EISEN & WENSEN mbt INFORMATIEBEVEILIGING & PRIVACY

In dit document zijn meerdere tabbladen opgenomen.
Hieronder staat een toelichting hoe de tabbladen geïnterpreteerd moeten worden.

Generieke maatregelen

Op dit tabblad zijn de maatregelen opgenomen die door Opdrachtgever altijd gesteld worden aan een oplossing ongeacht het beveiligingsniveau. Deze zijn dus op alle onderdelen die vallen onder de raamovereenkomst van toepassing.

Aanvullende maatregelen

Op dit tabblad zijn maatregelen opgenomen die door Opdrachtgever gesteld worden, afhankelijk van door Opdrachtgever vastgesteld beveiligingsniveau voor de oplossing. Het beveiligingsniveau is opgebouwd uit drie elementen, namelijk Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV). De niveau's kunnen per element verschillen.

Voor de meeste IT-prestaties/applicatie(onderdelen) die geleverd worden binnen de raamovereenkomst is het volgende niveau bepaald:
Beschikbaarheid: 2
Integriteit: 2
Vertrouwelijkheid: 2
Voor deze IT-prestaties/applicaties zijn alle maatregelen van toepassing vanuit tabblad Aanvullende Maatregelen Nivo 2.

Voor **iBurgerzaken** is een hoger niveau op het element Beschikbaarheid benodigd en komt daarmee op het volgende beveiligingsniveau:
Beschikbaarheid: 3
Integriteit: 2
Vertrouwelijkheid: 2
Voor iBurgerzaken betekent dit dat alle maatregelen van toepassing zijn vanuit tabblad Aanvullende Maatregelen Nivo 3.

Wensen

Dit zijn de maatregelen die gewenst zijn en daarbij wordt dezelfde definitie van een wens gehanteerd als in andere aanbestedingstrajecten.

Webcheck (technisch)

De webcheck is een verbijzonderde checklist vanuit het webbeleid (separaat toegestuurd).
Dit zijn specifieke maatregelen die van toepassing zijn wanneer er sprake is van een website, webapplicatie of portaal.
In dit tabblad is te zien waar Opdrachtgever technische tests op uitvoert en met welk instrument.

Webcheck (overig)

De webcheck is een verbijzonderde checklist vanuit het webbeleid (separaat toegestuurd).
Dit zijn specifieke maatregelen die van toepassing zijn wanneer er sprake is van een website, webapplicatie of portaal.
In dit tabblad staan de overige eisen/aanbevelingen die gesteld worden.
In dit tabblad dient Leverancier tevens een antwoord te geven hoe invulling wordt gegeven aan een eis/aanbeveling.

Generieke Maatregelen

Deze maatregelen zijn aanvullend op de GIBIT-voorwaarden.

