Bijlage 9 - Programma van Eisen -
Leveren elektrotechnische sluitsystemen met kenmerk TiU/FS07225

Door ondertekening van het Uniform Europees Aanbestedingsdocument verklaart Inschrijver aan onderstaande eisen te voldoen.

1. Algemene eisen

1.1	Het toegangscontrolesysteem (TCS) dient geschikt te zijn om in alle gebouwen toegepast te kunnen worden.
1.2	Het elektronisch slot werkt zonder dat deze aangesloten hoeft te worden op een gebouw gebonden stroomaansluiting.
1.3	Het elektronisch slot is configureerbaar zonder deze aan te hoeven sluiten op een gebouw gebonden ethernetkabel.
1.4	Het toegangscontrolesysteem moet een modulaire opbouw (hardware en software) hebben met de mogelijkheid tot uitbreiding van het toegangscontrolesysteem indien meer locaties, autorisatiemiddelen en/ of deuren(diktes) gewenst zijn.
1.5	Met het autorisatiemiddel kunnen gebruikers zelfstandig de deur waarin het slot zit openen, mits men daarvoor is geautoriseerd.
1.6	Het toegangscontrolesysteem dient gebruiksvriendelijk te zijn.
1.7	Het toegangscontrolesysteem met al zijn componenten dient door meerdere partijen te kunnen worden geleverd, beheerd en onderhouden in het geval dat Opdrachtnemer niet meer aan het contract kan voldoen.
1.8	Het toegangscontrolesysteem met al zijn componenten dient overdraagbaar te zijn naar een andere partij m.b.t. leveringen, beheer en onderhoud na einde contract.
1.9	De Opdrachtnemer dient de huisregels van de Opdrachtgever in acht te nemen voor het betreden van haar terreinen en objecten. TiU is gerechtigd deze regels gedurende de looptijd te wijzigen. De Opdrachtnemer ontvangt na een eventuele wijziging een geactualiseerde versie van TiU, waarbij Opdrachtnemer zich per ommegaande conformeert aan de nieuwe regels. De huisregels zijn opgenomen in bijlage 12.
1.10	De Opdrachtgever kan te allen tijden de toegangscontrolecomponenten plaatsen en demonteren en de beheersoftware configureren.

2. Technische specificaties

2.1	De deursloten moeten geschikt zijn om passend geplaatst te worden in een eurocilinderuitsparing in de deur. Dit kunnen hele of halve cilinders zijn, in diverse lengten. Er zijn twee configuraties mogelijk: de elektronische ontgrendeling aan één of aan beide zijden. Bij éénzijdige elektronische ontgrendeling zal aan de andere zijde een knop dienen te zitten (knopcilinder).
2.2	Alle producten voldoen aan de geldende CE-voorschriften.
2.3	De veldcomponenten hebben minimaal een classificatie van IP65.

2.4	Alle aangeboden sloten hebben een inbraakbestendigheid van SKG***.
2.5	De communicatie tussen deurcontroller en autorisatielezer dient versleuteld/ encrypted te zijn. Zoals doormiddel van AES-encryptie of een encrypted protocol zoals OSDP of RS485.
2.6	De communicatie tussen centrale server en deurcontroller dient versleuteld/ encrypted te zijn via minstens 128 bits asymmetrische encryptie.
2.7	Indien het autorisatiemiddel van een batterij is voorzien, dient deze bij een lage resterende batterijcapaciteit door middel van een optisch signaal aan te geven dat de batterij vervangen dient te worden.
2.8	Het slot ondersteund ontgrendeling via het Mifare/Desfare protocol.

