

Bij nr. 17

De SQL-records kunnen niet meer worden benaderd als de gebruiker niet meer is ingelogd. Uitloggen uit het systeem maakt deze bestanden nog steeds toegankelijk via de Verkenner of Finder op de eigen computer. De organisatie dient op de clientcomputers beveiligingsmaatregelen toe te passen, zoals het locken van client PC's bij afwezigheid langer dan een bepaalde tijd, het legen van TEMP- en download-directories bij uitloggen of afsluiten van de client PC, e.d. Alhoewel na uitloggen de applicatie niet meer toegankelijk is (zowel SQL-records als filesystem), zijn de geraadpleegde bestanden van het filesystem dat zonder maatregelen wel. Het is aan de organisatie om de raadpleging hiervan na uitloggen onmogelijk te maken.

Bij nr. 18

De applicatie kan alle bestandsformaten opnemen. In de Centrale Inlogomgeving (waarin AFAS aangeeft wat voor alle klanten geldig is) wordt gewerkt met white- en blacklists. Aangebrachte restricties in de opname van bestandsformaten gelden ter voorkoming van infecties. In de Centrale Inlogomgeving zouden die beperkingen kunnen worden aangebracht, maar dan zouden ze gelden voor alle klanten. Dat kan niet, omdat iedere organisatie andere wensen heeft. Als een organisatie een beperking op bestandsformaten wil, zal ze dat in de workflow moeten regelen en daarin een check moeten uitvoeren op bestandsformaat. De organisatie moet ook zelf zorgen dat er toepassingsprogrammatuur en/of viewers zijn voor de bestanden die zijn opgenomen in de dossiers. De applicatie doet het dus niet zelf, maar kan het via de workflow wel faciliteren.

Bij nr. 20. (Zie Verklaring bij nr. 18)

De check op bestandsformaten wordt uitgevoerd op basis van black and whitelist-validatie. Als de organisatie de bijlagen in specifieke formaten wenst op te nemen dan dient dat door de organisatie middels een faciliterende workflow te gebeuren, waarin wordt gecheckt op de bestandsformaten en ze ook kunnen worden klaargezet voor migratie.

Bij nr. 23

Het SQL-record kan tegelijkertijd door meerdere gebruikers worden geraadpleegd en wordt aan ieder van die gebruikers (uiteraard afhankelijk van autorisatie) op dezelfde wijze gepresenteerd. De software voor raadpleging van de als bijlagen toegevoegde bestanden (kantoorsoftware, viewers, e.d.) wordt door de organisatie geleverd (zie nr. 18) en kan onafhankelijk zijn van de software die de bestanden heeft gegenereerd.

Bij nr. 34

De applicatie sluit niet automatisch een SQL-record af, al kan wel gedefinieerd worden dat bij afronden van een specifieke workflow het SQL-record wordt afgesloten. Als alle zaken via workflow worden afgehandeld, zouden alle SQL-records automatisch kunnen worden afgesloten (als dat nodig is). Automatisch een nieuw SQL-record openen gebeurt echter niet. Dit kan alleen nog voorkomen bij factuurnummering, waar automatisch het volgende SQL-record wordt geopend. Er is nooit aanleiding geweest om een dergelijke functionaliteit te realiseren, buiten de afhandeling van facturen.

Bij nr. 37 (a-f)

De applicatie werkt in principe niet met hybride archivering, maar het kan wel. Alle metadata (ook voor papieren dossiers) zijn immers vast te leggen. Als hybride archivering moet worden ondersteund dan dient een workflow te worden ingericht, die dit hele punt ondersteunt en die alle volgende eisen (a-f) ondersteunt. De organisatie dient zelf de bewerking op de papieren files uit te voeren in overeenstemming met de metadata zoals die zijn toegekend aan het SQL-record, dat in de applicatie is aangemaakt.

Bij nr. 45

Beheerhandelingen (zoals bijvoorbeeld veranderingen in de configuratie van het metadatamodel en de audit trail) worden pas definitief vastgelegd een audit trail indien ze worden gegenereerd via een workflow. Om compliant te werken en om alle handelingen binnen de applicatie te documenteren via een audit trail is het nodig om te werken via een workflow, zowel voor de afhandeling van taken en activiteiten als voor het verwerken van data, de beheeractiviteiten uitgevoerd binnen de applicatie en het beheren van de content. Organisaties dienen goed te overwegen welke handelingen en activiteiten volgens het op hen van toepassing zijnde wet- en regelgevingskader gedocumenteerd dienen te worden en daarvoor de workflow-functionaliteit in te zetten. Alleen dan kan compliant werken worden afgedwongen.

Bij nr. 50

Een klant kan een kopie van de database aanvragen of een roll back. De functionaliteit wordt aangeboden in de applicatie en de klant kan aangeven dat een back-up moet worden gemaakt. Een roll back kan worden gerealiseerd, maar een klant moet daar specifiek om vragen, waarna het door de leverancier wordt uitgevoerd. Het specifiek aangeven door een klant dat een back-up moet worden gemaakt is een extra functionaliteit bovenop de bestaande back-up systematiek van AFAS. Deze back-up systematiek ziet er als volgt uit:

- Elke 24 uur wordt de back-up gemaakt en opgeslagen
- Deze back-up wordt 31 dagen lang bewaard
- Na 31 dagen wordt deze verwijderd, behalve indien het abonnement niet meer geldig is.
- Back-ups van niet geldige abonnementen worden na 1 jaar verwijderd, tenzij de verantwoordelijke van de data aangeeft dat deze eerder verwijderd dient te worden.

Bij nr. 52

Migratie naar andere applicaties wordt door de applicatie ondersteund. De totale SQL-records (Inclusief bijlagen) kunnen naar andere applicaties worden gemigreerd. Bestandsconversie echter wordt enkel gefaciliteerd door de applicatie in de workflow. De klant dient derden software te gebruiken om de bestanden zelf te converteren.

Bij nr. 58

Een archiefwettelijke vernietiging moet definitief zijn. De verwijderde SQL-records zijn niet meer te reconstrueren. Om te waarborgen dat de uitgevoerde vernietiging ook daadwerkelijk definitief wordt en de afzonderlijke records niet meer te reconstrueren zijn, dient een klant na een uitgevoerde vernietiging een nieuwe back-up te laten maken, waardoor de nieuwe situatie wordt vastgelegd. Een archiefwettelijke vernietiging wordt op basis van een vertrouwelijke workflow uitgevoerd, waarbij voldoende waarborgen zijn om niet 'per ongeluk' records te vernietigen. Eenmaal geaccordeerd is de vernietiging definitief. AFAS kan (en zal) op dat moment records niet meer terugplaatsen, aangezien de vernietiging op grond van wettelijke regels heeft plaatsgevonden en een dergelijke vernietiging onherstelbaar moet zijn.

Bij nr. 65 (b)

De SQL-database gebruikt zelf hashes en checksums voor alle data opgenomen in een SQL-record.

Het Filesystem echter doet dat niet. Het waarborgen van de integriteit van de bijlagen in SQL-records is gewaarborgd indien de bijlagen onderdeel zijn van een Dossieritem. Dan kan de bijlage niet veranderd worden (in ieder geval niet zonder autorisatie). In een reactie op het Dossieritem kunnen wel nieuwe bijlagen geplaatst worden, maar dit tast het Dossieritem zelf niet aan. Om te zien of alle bijlagen aanwezig zijn kan een analyse gemaakt worden, waarbij een match gemaakt wordt tussen het SQL-record en het filesystem. Dit geeft aan of er afwijkingen zijn in de bijlagen die aanwezig zouden zijn.