A	Eisen met betrekking tot de organisatie van informatiebeveiliging	Akkoord leverancier & toelichting	Reactie SWO
A1	Leverancier stelt de Opdrachtgever in staat te voldoen aan: • De (U)AVG; • De Baseline Informatiebeveiliging Overheid; • De beveiligingsrichtlijnen voor Apps van het NCSC; • Archiefwet 1995, Archiefbesluit 1995; • Het Algemeen en Technisch Informatiebeveiligingsbeleid van Opdrachtgever		
A2	Leverancier evalueert regelmatig, minimaal jaarlijks, of de getroffen beveiligingsmaatregelen door Leverancier nog passend zijn voor de beveiliging en passen zo nodig de maatregelen aan.		
B	**sen met betrekking tot de security van de applicatie, database, operating syste**	**Akkoord leverancier & toelichting**	**Reactie SWO**
B1	Leverancier past passende technische beveiligingsmaatregelen toe die relevant zijn voor de dienstverlening aan Opdrachtgever. Dit omvat maatregelen die in lijn zijn met internationaal erkende standaarden en praktijken om de integriteit, beschikbaarheid en vertrouwelijkheid van systemen en data te waarborgen. Voorbeelden van dergelijke maatregelen kunnen, maar zijn niet beperkt tot, het hardenen van systemen volgens internationale richtlijnen zoals CIS, waarbij overbodige functies worden verwijderd of uitgeschakeld, en het periodiek toetsen van de hardeningsrichtlijnen van IT-componenten in productie. Andere maatregelen kunnen onder meer intrusion detection en prevention, anti-malware en antivirusoplossingen met regelmatige updates, vulnerability scanning en management, effectief firewall management, security patching, netwerksegmentering, en robuust logging en log management omvatten. Indien Leverancier niet voldoet aan deze specifieke maatregelen, wordt verwacht dat zij een toelichting geven over hoe zij op een vergelijkbare wijze risicomitigatie toepassen.		
B2	Indien relevant voor de toepassing van de oplossing zijn de volgende **open standaarden** van het Forum Standaardisatie geïmplementeerd door Leverancier: • DKIM, DMARC, DNSSEC, HTTPS en HSTS, IPv6, SAML, SPF, STARTTLS, DANE, STIX en TAXII, TLS en WPA2. https://www.forumstandaardisatie.nl/open-standaarden/verplicht		
B4	Leverancier zorgt voor adequate (logische) scheiding tussen verwerkingen voor verschillende klanten van Leverancier (isolatie van gegevensverwerkingen) zodat het risico op ongeautoriseerde toegang tot data van Opdrachtgever wordt voorkomen.		
B5	Leverancier is ervoor verantwoordelijk dat gegevens die opgeslagen en/of uitgewisseld worden en de daarvoor ingezette verbindingen afdoende beveiligd zijn, o.a. door encryptie (minimaal AES256), certificaten (met minimaal validatie van aanvrager), VPN of een combinatie hiervan.		
B9	Leverancier past secure by design principes toe bij ontwikkeling van diensten en applicaties, waaronder secure software development in geval van een dienst op afstand. Hierbij wordt gebruik gemaakt van industrie-standaarden voor veilige software (ontwikkeling) zoals OWASP, CIP (NL) en NCSC (NL).		
B10	Leverancier voorkomt dat er ongeautoriseerde wijzigingen in de code gedaan kunnen worden en dat rechten voor het wijzigen van code, uitvoeren van pipelines en het installeren van nieuwe versie is voorbehouden aan geautoriseerde medewerkers.		