3. **Beheersoftware en autorisatie(middelen)beheer**

3.1	Beheer van het toegangscontrolesysteem dient door de Opdrachtgever zelfstandig op de eigen locatie plaats te kunnen vinden zonder tussenkomst van de Opdrachtnemer. De beheerapplicatie dient op meerdere werkplekken van de Opdrachtgever uitgevoerd te kunnen worden.
3.2	Het opvoeren, toekennen en wijzigen van autorisaties en verwijderen van autorisatiemiddelen dient door de Opdrachtgever zelfstandig plaats te kunnen vinden zonder tussenkomst van de Opdrachtnemer.
3.3	De software en gebruikershandleidingen dienen in de Nederlandse taal te zijn opgezet. Voor de gebruikers (bedieners van het toegangscontrolesysteem) dient een bedieninstructie in de Nederlandse taal te worden verzorgd.
3.4	Minimaal 5.000 gebruikers, beheerders en autorisatiegroepen dienen geconfigureerd te kunnen worden in de beheersoftware.
3.5	Alle gebruikers dienen gelijktijdig op de applicatie te kunnen inloggen en werken. Naast de gebruikers dient het eveneens mogelijk te zijn om met alle beheerders gelijktijdig te kunnen inloggen op de beheerdersapplicatie. Het inloggen door een beheerder dient geen invloed te hebben op het aantal gelijktijdige gebruikers die kunnen inloggen.
3.6	Aanmelden op basis van single sign-on.
3.7	Vanuit de beheersoftware dient het mogelijk te zijn (geanonimiseerde) gegevens en standaard rapporten uit te draaien inclusief mogelijkheid tot het aanpassen van de rapportagevorm naar eigen inzicht/ wens van Opdrachtgever, zoals filteren van autorisatiemiddel, tijdsvenster, locatie/ doorgang. Dit dient minimaal in .pdf, .xlsx en .csv formaat mogelijk te zijn.
3.8	Binnen het beheer dienen verschillende autorisatieniveaus geconfigureerd te kunnen worden op basis van ‘role-based access control (RBAC)’, zoals bijvoorbeeld toegangscontrolesysteembeheerder, beheerder autorisatiemiddelen, gebruiker.
3.9	Het dient mogelijk te zijn om autorisatieprofielen aan te maken waarmee een bundeling van autorisaties makkelijk en snel op een autorisatiemiddelen gezet kunnen worden.
3.10	Het dient mogelijk te zijn om autorisatieprofielen te stapelen.

3.11	Autorisaties inclusief tijdvensters dienen per autorisatiemiddel en autorisatiegroep toebedeeld te kunnen worden.
3.12	Autorisatiemiddelen dienen na een instelbare periode automatisch geblokkeerd te kunnen worden.
3.13	Elke toegangspoging dient geregistreerd te worden, zowel bij het aanbieden van een geautoriseerde autorisatiemiddel als een ongeautoriseerde.
3.14	Alle aanbiedingen, van een autorisatiemiddel, die worden geregistreerd en gelogd dienen voor een periode van 1 jaar bewaard te kunnen worden. De loggegevens zijn gedurende de bewaarperiode direct (zonder tussenkomst van Opdrachtnemer etc.) beschikbaar. Na de bewaarperiode dienen de loggegevens automatisch overschreven te worden. De bewaarperiode dient door Opdrachtgever zelf instelbaar te zijn.
3.15	De beheerder kan het cilinderslot te allen tijde in de ongeprogrammeerde toestand terugzetten, zodat deze kan worden (her)gebruikt.

4. Continuïteit

4.1	Software en hardware componenten van het toegangscontrolesysteem dienen 10 jaar na opdrachtgunning en opdrachtverlenging geleverd te kunnen worden, of één op één vervangen kunnen worden door een nieuw type / versie zonder extra kosten.
4.2	Toe te passen producten dienen voor tenminste 10 jaar na einde opdracht te kunnen worden onderhouden en uitgebreid.
4.3	Op basis van het afgesloten contract garandeert de Opdrachtnemer dat de applicatie, gedurende de contractperiode plus één jaar, doorontwikkeld en beschikbaar gesteld zal worden zonder additionele kosten. Onder deze doorontwikkeling wordt, naast additief, correctief en preventief onderhoud, ook verstaan dat op de applicatie adaptief onderhoud wordt uitgevoerd om te blijven voldoen aan de geldende wet- en regelgeving. Dit betreft software en firmware.
4.4	Bij nieuwe versies zijn de release notes voorzien van een duidelijke omschrijving van de aanpassingen. Bij nieuwe versies vanwege oplossing van fouten zijn de release notes voorzien van een duidelijke omschrijving van de oorzaak en oplossing. Security issues worden apart aangemerkt.
4.5	De aangeboden applicatie kent geen maatwerk om te voldoen aan de in dit document gestelde eisen. Als toch bepaalde functionaliteit specifiek voor deze aanbesteding is ontwikkeld, dan wordt deze in de eerstvolgende release opgenomen als standaardfunctionaliteit van de applicatie.

