisen voor de Contractant

Om onderscheid te maken tussen eisen voor de contractant en interne (gemeente Tilburg) instructies zijn er kolommen toegevoegd:
C: Contractant (cloud leverancier)
T: gemeente Tilburg

Standaard worden de volledige eisen gesteld aan de Contractant (C – Full)
Als een leverancier zelf beschikt over een iso27001 certificaat en de voorgenomen url's een A score hebben op ssllabs dan hanteren we de mini eisen. (C-Mini)

	C Full	C Mini	T	Antwoord/toelichting door de contractant dat zij zich committeren aan de eis en voorzien van onderbouwing.
1. Gemeente Tilburg heeft het recht om audits te mogen (laten) uitvoeren over alle afspraken.	X	X	X	
2. De contractant/ hoofdaannemer moet ervoor zorgen dat eventuele onderaannemer(s) dezelfde waarborgen biedt bij de uitvoering van de overeenkomst als de hoofdaannemer. Rechten en plichten blijven bij de hoofdaannemer. Onderaannemer werkt uitsluitend onder verantwoordelijkheid van hoofdaannemer. Dit is ook op datahosting (via een andere partij) van toepassing	X	X		
3. Opdrachtnemer is gehouden tot geheimhouding van alle gegevens die zij verwerkt.	X	X		
4. Naleving van alle relevante wet- en regelgeving is verplicht.	X	X	X	

5. Autorisaties dienen transparant te zijn, er dient in 1 overzicht een duidelijke autorisatietabel met rollen/functies en bijbehorende rechten te zijn. Role Based Acces Control dient ingericht te zijn. ("RBAC") Autorisaties zijn ingericht op basis van "need to know" : alleen personen die informatie nodig hebben voor het uitvoeren van hun werkzaamheden hebben toegang. Rechten dienen te worden toegekend volgens het "Least Priviliges" principe.	X	X	X	
6. Er dient strikte functiescheiding te zijn. Bijvoorbeeld voor een persoon die zowel een reguliere gebruiker is als beheerder. Beheer en Functioneel gebruik dient gescheiden te zijn.	X	X	X	
7. Er zijn maatregelen ingevoerd om de dreiging tegen te gaan dat informatie wordt misbruikt door uw personeel en (onder)aannemers. Bijvoorbeeld het ongeoorloofd inzien van diensten en gegevens dient voorkomen te worden.	X			
8. Er zijn maatregelen ingevoerd om het ten onrechte verstrekken van informatie aan onbevoegden te voorkomen.	X			

9. Met betrekking tot remote sessies: Het gebruik van RDP (remote desktop protocol) is niet toegestaan tenzij dit - bij uitzondering - niet anders kan en deze aantoonbaar sterk beveiligd is met bijvoorbeeld TLS beveiliging in combinatie met een RDS Gateway of een VPN/SSH tunnel. Publieke port forwarding is niet toegestaan. Diensten dienen binnen een beveiligde omgeving te worden aangeboden. Eventuele koppelingen dienen enkel via veilige verbindingen te verlopen. Directe koppelingen met lokale hardware tijdens remote sessies zijn niet toegestaan, als voorbeeld geen lokale usb support tijdens een remote sessie. Afstemming en goedkeuring hieromtrent dient vooraf plaats te vinden met CISO/ISO en Architectuur en Technisch Beheer van de Gemeente Tilburg.	X	X	X	
10. Er is een informatiebeveiliging risico analyse uitgevoerd met opvolging van te nemen maatregelen uit deze analyse.	X	X	X	
11. Er zijn maatregelen getroffen om de dreiging van hack/inbreuk of kwaadaardige software aan te pakken.	X			

12. Hardening van systeem en proces is ingericht en toegepast (bijvoorbeeld uitschakelen van ongebruikte services en poorten).	*X*			
13. De contractant hanteert een actief patchmanagementbeleid waarbij kritische/hoog risico kwetsbaarheden binnen een week (deze termijn is in lijn met de IBD/NCSC richtlijn) worden opgelost.	*X*	*X*		
14. *Indien in overleg de contractant e-mail mag versturen namens gemeente Tilburg moet dit afgestemd worden met* een tactisch IT adviseur. Met betrekking tot techniek wordt gestuurd richting het gebruik van e-mail sub domeinen (bijvoorbeeld factuur@extern.tilburg.nl).	*X*	*X*	*X*	
15. De contractant past actuele beveiligingsopties toe, zoals aangegeven door de IBD en NCSC. Zo dienen de in sectie (2.0 Algemene zakelijke informatie van de Contractant) opgegeven weblinks goed (“groen”) te scoren op **https://www.internet.nl/** De eisen staan uitgewerkt in de bijlage van het beleid websites. **Servicepunt - Beleid websites** Let op dit is een interne link en niet extern benaderbaar. De afstemming hieromtrent gebeurt door de aanvragende partij, de desbetreffende business unit van gemeente Tilburg, welke contact zoekt met het expertiseteam websites, dit kan onder andere via het e-mail adres: **websites@tilburg.nl**	X	X	X	