B11	Leverancier implementeert adequaat logging, waarbij alle activiteiten en gebeurtenissen die de beveiliging en integriteit van gegevens beïnvloeden worden gelogd en bewaard, conform beleid van Opdrachtgever. Leverancier zorgt dat er passende maatregelen worden getroffen waarmee persoonsgegevens die in dergelijke logbestanden verschijnen, voldoende worden beschermd en niet voor andere doeleinden worden gebruikt.		
B12	Leverancier beheerst kwetsbaarheden. Dit betekent het volgende: i Leverancier hanteert patch management proces. ii Leverancier schat geïdentificeerde kwetsbaarheden in volgens de Common Vulnerability Scoring System (CVSS). iii Leverancier zal kwetsbaarheden oplossen volgens onderstaande maximale oplostijden (vanaf het moment dat patches beschikbaar zijn): CVSS Risico Maximale oplostijd 9 - 10 Kritiek 24 uur 7 – 8.9 Hoog 1 weken 4 – 6.9 Midden 2 weken 0 – 3.9 Laag eerst volgende onderhoudsronde iv Bij alle risico's van hoger en kritiek dient leverancier Opdrachtgever onverwijld te informeren van het bestaan van een kwetsbaarheid met een risico voor Opdrachtgever. v Deze waarschuwing dient voorzien te zijn van een inschatting van het risico wat Opdrachtgever loopt, de verwachtte oplostijd en welke stappen Opdrachtgever zelf kan nemen om risico's te mitigeren.		
B13	Leverancier test software en firmware updates voorafgaand aan installatie volgens vastgestelde (test)procedures als onderdeel van patchmanagement, releasemanagement en/of lifecycle management.		
B14	Indien van toepassing worden e-mailberichten veilig verstuurd Indien de oplossing communiceert met eindgebruikers via e-mail dient de mail afkomstig te zijn van een mailadres waarvan het top-level domein toebehoort aan een domein waar Opdrachtgever juridisch verantwoordelijk voor is. In dit geval verstuurt de oplossing mails naar eindgebruikers middels geauthentiseerde SMTP via de infrastructuur van Opdrachtgever, OF Opdrachtgever zal via SPF records Opdrachtnemer machtigen om namens een specifiek sub-domein te mailen. In geval dat mailservers van Opdrachtgever gebruikt worden voldoen die aan geldende beveiligingstandaarden t.a.v. DKIM, DMARC, DNSSEC zoals omschreven op: https://www.forumstandaardisatie.nl/openstandaarden/verplicht?domein=125&trefwoord=180		
B15	Tijdens de verificatiefase (voorafgaand aan definitieve gunning), als onderdeel van de acceptatie van de oplevering en/of tijdens looptijd contract wordt geverifieerd of aan de gestelde beveiligingseisen is voldaan.		
C	**Eisen met betrekking tot fysieke beveiliging en continuïteit**	**Akkoord leverancier & toelichting**	**Reactie SWO**
C1	Leverancier zorgt voor adequate maatregelen voor fysieke beveiliging en fysieke toegangsbeveiliging van de verwerkingslocaties.		
C2	Leverancier dient te zorgen voor een effectief back-up- en herstelproces dat voldoet aan de door de Opdrachtgever vastgestelde Recovery Point Objective (RPO) en Recovery Time Objective (RTO) zoals vermeld in het volgende tabblad om de continuïteit van de dienstverlening te waarborgen.		
D	**Eisen met betrekking tot logische toegangsrechten**	**Akkoord leverancier & toelichting**	**Reactie SWO**