5. Support

5.1	Opdrachtnemer dient een passend opstartteam op te zetten waarbij een opstartmanager van Opdrachtnemer aangewezen wordt die gedurende de gehele implementatie betrokken blijft en als direct aanspreekpunt functioneert voor TiU. De opstartmanager dient gedurende de implementatieperiode telefonisch en per e-mail goed bereikbaar te zijn. In voorkomende gevallen dient de opstartmanager de dag volgend op een verzoek beschikbaar te zijn voor fysiek overleg. De opstartmanager dient tot minimaal vier (4) maanden, na start raamovereenkomst, betrokken te blijven.

5.2	De Opdrachtnemer dient in nauw overleg met de gebruiker de programmering van de beheersoftware te verzorgen voor ingebruikname. Inschrijver dient alle benodigde software volledig werkend te configureren. Inschrijver kan op verzoek van Opdrachtgever ondersteuning bieden bij het onderhouden en beheren van de software.
5.3	Voordat het toegangscontrolesysteem door Opdrachtnemer ter beschikking aan de gebruiker wordt gesteld, dient deze in bedrijf te worden gesteld en in het bijzijn van de Opdrachtgever te worden getest.
5.4	De digitale handleiding en hulpfunctie is volledig bij oplevering en wordt door de Opdrachtnemer bijgewerkt bij updates.
5.5	De Opdrachtnemer dient storingen conform het Storingsprotocol van de Tilburg University op te lossen. Het Storingsprotocol is opgenomen in bijlage 13.
5.6	De Opdrachtnemer dient een servicecontract aan te bieden voor het oplossen van storingen met een 24/7 actieve alarmopvolging conform het Storingsprotocol van de Tilburg University.
5.7	Opdrachtnemer zorgt voor het beschikbaar hebben van alle benodigde materieel om te kunnen voldoen aan het geldende Storingsprotocol.
5.8	Opdrachtnemer dient de gangbare reserveonderdelen, vervangingsonderdelen, gebruiks- en slijtage onderdelen op voorraad te houden gedurende de looptijd van het contract.
5.9	Inschrijver moet programmeer- en montage-ondersteuning aan kunnen bieden bij grootschalige aanpassingen die plaatsvinden bij nieuwbouw- en renovatieprojecten of grootschalige verhuizingen waarbij veel gebruikers betrokken zijn.

6. Interface

6.1	Het is gewenst dat voor ieder veldcomponentsoort een grafische gebruikersinterfacecomponent kan worden gemaakt waarop status, overige informatie en bedieningsknoppen worden gepresenteerd. Deze gebruikersinterface moet kunnen worden opgeroepen voor interactie met het veldcomponent. Het doel is de centralist een hoogst intuïtieve besturing van een veldcomponent te geven.
6.2	Het zal mogelijk zijn minimaal 15.000 locaties samen te stellen. De informatie over een locatie omvat tenminste: a. Type (bv. technische ruimte, kantoorruimte, algemene ruimte,...) b. Unieke naam en nummer van de locatie conform aanduiding Tilburg University.
6.3	Het dient mogelijk te zijn om plattegronden in PDF in te lezen.

