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 Certificate Authoroty		
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	De applicatie is geschikt voor Multi-Factor Authenticatie (MFA). Er wordt standaard MFA toegepast als er bijzondere persoonsgegevens worden opgeslagen. Zie bijlage Privacy sluiter in de Standaard verwerkersovereenkomst Aventus (Bijlage 8) voor de lijst met gegevens waarvoor MFA is vereist: - urfSSecureID		
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). De leverancier heeft een adequaat en effectief patching beleid dat voldoet aan de eisen van het Beleid patchmanagement Aventus. • 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 penetratietest bij ingebruikname en major updates.		
A8	De leverancier voert regelmatig penetratietesten uit. De diepgang en frequentie van deze penetratietesten is (mede) afhankelijk van de BIV-classificatie zoals vastgesteld door Aventus en voldoet aan in de markt gehanteerde best practices. Aventus hanteert het Certificeringsschema Informatiebeveiliging en Privacy ROSA. Indien de applicatie BIV-classificatie Vertrouwelijkheid Hoog heeft, dan dient de leverancier minimaal tweejaarlijks een pentest uit te laten voeren.		
A9	Aventus moet in goed overleg met de leverancier aanvullend de mogelijkheid hebben om controles met betrekking tot de applicatie te kunnen uitvoeren, inclusief, maar niet beperkt tot het (laten) uitvoeren van penetratietesten.		
A10	De leverancier treft beveiligingsmaatregelen in lijn met de BIV-classificatie zoals vastgesteld door Aventus om de beschikbaarheid, integriteit en vertrouwelijkheid van de applicatie en de gegevens daarin te waarborgen en treedt hierover in overleg met Aventus ter vaststelling of deze maatregelen voldoende zijn.		
B. Privacy en Informatiebeveiliging			
B1	De leverancier heeft haar beveiliging zodanig ingericht zodat het voldoet aan het Informatiebeveiligings- en privacy beleid Aventus		

B2	De applicatie voorziet in Privacy by Design (waaronder anonimiseren, dataminimalisatie, pseudonimiseren, encryptie, access control, Privacy by Default, bewaren/vernietigen, faciliteren rechten betrokkenen, beheer).		
B3	Persoonsgegevens worden alleen opgeslagen en verwerkt in de EU/EER.		
B4	De door Aventus gehanteerde bewaar- en vernietigingstermijnen kunnen via de applicatie worden gehandhaafd.		
B5	De leverancier heeft Informatiebeveiliging ingericht conform een relevante normenkader (NEN-ISO/IEC: 27001 / 27002/ISAE3402).		
B6	De leverancier is bereid een door Aventus goedgekeurde verwerkersovereenkomst te ondertekenen: Aventus standaard verwerkersovereenkomst, Model verwerkersovereenkomst Privacy convenant MBO of Surf Model verwerkersovereenkomst		
B7	De leverancier verwerkt zonder toestemming geen gegevens van Aventus voor eigen doelen (zoals testen en data-analyses).		