D1	Leverancier zorgt ervoor dat toegang tot de data van Opdrachtgever exclusief voorbehouden blijft aan geautoriseerde personen, waarbij deze toegang beperkt wordt tot medewerkers van Leverancier en diens onderaannemers die deze toegang strikt noodzakelijk hebben voor het uitvoeren van hun functies.		
D2	De oplossing biedt de functionaliteit om autorisaties in te richten op basis van rollen.		
D3	Wachtwoord eisen en geldigheidsduur kunnen gesteld worden vanuit de oplossing. Het kan daarmee voldoen aan de wachtwoordrichtlijnen van Opdrachtgever.		
D4	Leverancier beschikt over adequate processen voor (logische) toegangsverlening en monitoring van medewerkers van Leverancier tot data die onderdeel is van de dienstverlening aan Opdrachtgever.		
D5	Op verzoek van Opdrachtgever levert Leverancier een overzicht van welke medewerkers vanuit hun functie welke toegang tot de data van Opdrachtgever of de klanten hebben.		
D6	Op verzoek van Opdrachtgever levert Leverancier een overzicht van high privileged accounts binnen die dienstverlening aan Opdrachtgever, op basis van logging van de activiteiten van deze accounts.		
D7	Als onderdeel van de dienstverlening aan Opdrachtgever zorgt Leverancier voor sterke authenticatiemogelijkheden, minimaal dient Leverancier een sterk wachtwoordbeleid toe te passen.		
D8	Gebruikers van de oplossing hebben een **unieke login ID** voor hun gebruikersaccount. De unieke login ID van gebruikersaccounts zijn persoonsgebonden en zijn herleidbaar naar een natuurlijk persoon/individu, zijnde de gebruiker/beheerder. Systeemprocessen draaien onder een unieke login ID (een functioneel account).		
D9	Leverancier hanteert een adequaat wachtwoordenbeleid en volgt daarbij best practices zoals de CIS benchmarking of vergelijkbaar. https://www.cisecurity.org/insights/white-papers/cis-password-policy-guide		
D10	Leverancier zorgt dat bij toepassing van service accounts (o.a. t.b.v. koppelingen) deze altijd draaien met minimale rechten. Service accounts krijgen alleen de specifieke rechten die ze nodig hebben. Ook kunnen ze niet gebruikt worden om in te loggen (i.e. geen shell). Er zijn beperkingen aanwezig op het aantal inlogpogingen of er wordt d.m.v. certificaten ingelogd. Er zijn beperkingen op herhaaldelijk verkeerd inloggen.		
D11	Alle login acties/pogingen worden gelogd in de oplossing		
E	**Eisen van uit wet- en regelgeving**	**Akkoord leverancier & toelichting**	**Reactie SWO**
E1	Leverancier zorgt voor tijdige informatie aan Opdrachtgever in geval Opdrachtgever gegevens of gegevens van Opdrachtgever klanten onderdeel is van een gerechtelijk bevel of andere verplichte wettelijke toegang. Leverancier zal verzoeken om toegang tot de data zonder dat hier een gerechtelijk bevel voor is altijd afwijzen.		
E2	Leverancier zorgt dat hosting fysiek plaatsvindt binnen de EER (Europese Economische Ruimte) tenzij Opdrachtgever afwijking hiervan van tevoren heeft goedgekeurd. Leverancier blijft exclusief verantwoordelijk voor de uitvoering van alle afspraken en voor het corrigeren of compenseren van alle eventuele tekortkomingen van derde partijen die leverancier heeft ingeschakeld.		
E5	Op verzoek van Opdracht levert Leverancier een overzicht van alle onderaannemers. Leverancier garandeert dat afspraken tussen Opdrachtgever en leverancier over informatiebeveiliging ook van toepassing zijn op de onderaannemers van Leverancier en dat daarmee het overeengekomen beveiligingsniveau tussen Opdrachtgever en Leverancier in de gehele keten is gewaarborgd.		
F	**Eisen vanuit Archivering**	**Akkoord leverancier & toelichting**	**Reactie SWO**
F1	Leverancier waarborgt dat de oplossing voldoet aan de vereisten van Opdrachtgever voor het bewaren en vernietigen van gegevens, in overeenstemming met de 'Richtlijn bewaren en vernietigen'. Dit houdt in dat Leverancier gedurende de looptijd van de overeenkomst de verwerkte gegevens aantoonbaar bewaart voor de vastgestelde bewaartermijn en zorgt voor passende maatregelen voor het schonen van data in applicaties, databases en back-ups. Na afloop van de bewaartermijn, of bij toestemming van Opdrachtgever, zal Leverancier de gegevens vernietigen. Verder draagt Leverancier zorg voor de anonimisering van persoonsgegevens bij het verstrijken van de bewaartermijn, indien verwijdering uit de database van de IT-dienst of Cloud SaaS-toepassing niet mogelijk is.		
F2	Leverancier zal, behoudens op haar rustende wettelijke (archief)verplichtingen, alle (persoons)gegevens na beëindiging van de overeenkomst, per ommegaande kosteloos retourneren aan de Opdrachtgever en, indien de Opdrachtgever daartoe opdracht heeft gegeven, wissen en uit haar systemen (incl. back-up) verwijderen danwel vernietigen op de wijze als door de Opdrachtgever bepaald. De vernietiging moet, binnen nader overeen te komen termijn, uitgevoerd worden en hiervan wordt een verslag gemaakt.		