7. **Eisen met betrekking tot de configuratie**

7.1	Het aantal aan te sluiten veldcomponenten is minimaal 15.000.
7.2	Het toegangscontrolesysteem moet programmeerbaar zijn en de volgende mogelijke bedrijfsstanden kennen: a. blokuren, tijdens de blokuren zijn de autorisatielezers van de betreffende deuren niet geactiveerd, passeren is voor iedereen mogelijk. b. normale situatie, elke autorisatielezer bepaalt op basis van de vastgestelde autorisatie of de aanbieder mag passeren.

8. **Eisen met betrekking tot de centrale en decentrale apparatuur**

8.1	De beheersoftware van het toegangscontrolesysteem dient gekoppeld te worden met het bestaande security management systeem (SMS/ PSIM). Hiervoor stelt de Opdrachtnemer kosteloos een goed werkende API beschikbaar.
8.2	Bij storingen/ uitval van de software dienen alle locaties zelfstandig te kunnen blijven functioneren. Deurcontrollers dienen zelfstandig op basis van de laatst geladen autorisaties voor uitval van het toegangscontrolesysteem toegang te kunnen geven of weigeren voor de gecontroleerde doorgangen.
8.3	Lokaal dient er een buffer aanwezig te zijn om alle gebeurtenissen vast te leggen tussen twee communicatiemomenten met de centrale toegangscontrolesysteem. Als buffer geldt minimaal 1.000 gebeurtenissen en handelingen met betrekking tot autorisatiemiddelen.
8.4	Per gebeurtenis dient minimaal de specifieke cilinder, specifieke sleutel, tijd en datum geregistreerd te worden en of de handeling het slot ontgrendeld of vergrendeld heeft.

9. Contractmanagement

9.1	Tussen Opdrachtgever en Opdrachtnemer wordt een Service Level Agreement (SLA) afgesloten. Opdrachtnemer stelt binnen 2 weken na definitieve gunning een SLA op gebaseerd op het Programma van Eisen en legt deze ter goedkeuring voor aan de Opdrachtgever.
9.2	Overleggen - Eén keer per jaar wordt een strategisch overleg gehouden om de langetermijn roadmap (1-2 jaar vooruit), de beveiligingsroadmap, strategische ontwikkelingen, status en verlenging van de Overeenkomst te bespreken. - Er wordt vier keer per jaar een tactisch overleg gehouden om de kwaliteit van de geleverde services, mogelijke serviceverbeteringen, ontwikkelingen op het gebied van beveiliging (incl. certificeringen), geïdentificeerde risico's en risicomanagement te bespreken. Tijdshorizon ca. 6 maanden. - Minimaal vier keer per jaar vindt een operationeel overleg plaats tussen de Product Owner van de Opdrachtgever en de Servicemanager van de Opdrachtnemer. Bespreken van analyse van en verbeteringen in het incident- en wijzigingsproces, beveiligingsincidenten, incidenten die niet binnen SLA zijn opgelost, geplande projecten of wijzigingen.