16. De in sectie (2.0 Algemene zakelijke informatie van de Contractant) opgegeven weblinks scoren minimaal een A rating op ssllabs.com. **https://www.ssllabs.com/ssltest/** De afstemming hieromtrent gebeurt door de aanvragende partij, de desbetreffende business unit van gemeente Tilburg, welke contact zoekt met het expertiseteam websites, dit kan onder andere via het e-mail adres: **websites@tilburg.nl**	X	X	X	
17. De in sectie (2.0 Algemene zakelijke informatie van de Contractant) opgegeven weblinks voldoen aan de Tilburgse beleidsregels voor websites, met name de "veiligheids en inrichtingseisen webtoepassingen." De eisen staan uitgewerkt in de bijlage van het beleid websites. **Servicepunt - Beleid websites** Let op dit is een interne link en niet extern benaderbaar. De afstemming hieromtrent gebeurt door de aanvragende partij, de desbetreffende business unit van gemeente Tilburg, welke contact zoekt met het expertiseteam websites, dit kan onder andere via het e-mail adres: **websites@tilburg.nl**	X	X	X	

18. De contractant heeft aantoonbaar maatregelen ingevoerd om de kans dat informatie kan worden onderschept tijdens transport/overdracht door onbevoegden te minimaliseren.	X			
19. De contractant volgt en voldoet aan de actuele beveiligingsrichtlijnen van de IBD en NCSC. **https://www.informatiebeveiligingsdienst.nl/** **https://www.ncsc.nl/**	X	X		
20. Indien de gemeente Tilburg het nodig acht dient het gebruik van Certificaten ondersteund te worden.	X	X		
21. De informatievoorziening (gegevens) van gemeente Tilburg dient logisch gescheiden te zijn van andere partijen.	X	X		
22. Data classificatie van gemeente Tilburg onderscheidt 4 niveaus: publieke, interne, vertrouwelijke en geheime data. Bij vertrouwelijke data is data encryptie sterk aanbevolen. Bij geheime data zijn zowel multi-factor authenticatie voor toegang als data encryptie verplicht.	*X*	*X*	*X*	

23. Vooraf dienen de eisen m.b.t. beschikbaarheid, integriteit en vertrouwelijkheid (BIV) helder te zijn doorgegeven aan de leverancier/contractant zodat passende maatregelen en serviceniveaus kunnen worden afgesproken (in contract/sla), ingericht en bewaakt.			X	
24. Back-up en uitwijk voorzieningen, Continuïteit van het systeem. De contractant heeft aantoonbaar maatregelen getroffen om in het geval van een incident of calamiteit de afgesproken informatievoorziening binnen de afgesproken termijn weer operationeel te hebben. Gemeente Tilburg is verantwoordelijk voor het aangeven van deze termijn op basis van onze business continuïty documentatie.	X	X	X	
25. De Tilburgse voordeur dient gebruikt te worden voor identificatie/authenticatie. *Single sign on dient ondersteund te worden, ter voorkoming van een wildgroei van username/password combinaties.* *Momenteel via Microsoft ADFS en/of Microsoft AzureAD.*	X	X	X	
26. De contractant heeft aantoonbaar maatregelen ingevoerd ten behoeve van sterke user authenticatie voor toegang tot de data. U overlegt een beschrijving van de wijze van user authenticatie voor toegang tot data.	X			
27. Multi factor authenticatie (MFA) dient ondersteunt te worden. Voorkeur voor Microsoft Authenticator.	X	X	X	

28. Het is mogelijk om de toegang tot de applicatie te beperken tot IP-adressen van het netwerk van de gemeente Tilburg indien MFA niet mogelijk is.	X	X		
29. Het wachtwoordbeleid van de gemeente Tilburg dient opgevolgd te worden.	X	X	X	
30. Generieke accounts dienen zo veel mogelijk beperkt te worden. Uitgangspunt is gebruik van persoonlijke accounts.	X	X	X	
31. Wachtwoorden dienen veilig opgeslagen te worden. Geef in de toelichting aan welke waarborgen genomen zijn voor het veilig opslaan van wachtwoorden	X	X	X	
32. De samenwerking met ketenpartners wordt belangrijker. Het uitwisselen van informatie (bestanden) en toegang tot data-bronnen (via API's) dient juist ingeregeld te zijn. Voor vertrouwelijke informatie is encryptie van data in ruste optioneel. Voor geheime data is encryptie van data in ruste verplicht.	X	X	X	
33. De cloud provider is verplicht hoog risico beveiligings incidenten binnen een dag te melden aan de gemeente Tilburg.	X	X	X	
34. De cloud provider is verplicht zo spoedig mogelijk beveiligingsincidenten op te lossen, doch maximaal binnen 1 week.	X	X		