Aanvullende Maatregelen Nivo 2

Deze maatregelen zijn aanvullend op de GIBIT-voorwaarden.

ID	Topic	Eis	Akkoord leverancier & toelichting	Reactie SWO
1	**Assurance**	Opdrachtnemer is NEN/ISO 27001, ISAE 3402 en/of gelijkwaardig gecertificeerd, waarbij dan de volgende voorwaarden van kracht zijn: • Opdrachtnemer overlegt het certificaat. • Het certificaat is niet ouder dan 3 jaar en afgegeven onder accreditatie van de RVA. • Opdrachtnemer communiceert over de jaarlijkse audit. • Opdrachtnemer levert de bijbehorende statement of applicability (SOA) (ook wel: verklaring van toepasselijkheid). • De scope (certificering) en de verklaring (SOA) passen voor of bij de onderhavige opdracht. • Opdrachtnemer laat jaarlijks zien dat het verschil tussen de ISO 27001 / ISAE3402 certificering en de in de BIO genoemde overeenkomstige harde maatregelen (passend op de SOA) is opgelost dan wel geïmplementeerd door middel van het afgeven van een Statement of Compliance (zie ook BIO 4.4 laatste paragraaf) (het verschil tussen de ISO en de BIO is dat de ISO implementatie voorbeelden kent en de BIO kent harde verplichte maatregelen).		
2	**Assurance**	Op verzoek van Opdrachtgever levert Leverancier (jaarlijks) een onafhankelijke assurance rapportage aanleveren op basis van de contracturele afspraken die zijn gemaakt over de dienstverlening aan Opdrachtgever, op basis van de vereiste certificeringen, waarbij de scope van de verklaring in overeenstemming is met de dienstverlening aan Opdrachtgever.		
4	**Beschikbaarheid**	Indien het een systeem betreft waarbij gegevens worden verwerkt bedraagt het dataverlies (RPO) in geval van calamiteiten maximaal 24 uur (conform GIBIT 2023, art 29.4). Voor gewone verstoringen gelden de hersteltijden die vastgelegd zijn in de Service Level Agreement (SLA).		
5	**Beschikbaarheid**	De maximale hersteltijd processen (MTD) in geval van calamiteiten bedraagt maximaal 120 klokuren, hersteltijd IT/systeem/applicatie (RTO) bedraagt maximaal 72 klokuren. Voor gewone verstoringen gelden de hersteltijden die vastgelegd zijn in de Service Level Agreement (SLA).		
8	**Back up**	Leverancier zorgt voor adequate back-up van data en (disaster) recovery, als onderdeel van de dienstverlening aan Opdrachtgever.		
9	**Continuiteit**	De leverancier heeft voor herstel in ieder geval een uitwijklocatie geïmplementeerd die minimaal jaarlijks wordt getest; en een business continuity plan en een disaster recovery procedure is aanwezig. Deze zijn actueel en worden minimaal jaarlijks getest.		
10	**Rapportage**	De leverancier draagt zorg voor periodiek onderhoud in samenwerking met SWO de Wolden Hoogeveen en rapporteert minimaal **elk half jaar** over de kwaliteit van dienstverlening conform de eisen in de SLA. Hierbij wordt minimaal ingegaan op: i Relevante voorgedane verstoringen/beveiligingsincidenten/datalekken en opvolging (binnen de gestelde kpi uit de SLA) ii Resultaten kwetsbaarheidsscans en opvolging iii Resultaten van uitgevoerde recoverytesten die eens per jaar wordt uitgevoerd (uitval, uitwijk, back-up restore) (hoge beschikbaarheid) iv Resultaten pentest en opvolging bevindingen die minimaal eens per jaar wordt uitgevoerd		
12	**Monitoring**	Logging kan naar een extern logging systeem (SIEM) gestuurd worden. De uitwisseling van deze informatie is mogelijk op basis via een connector, API of via STIX en TAXII.		
13	**Monitoring**	Leverancier heeft een logging- en monitoringsfunctie (SIEM/SOC) geïmplementeerd voor de oplossing ter bescherming tegen ICT-gerelateerde dreigingen die een impact kunnen hebben op de bedrijfsvoering en dienstverlening van SWO de Wolden Hoogeveen. Er wordt hiermee gemonitord door leverancier (via een review/analyse op de logbestanden) op informatiebeveiligingsgebeurtenissen; de opvolging daarvan is in lijn met de urgentie / impact van de gebeurtenis en er wordt gecommuniceerd met het CERT van SWO de Wolden Hoogeveen. Monitoring en response vindt plaats basis van voorgedefinieerde usecases		
17	**Logische toegang**	Gebruikers en beheerders moeten een tweede factor gebruiken om te verifiëren voordat ze toegang krijgen tot gegevens of functionaliteit.		
19	**Logische toegang**	Per reguliere gebruiker kan maar één sessie geopend zijn.		
21	**Testen**	Binnen de test omgeving wordt geen gebruik gemaakt van productie data		

Aanvullende Maatregelen Nivo 3

Deze maatregelen zijn aanvullend op de GIBIT-voorwaarden.