	De frequentie van deze bijeenkomsten kan in onderling overleg tussen Partijen worden aangepast.
9.3	Opdrachtnemer identificeert, classificeert, en beoordeelt risico's gedurende de looptijd van de overeenkomst, stelt beheersmaatregelen voor en informeert Opdrachtgever periodiek, maar ten minste ieder kwartaal, over de geïdentificeerde risico's en voorgestelde risico(beheers)maatregelen.
9.4	In geval van problemen in de beschikbaarheid en/of prestaties van de IT-Oplossing is Opdrachtnemer verplicht eigenaarschap te nemen om de oorzaak te onderzoeken en eigenaarschap te nemen in het oplossen van het probleem over de gehele keten van Opdrachtgever tot Opdrachtnemer.
9.5	Opdrachtnemer sluit een geheimhoudingsovereenkomst af met haar werknemers en eventuele derden die zij inschakelt.
9.6	De IT-Oplossing voldoet gedurende de looptijd van de raamovereenkomst aan de relevante geldende wet- en regelgeving (Adaptief onderhoud), zonder dat hiervoor additionele kosten in rekening worden gebracht aan de Opdrachtgever.
9.7	Als Opdrachtnemer nieuwe functionaliteit, nieuwe diensten en/of nieuwe technologie op de markt brengt, zullen deze (indien gewenst) direct beschikbaar zijn voor Opdrachtgever. Er zullen geen extra kosten in rekening worden gebracht voor deze functionaliteiten, diensten of nieuwe technologie, wanneer de toegevoegde functionaliteit een productlijn uitbreiding / ontwikkeling en/of verbetering van de IT-Oplossing betreft. In het uitzonderlijke geval dat dit niet het geval is zal Opdrachtnemer dit onderbouwen en dient Opdrachtgever eerst akkoord te gaan met de onderbouwing (inclusief marktconforme pricing) van Opdrachtnemer alvorens deze in gebruik wordt genomen. Indien Opdrachtgever niet akkoord gaat, is Opdrachtnemer verplicht het product aan te bieden voor de oorspronkelijk overeengekomen prijs, met de toegevoegde functionaliteit, diensten en/of technologie. Opdrachtgever zal niet op onredelijke gronden zijn akkoord onthouden.

10. Bruikbaarheid

10.1	Indien de IT-Oplossing een internet browser vereist, dan dient deze te voldoen aan Web Content Accessibility Guidelines (WCAG) niveau A en AA (als beschreven in EN 301 549).
10.2	Elke vorm van zichtbare communicatie en documentatie zoals, maar niet beperkt tot, schermen, rapporten en gebruikershandleidingen van de IT-Oplossing, zijn in de Nederlandse taal.
10.3	De IT-Oplossing toont informatieobjecten op elk aggregatieniveau binnen een redelijke termijn ongeacht de hoeveelheid informatieobjecten die in de IT-Oplossing aanwezig zijn: - Voor zoekopdrachten, schermwisselingen, simpele selecties een redelijke termijn is minder dan 2 seconden - Voor het genereren van complexe rapporten en overzichten is een redelijke termijn minder dan 15 seconden
10.4	Bruikbaarheidsheuristieken zijn toegepast om de gebruiksvriendelijkheid van de IT-Oplossing te stimuleren.

11. **Privacy en security**

11.1	Inschrijver beschikt over een privacy statement waarmee in duidelijke taal (in het Nederlands) betrokkenen worden geïnformeerd over de verwerking van persoonsgegevens door de contractpartij.
11.2	Inschrijver beschikt over een duidelijke procedure voor het behandelen van verzoeken met betrekking tot de rechten van betrokkenen.
11.3	Inschrijver beschikt over een duidelijke procedure voor het afhandelen van datalekken, waarbij Inschrijver nadat zij zelf kennis heeft genomen van een datalek, of een beveiligingsincident wat mogelijk een datalek kan zijn, de verwerkingsverantwoordelijke (Tilburg University) onverwijld op de hoogte brengt hiervan, uiterlijk binnen 24 uur nadat Inschrijver zelf kennis heeft genomen van het incident.
11.4	Inschrijver beschikt over een overzicht van de verwerkingsactiviteiten van persoonsgegevens die Inschrijver in het kader van de opdracht gaat uitvoeren, en verstrekt deze aan Tilburg University voorafgaand aan de voorlopige gunning. Per verwerkingsactiviteit is tevens aangegeven of de Inschrijver zich ziet als verwerkingsverantwoordelijke of als verwerker in de zin van de Algemene Verordening Gegevensbescherming.
11.5	Indien Opdrachtnemer (en eventuele Onderaannemer) persoonsgegevens verwerkt, wordt dit in beginsel alleen binnen de Europese Economische Ruimte (EER) gedaan. Zonder voorafgaande schriftelijke toestemming van TiU is het Opdrachtnemer - en eventueel door haar ingeschakelde Derden - niet toegestaan om persoonsgegevens te verwerken buiten de EER.
11.6	Inschrijver garandeert dat: a. het te leveren product/dienst is ontworpen op basis van de 'privacy by design'-waarborgen. b. het te leveren product/dienst is geconfigureerd op basis van de 'privacy by default'-waarborgen. c. het uitgangspunt van het te leveren product/dienst is dat er zo min mogelijk persoonlijke data wordt verzameld.
11.7	Het product/dienst maakt het mogelijk om verschillende bewaartermijnen te hanteren voor verschillende (categorieën van) persoonsgegevens.
11.8	Het product/dienst heeft de mogelijkheid om geautomatiseerd de gegevens op te schonen/verwijderen zodra de bewaartermijn voor de betreffende gegevens is verstreken.
11.9	Inschrijver dient te voldoen aan de eisen die gesteld zijn in het SURF Juridisch Normenkader (Cloud) services (JNK) en zorgt dat de inrichting blijvend aan deze eisen voldoet. De eisen zijn te vinden op: https://www.surf.nl/files/2019-01/surf_c-handreiking-beveiligingsmaatregelen---bijlage-c---versie-mei-2018.pdf
11.10	Inschrijver garandeert dat het applicatielandschap en gegevensuitwisseling blijvend voldoet aan de minimale veiligheidseisen als opgenomen in de Security Technical IT Checklist (STITCH). Inschrijver aan wie de opdracht voorlopig is gegund dient voor ondertekening van de raamovereenkomst aan te tonen aan de STITCH voorwaarden te voldoen. De bewijsvoering om te voldoen aan STITCH ligt bij Inschrijver. Inschrijver kan dit aantonen middels een pen test rapport of security rapport.