35. De gemeente Tilburg heeft het recht om logging gegevens op te vragen en in te zien. Indien gemeente Tilburg gebruik maakt van een centrale log infrastructuur (zoals bijvoorbeeld met SIEM oplossingen) dan dient de logging van de contractant - waar mogelijk - aan te sluiten op de centrale logging van de gemeente Tilburg.	X	X	X	
36. De externe informatievoorziening is ondergebracht binnen de EER (Europese Economische Ruimte)	X	X		
37. Indien er gebruik wordt gemaakt van Microsoft Azure Kubernetes/K8s dan dient de leverancier de Microsoft Azure Security Baseline for Azure Kubernetes Service te volgen en hieraan aantoonbaar te voldoen. **Azure security baseline for Azure Kubernetes Service | Microsoft Learn**	X	X		

38. U geeft grafisch (.jpg), schematisch, technisch en volledig aan op welke wijze verbindingen zijn dan wel worden gemaakt tussen de gemeente Tilburg Infrastructuur en de aangeboden(cloud) omgeving. Een eventueel extern datacenter is schematisch ook weergegeven. Dit omvat onder andere: • Type verbindingen; • Wijze van toegang; • Serverbenamingen/IP nummers; • Encryptie methoden (bijv. TLS, Clientcertificaten); • Wijze van endpoint beveiliging (bijv. OAuth 2.0 voor API's) • Netwerkpoorten voor verkeer; Encryptie techniek voor dataopslag;	X	X		
39. Iedere API wordt ontsloten via het integratieplatform van de Gemeente Tilburg. De API Gateway is hiervoor het verplichte functionele bouwblok. De API Gateway biedt onder andere de volgende functies: • Toegangscontrole • Throttling • Logging	x	x	x	
40. In principe kan er geen sprake zijn van direct cloud-cloud verkeer zonder tussenkomst van de gemeente Tilburg. In het geval hier wel sprake van is dan aangeven welke verkeerstromen dit zijn en wat voor data dit betreft. Verdere afstemming is nodig met een Tactisch IT adviseur alsmede een Architect.	x	x	x	

41. Data ontsluiting van M365 en overige data door applicaties van de contractant dient via het Microsoft GRAPH protocol plaats te vinden en niet via het oude EWS (Exchange Web Services) protocol. Ook hier geldt: gebruik van moderne identificatie en authenticatie methoden, role based access, least privileges.	x	x	x	

2.3Wensen voor de Contractant

42. Heeft uw organisatie een ISAE3402 (SOC1) verklaring van uw informatiebeveiliging?
    De onafhankelijk auditor dient te verklaren dat het systeem en de achterliggende processen voldoen. De verklaring dient te zijn verstrekt door een derde partij die zich houdt aan de norm voor auditors (NL:Norea). De verklaring dient recent te zijn en is maximaal 2 jaar oud. Indien ja, dan ontvangen we graag een kopie hiervan. (+10 punten)

43. Heeft uw organisatie een ISO 27001/27002 verklaring van uw informatiebeveiliging?
    De onafhankelijk auditor dient te verklaren dat het systeem en de achterliggende processen voldoen. De verklaring dient te zijn verstrekt door een derde partij die zich houdt aan de norm voor auditors (NL:Norea). De verklaring dient recent te zijn en is maximaal 2 jaar oud. Indien ja, dan ontvangen we graag een kopie hiervan. (+7 punten)

44. Laat uw organisatie met regelmaat (jaarlijks/om de 2 jaar) penetratietest(s) en/of vulnerability scan(s) uitvoeren op de infrastructuur – waarbij de aangeboden dienstverlening aantoonbaar in scope is - door een onafhankelijke (met gecertificeerde ethical hackers etc) partij? Indien ja, dan ontvangen we graag een kopie van het meest recente rapport wat minimaal een management samenvatting bevat met bevindingen geclassificeerd in risico's. Dit aangevuld door de leverancier mbt de aangegeven huidige status van de geconstateerde bevindingen en oplossingstermijnen. (+4 punten)

45. Heeft het datacenter een ISO 27001 verklaring van uw informatiebeveiliging?
    De verklaring dient te zijn verstrekt door een derde partij die zich houdt aan de norm voor auditors (NL:Norea). De verklaring dient recent te zijn en is maximaal 2 jaar oud.
    Indien ja, dan ontvangen we graag een kopie hiervan. (+2 punten)

Ter referentie:

- Een SOC 2 verklaring geeft in het algemeen meer zekerheid over de werking van controls en de ISO27001 over het managementsysteem van informatiebeveiliging
- ISAE3000
- SOC2/SOC3
- ISO 27017 is een internationale norm voor cloudbeveiliging
- ISO 27018 is een internationale norm voor privacy- en gegevensbescherming toegespitst op leveranciers van clouddiensten die persoonlijke gegevens namens hun klanten verwerken.