Acceptatiecriteria cloudapplicaties Aventus

Nummer	Omschrijving	Ja/Nee/NVT	Eventuele toelichting
A. Technische eisen			
A1	Alle gegevens worden versleuteld getransporteerd: • Datatransport wordt volgens up-to-date encryptie-standaarden en standaard transportprotocollen versleuteld. Transport over TLS of SSl mogen niet op basis van self signed certificaten verlopen • Als het transportprotocol geen mogelijkheden biedt, moet de data versleuteld worden met AES-256 encryptie of veiliger • Bij fysiek transport van gevoelige data, zoals USB-sticks, dient de data volgens up-to-date encryptie-standaarden versleuteld te zijn. • Leverancier heeft certificaatbeheer ingericht en onderhoud de certificaten via een Third Party Signed.		
A2	De identiteit van gebruikers is gecontroleerd en federatief beheerd: • Applicaties maken gebruik van (SAML 2.0 / OpenID Connect) voor identificatie en authenticatie. Aventus geniet de voorkeur voor SurfConext. • Het is mogelijk om een lock-out mechanisme in te stellen tegen brute-forcing. Dit gaat in overleg met Aventus.		
A3	Er wordt Multi-Factor Authenticatie (MFA) toegepast als er bijzondere persoonsgegevens worden opgeslagen. Zie bijlage 1 Standaard verwerkersovereenkomst Aventus: SurfSecureID		
A4	Veilig sessiemanagement wordt toegepast: • Gebruik HTTP-headers, zie https://securityheaders.com • Richt sessiemanagement in, zie: https://www.owasp.org/index.php/Session_Management_Cheat_Sheet • Gebruik sessie-cookies met 'HttpOnly' en 'Secure' flags		
A5	Alle in- en uitvoer van data wordt genormaliseerd, gevalideerd en ingeperkt: • Bij in- en uitvoer van data moet normalisatie, validatie en inperking toegepast worden. • Documenten moeten indien nodig worden omgezet in een formaat dat geen schade kan aanrichten.		
A6	Configuratie-lekken worden voorkomen: • Banners en headers dienen geen configuratiegegevens te lekken.		

	• Foutpagina's dienen geen configuratiegegevens te lekken. Denk hierbij aan stacktraces en interne debug-informatie. • Commentaar in code wordt niet aan eindgebruikers getoond.		
A7	De leverancier heeft een proces ingericht ter voorkoming van het benutten van technische kwetsbaarheden en rapporteert periodiek hierover aan Aventus. Het proces omvat in ieder geval: • het regelmatig up-to-date houden van systemen en software (patching), • het tijdig vergaren van informatie over nieuwe kwetsbaarheden (intelligence), • het controleren van netwerk en systemen op kwetsbaarheden (vulnerability assessment), • het testen van webapplicaties, op regelmatige basis, op kwetsbaarheden (Web application scanning), • het gebruik van antivirussoftware die dagelijks wordt geactualiseerd, • beperkingen op het installeren van (ongeautoriseerde) software, • het uitvoeren van een pentest bij ingebruikname en major updates.		
B. Privacy en Informatiebeveiliging			
B1	De applicatie voorziet in Privacy by Design (waaronder anonimiseren, dataminimalisatie, pseudonimiseren, encryptie, access control, Privacy by Default, bewaren/vernietigen, faciliteren rechten betrokkenen, beheer).		
B2	Persoonsgegevens worden alleen opgeslagen en verwerkt in de EU/EER.		
B3	De door Aventus gehanteerde bewaar- en vernietigingstermijnen kunnen via de applicatie worden gehandhaafd. Zie bijlage 2 Bewaartermijnen documenten.		
B4	De leverancier heeft Informatiebeveiliging ingericht conform een relevante normenkader (NEN-ISO/IEC: 27001 / 27002/ISAE3402).		
B5	De leverancier is bereid een door Aventus goedgekeurde verwerkersovereenkomst te ondertekenen. (Aventus standaard verwerkersovereenkomst, Model verwerkersoverenkomst Privacyconvenant MBO of Surf Model verwerkersovereenkomst)		
B6	De leverancier verwerkt zonder toestemming geen gegevens van Aventus voor eigen doelen (zoals testen en data-analyses).		
C. Gegevensbescherming			
C1	Als een applicatie toegang nodig heeft tot een apparaat (zoals een laptop of smartphone), dan is die toegang beperkt tot wat nodig is om de functionaliteit te bieden waarvoor de applicatie is bedoeld.		