11.11	Inschrijver stemt er mee in dat de Aanbestedende Dienst de mogelijkheid heeft tot het uitvoeren van een veiligheidsaudit na voorlopige gunning en tijdens de looptijd van de overeenkomst door het CERT team van de Aanbestedende Dienst. Inschrijver verleent hieraan volledige medewerking.
11.12	Hosting vindt plaats binnen de EEA (European Economic Erea)/ Europese Economische Ruimte (EER).

12. IT-systeemveerkracht en -betrouwbaarheid

12.1	De IT-Oplossing wordt 24/7 gemonitord door Opdrachtnemer. Indien incidenten of defecten optreden, zal Opdrachtnemer actie ondernemen, een prioriteit toekennen en Opdrachtgever informeren in geval van P1, beveiligings- en/of privacy incidenten.
12.2	De RTO (Recovery Time Objective) van de IT-Oplossing is maximum 4 uur. Opdrachtnemer garandeert een Maximum Tolerable Downtime (MTD) van 12 uur.
12.3	De RPO (Recovery Point Objective) van de (gegevens in de) IT-Oplossing is maximaal 24 uur in 99,95% van de gevallen. Opdrachtnemer maakt minimaal één keer per dag back-ups van alle gegevens in de IT-Oplossing. Dit back-upproces mag de prestaties van de IT-Oplossing niet beïnvloeden. Opdrachtnemer zal back-ups opslaan op een geografisch andere locatie dan waar de primaire gegevens van de IT-Oplossing is opgeslagen. Opdrachtgever mag Opdrachtnemer te allen tijde verzoeken om gegevens uit de back-up beschikbaar te stellen. Er zullen hierover nadere afspraken gemaakt worden.
12.4	De Beschikbaarheid, Prestatie en Onderhoud van de IT-Oplossing moeten worden gewaarborgd (bv. graceful degradation, redundantie of automatische rollback mechanismen). Dit betekent ook dat eventueel herstel van gegevens en clouddiensten wordt gefaciliteerd door infrastructuur en (ondersteunende) IT-diensten die robuust en redundant zijn en die periodiek en aantoonbaar door Opdrachtnemer worden getest.
12.5	Opdrachtnemer heeft een disaster recovery procedure / plan en een rollback procedure voor de IT-Oplossing gedocumenteerd en getest. Op verzoek levert Opdrachtnemer documentatie aan Opdrachtgever en/of geeft instructie over stappen die Opdrachtgever dient te nemen in het geval een ramp of rollback scenario zich voordoet.
12.6	Onderhoud zal minimaal 10 werkdagen voorafgaand aan het onderhoud worden aangekondigd aan Opdrachtgever. Onderhoud wordt gepland in samenspraak met Opdrachtgever. Onderhoud met downtime is niet toegestaan tijdens tentamenperiodes als beschreven in de Opdrachtgevers' kalender van het academisch jaar.
12.7	Onderhoudsactiviteiten aan het toegangscontrolesysteem dienen parallel aan operationele processen uitgevoerd te kunnen worden, zonder verstoring van die operationele processen. Daaronder valt tenminste: het maken van back-ups, het opschonen van logbestanden en het inladen van nieuwe data.