ID	Topic	Eis	Akkoord leverancier & toelichting	Reactie SWO
1	**Assurance**	Opdrachtnemer is NEN/ISO 27001, ISAE 3402 en/of gelijkwaardig gecertificeerd, waarbij dan de volgende voorwaarden van kracht zijn: • Opdrachtnemer overlegt het certificaat. • Het certificaat is niet ouder dan 3 jaar en afgegeven onder accreditatie van de RVA. • Opdrachtnemer communiceert over de jaarlijkse audit. • Opdrachtnemer levert de bijbehorende statement of applicability (SOA) (ook wel: verklaring van toepasselijkheid). • De scope (certificering) en de verklaring (SOA) passen voor of bij de onderhavige opdracht. • Opdrachtnemer laat jaarlijks zien dat het verschil tussen de ISO 27001/ISAE3402 certificering en de in de BIO genoemde overeenkomstige maatregelen (passend op de SOA) is opgelost dan wel geïmplementeerd door middel van het afgeven van een Statement of Compliance (zie ook BIO 4.4 laatste paragraaf) (het verschil tussen de ISO en de BIO is dat de ISO implementatie voorbeelden kent en de BIO kent harde verplichte maatregelen).		
2	**Assurance**	De Leverancier kan op verzoek van de Opdrachtgever (jaarlijks) een onafhankelijke assurance rapportage aanleveren op basis van de contracturele afspraken die zijn gemaakt over de dienstverlening aan Opdrachtgever, op basis van de vereiste certificeringen, waarbij de scope van de verklaring in overeenstemming is met de dienstverlening aan Opdrachtgever.		
3	**Assurance**	De leverancier dient een actuele SOC2-verklaring of vergelijkbaar te overhandigen, waarin wordt bevestigd dat hun diensten en operationele processen voldoen aan de Trust Services Criteria van SOC2. Deze verklaring moet gedetailleerd inzicht geven in de wijze waarop de leverancier de principes van beveiliging, beschikbaarheid, verwerkingsintegriteit, vertrouwelijkheid en privacy, zoals vastgesteld in de SOC2-standaarden, naleeft. De SOC2-verklaring dient regelmatig te worden vernieuwd om te verzekeren dat de leverancier voortdurend voldoet aan deze standaarden en adequaat reageert op nieuwe beveiligingsuitdagingen en -risico's.		
6	**Beschikbaarheid**	Indien het een systeem betreft waarbij gegevens worden verwerkt bedraagt het dataverlies (RPO) in geval van calamiteiten maximaal 8 uur		
7	**Beschikbaarheid**	De maximale hersteltijd processen (MTD) in geval van calamiteiten bedraagt maximaal 48 klokuren, hersteltijd IT/systeem/applicatie (RTO) bedraagt maximaal 24 klokuren. Voor gewone verstoringen gelden de hersteltijden die vastgelegd zijn in de Service Level Agreement (SLA).		
8	**Back up**	Leverancier zorgt voor adequate back-up van data en (disaster) recovery, als onderdeel van de dienstverlening aan Opdrachtgever.		
9	**Continuiteit**	De leverancier heeft voor herstel in ieder geval een uitwijklocatie geïmplementeerd die minimaal jaarlijks wordt getest; en een business continuity plan en een disaster recovery procedure is aanwezig. Deze zijn actueel en worden minimaal jaarlijks getest.		
11	**Rapportage**	De leverancier draagt zorg voor periodiek onderhoud in samenwerking met SWO de Wolden Hoogeveen en rapporteert minimaal **elk kwartaal** over de kwaliteit van dienstverlening conform de eisen in de SLA. Hierbij wordt minimaal ingegaan op: i Relevante voorgedane verstoringen/beveiligingsincidenten/datalekken en opvolging (binnen de gestelde kpi uit de SLA) ii Resultaten kwetsbaarheidsscans en opvolging iii Resultaten van uitgevoerde recoverytesten die eens per jaar wordt uitgevoerd (uitval, uitwijk, back-up restore) (hoge beschikbaarheid) iv Resultaten pentest en opvolging bevindingen die minimaal eens per jaar wordt uitgevoerd		
12	**Monitoring**	Logging kan naar een extern logging systeem (SIEM) gestuurd worden. De uitwisseling van deze informatie is mogelijk op basis via een connector, api of via STIX en TAXII.		
13	**Monitoring**	Leverancier heeft een logging- en monitoringsfunctie (SIEM/SOC) geïmplementeerd voor de oplossing ter bescherming tegen ICT-gerelateerde dreigingen die een impact kunnen hebben op de bedrijfsvoering en dienstverlening van SWO De Wolden Hoogeveen. Er wordt hiermee gemonitord door leverancier (via een review/analyse op de logbestanden) op informatiebeveiligingsgebeurtenissen; de opvolging daarvan is in lijn met de urgentie / impact van de gebeurtenis en er wordt gecommuniceerd met het CERT van SWO De Wolden Hoogeveen. Monitoring en response vindt plaats basis van voorgedefinieerde usecases.		
17	**Logische toegang**	Gebruikers en beheerders moeten een tweede factor gebruiken om te verifiëren voordat ze toegang krijgen tot gegevens of functionaliteit.		

21	**Testen**	Binnen de test omgeving wordt geen gebruik gemaakt van productie data		

Wensen

Deze maatregelen zijn wensen en moeten gelezen worden vanuit de aard van de dienstverlening.

A	Logische toegang	Toelichting door leverancier	Reactie SWO
A1	Er is een koppeling mogelijk met Azure AD (Azure Single Sign-ON (SSO)voor zowel gebruikers van Opdrachtgever als voor beheerwerkzaamheden door de medewerkers van Leverancier.		