C2	De gegevens van Aventus zijn logisch of fysiek afgeschermd van partijen die die gegevens niet mogen inzien. Denk aan het scheiden van databanken tussen de diverse afnemers van een SAAS-dienst.		
D. Logging			
D1	De applicatie biedt voldoende mogelijkheden voor auditing en logging: • Logging en auditing worden opgeslagen. • Logging en auditing is beveiligd tegen ongeautoriseerde toegang. • Kritieke handelingen van gebruikers (zoals aanmaken van accounts, wijzigen van autorisaties, goedkeuren van een examen, wissen van belangrijke gegevens, toegang tot gevoelige gegevens) worden gelogd. • Logging en auditing is voldoende gedetailleerd zodat incidenten herleid kunnen worden naar natuurlijke personen. Deze gegevens zijn op verzoek beschikbaar voor Aventus.		
D2	De leverancier legt activiteiten van systeembeheerders en -operators vast en beoordeelt ze regelmatig en rapporteert hierover periodiek aan Aventus.		
D3	De leverancier bewaart alle informatie in de logbestanden tenminste 1 maand en ten hoogste 3 maanden, tenzij wettelijke verplichtingen anders voorschrijven of de logbestanden nodig zijn voor onderzoek in het kader van een (vermoed) beveiligingsincident. Gedurende die periode kan deze informatie worden ingezien door de opdrachtgever.		
E. Toegangsrechten			
E1	De leverancier heeft een formeel proces ingericht voor het beheer van toegangsrechten van de eigen medewerkers. Het toegangsbeheerproces omvat ten minste: • het registreren van gebruikers en de aan hen toegekende rechten, • het toekennen van niet meer rechten dan nodig voor de uitoefening van taken en • het wijzigen of intrekken van die rechten bij wijziging of beëindiging van het dienstverband of contract. Wijzigingen die relevant zijn voor Aventus worden zo snel mogelijk doorgegeven aan Aventus.		
E2	De leverancier controleert minimaal 2 keer de toegangsrechten van de eigen medewerkers en minimaliseert die tot het strikt noodzakelijke.		
E3	Autorisatiebeheer vindt plaats op basis van functiescheiding en rollen waarmee kan worden afgedwongen dat gebruikers alleen toegang hebben tot informatie die strikt nodig is voor hun werkzaamheden (need-to-know, time-to-know, least privilege). De applicatie beschikt over ingericht rollenbeheer.		