13. Datamanagement & -opslag

13.1	De IT-Oplossing beschikt over een niet muteerbare audittrail waarbij minimaal de volgende metadata automatisch opgeslagen worden: - inhoud uitgevoerde mutatie - gebruiker die de handeling uitvoert - of het een (on)geautoriseerde handeling is - datum en tijd van de uitvoering van de mutatie
13.2	De IT-Oplossing exporteert informatieobjecten en (meta)data in duurzame, valideerbare en volledig gedocumenteerde formaten (bijvoorbeeld TXT, CSV, XML, JSON), die voldoen aan open standaarden en kan zelfstandig door Opdrachtgever worden uitgevoerd.
13.3	De IT-Oplossing moet de samenhang tussen informatieobject en bijhorende metadata op elk aggregatieniveau garanderen tot het moment van verwijderen.
13.4	De IT-Oplossing importeert, converteert, migreert en exporteert informatieobjecten en de bijbehorende metadata uitsluitend zonder aantasting van de authenticiteit, betrouwbaarheid, integriteit en bruikbaarheid op elk aggregatieniveau.
13.5	De IT-Oplossing kan blijvend te bewaren informatieobjecten, indien deze zich in de IT-Oplossing bevinden, inclusief de metadata exporteren in een duurzaam te bewaren bestandsformaat minimaal PDF, of XML/JSON als tweede keus.
13.6	De IT-Oplossing moet informatie definitief vernietigen na afloop van de in de IT-Oplossing vastgelegde bewaartermijn. Opdrachtgever kan per (groep) informatieobjecten een (specifieke) bewaartermijn instellen. Elke vernietiging wordt geregistreerd in een exporteerbaar logbestand. Het logbestand bevat minimaal de volgende metadata: objectnaam, objectid, creatiedatum, vernietigingsdatum, eigenaar bestand, onderwerp, bewaartermijn.
13.7	De IT-Oplossing kan versiebeheer toepassen op een opgeslagen informatieobject, zodat de gebruiker inzicht heeft in de wijzigingen aan het informatieobject.
13.8	De Opdrachtnemer (indien verwerker) draagt bij het einde van de Overeenkomst alle gegevens over aan Opdrachtgever en/of vernietigt deze (naar wens van Opdrachtgever) en bewaart of behoudt geen gegevens voor eigen doeleinden.
13.9	De IT-Oplossing biedt de mogelijkheid om het verwerken van Persoonsgegevens die niet strikt noodzakelijk zijn, te voorkomen bijvoorbeeld door functionaliteit uit te schakelen (dataminimalisatie).
13.10	De werking van de IT-Oplossing kan worden getest zonder gebruik te maken van echte persoonsgegevens.