F. Back-up & restore			
F1	Alle gegevens in de applicatie zijn opgenomen in een back-up. De frequentie en de omvang hiervan zijn in overeenstemming met de (te verwachten) risicoscores (BIV).		
F2	De leverancier heeft up-to-date back-up en restore procedures opgesteld en werkt hier mee.		
F3	Deze procedures worden periodiek getest en er zijn hier rapportages van beschikbaar. Op verzoek kan		
F4	De back-up wordt op een veilige locatie opgeborgen; fysiek gescheiden van de productielocatie.		
F5	De omgeving (applicatie en gegevensbestanden) kan worden hersteld na een calamiteit. De omvang en snelheid hiervan zijn in overeenstemming met de (te verwachten) risicoscores (BIV).		
G. Service & Support			
G1	Er is een helpdesk aanwezig die tijdens kantooruren (tussen 8.00 – 17.00uur) bereikbaar is.		
G2	De leverancier rapporteert elk kwartaal of vaker aan Aventus over security management. Minimaal zijn de onderstaande onderdelen opgenomen: - Security incidenten (aantal, status, voortgang, oorzaak, impact en oplossing) Implementatie van beveiligingsmaatregelen.		
G3	Er is een up-to-date SLA aanwezig. Deze wordt gemonitored en er wordt minimaal per kwartaal over gerapporteerd.		
G4	De leverancier heeft een proces ingericht voor incidentenbeheer		
G5	De leverancier heeft een proces ingericht voor wijzigingsbeheer		
H. OTAP			
H1	De leverancier test wijzigingen in een test- of acceptatieomgeving alvorens deze in productie te brengen en legt testresultaten vast.		
H2	Er wordt door de leverancier niet getest met productie gegevens van Aventus, tenzij deze gegevens geanonimiseerd zijn.		
I. Integratie (koppelingen)			
I1	Het systeem heeft de mogelijkheid om gegevens uit te wisselen met andere systemen d.m.v. API koppelingen		
I2	Berichtuitwisseling tussen pakket en bestaande systemen binnen Aventus vindt veilig plaats op basis van meest gangbare encryptie methodes (TLS 1.2 of hoger).		
J. Integratie (apparatuur/software)			
J1	Het pakket ondersteunt de laatste 2 versies van veel gebruikte internetbrowsers zoals Microsoft Edge, Mozilla Firefox, Google Chrome en Safari.		

J2	Het pakket werkt zonder problemen op de: - Laatste twee beschikbare Windows versie en Mac Os versie Tablets en Smartphones (IOS en Android)		
K. Beschikbaarheid			
K1	De omgeving is HA (highly available) met gegarandeerde beschikbaarheid van 99,99 procent tijdens kantooruren en 99,9 procent in daluren. De beschikbaarheid van de omgeving is gegarandeerd volgens de BIV-score.		
K2	Nieuwe software versies dienen minimaal 2 weken voorafgaand aan implementatie gemeld te worden.		
K3	Onderhoudswerkzaamheden worden alleen in overleg met Aventus uitgevoerd. Ze moeten minimaal 48 uur voor het geplande onderhoud gemeld worden. Afhankelijk van de BIV-score worden onderhoudswerkzaamheden uitsluitend buiten kantooruren uitgevoerd.		
K4	De leverancier voert wijzigingen uit in de afgesproken servicevensters en overlegt wijzigingen met grote impact voorafgaand aan realisatie met de opdrachtgever.		
K5	Opdrachtgever krijgt de mogelijkheid om rapportages te genereren met betrekking tot gebruik en beschikbaarheid.		
L. Beëindiging			
L1	Dataportabiliteit is geborgd. Er is een exit-plan aanwezig. De leverancier draagt bij einde dienstverlening alle gegevens over aan Aventus en/of vernietigt deze op verzoek van Aventus en bewaart geen gegevens voor eigen doeleinden.		
L2	Er is een escrow regeling aanwezig voor zowel de broncode als data. De data wordt in een uitleesbaar formaat in bewaring gegeven en regelmatig geüpdatet. Bij beëindiging worden deze gegevens in een voor Aventus geautomatiseerd verwerkbaar formaat (excel/CSV of SQL Dump) aangeleverd. Deze export en de originele live data zijn minimaal twee maanden beschikbaar voor volledigheidscontrole.		
L3	De leverancier heeft een procedure ingericht om de opdrachtgever tijdig en adequaat te informeren over potentiële datalekken en security incidenten waarvan hij kennis krijgt (inclusief die bij sub-bewerkers of hulpleveranciers) en documenteert bij een incident alle stappen die zijn ondernomen in het kader van de meldplicht datalekken.		
L4	Leverancier hanteert actief een strikte geheimhoudingsovereenkomst welke door de medewerkers en derden specifiek voor de werkzaamheden met de gegevens van Aventus ondertekend is.		

Bijlage 1 Aventus standaard verwerkersovereenkomst

Aventus standaard-verwerkersovereenkomst .docx

Bijlage 2 Bewaartermijnen Documenten

Bewaartermijnen documenten.docx (sharepoint.com)