14. IT-systeemarchitectuur

14.1	De IT-Oplossing wordt in principe in de cloud (SaaS/PaaS/IaaS) geleverd.
14.2	De IT-Oplossing ondersteunt gedurende de looptijd van de overeenkomst clients op alle door Microsoft ondersteunde operating systemen die mainstream support hebben.
14.3	Indien de IT-Oplossing een internet browser vereist, dan dient deze compatible zijn en werken op minimaal de één na laatste major-release (n-1) van de 5 meest gangbare internet browsers, als gepubliceerd op statcounter.com (browser marketshare worldwide, van de laatste 12 maanden) en op alle versies daarvan die nog steeds ondersteund worden en secure zijn conform de opgaaf van de leverancier van de browser gedurende de gehele looptijd van de overeenkomst.
14.4	Voor de werking van de IT-Oplossing heeft een eindgebruiker geen proprietary of uitgefaseerde technologieën nodig waaronder, maar niet beperkt tot, Adobe Flash, Microsoft Silverlight, Java (corporation) applets, ActiveX applicaties.

15. Identiteit en toegangsmanagement

15.1	Webgebaseerde single sign-on (SSO) is mogelijk en wordt ondersteund via OpenIDConnect (OAuth) / SAML v2-protocol en is gekoppeld aan SURFconext/AzureAD/EntraID.
15.2	Wanneer (omgevingen van) de IT-Oplossing worden geupdate, voorzien van een nieuwe release of nieuwe data/Gegevens, blijven alle instellingen (authenticatie/connection string/usernames/passwords/tokens/etc.) gelijk ten opzichte van voor de update/release/verversing van Gegevens.
15.3	De IT-Oplossing ondersteunt (open) API's (REST etc.) om integratie tussen de Identity Governance and Administration applicatie en de IT-Oplossing mogelijk te maken voor provisioning en de-provisioning.
15.4	Voor veilige communicatie met de IT-Oplossing en IGA-applicatie mogen VPN-tunnels niet vereist zijn.
15.5	De IT-Oplossing moet een CSV (bestand) export of een combinatie van CSV exports van alle autorisatie-informatie (gebruikers, rollen, rechten etc.) ondersteunen zodat de IGA-applicatie role-mining kan uitvoeren.

16. Integratie

16.1	Opdrachtnemer levert ondersteuning bij realisatie van koppelingen met het integratieplatform van de Opdrachtgever. Onder ondersteuning wordt verstaan: deskundige en tijdige technische informatievoorziening en samenwerking met Opdrachtgever teneinde de koppelingen te kunnen realiseren.
16.2	Om data via koppelingen van de IT-Oplossing naar het integratieplatform van Opdrachtgever te ontsluiten ondersteunt de IT-Oplossing event-driven integratie óf stelt de IT-Oplossing API’s ter beschikking. Event-driven integratie houdt in dat de IT-Oplossing automatisch verbinding maakt met het data-integratieplatform van de Opdrachtgever. Dit gebeurt telkens wanneer er belangrijke

	gebeurtenissen plaatsvinden, zoals het aanmaken, bijwerken of verwijderen van relevante gegevens binnen de IT-Oplossing.
16.3	Dataverkeer van de IT-Oplossing naar Opdrachtgever wordt vanaf een beperkte set IP-adressen (<20) geïnitieerd zodat IP-filtering in te richten is door Opdrachtgever.
16.4	De documentatie van elke API van de IT-Oplossing is duidelijk en actueel en bevat minimaal het volgende: • URL's van de verschillende webservices • Dataformaat dat de webservices leveren / verwachten • Voorbeelden van de responses en responsecodes • Lijst van mogelijke foutcodes en wat deze betekenen • Gebruikte authenticatie en evt. autorisatie
16.5	De gegevens die via de API's van de IT-Oplossing worden geleverd / verzonden bestaan uit gegevens in XML of JSON formaat.
16.6	De structuur van de gegevens die door de IT-Oplossing worden verzonden of ontvangen, wordt beschreven in ofwel XSD's (in het geval van XML-gegevens) of JSON-schema's (in het geval van JSON-gegevens), zodat de gegevens gevalideerd kunnen worden.
16.7	De API's van de IT-Oplossing zijn beveiligd door middel van authenticatie die geen gebruikersinteractie vereist (system-to-system). De API's van de IT-Oplossing zijn bij voorkeur beveiligd door één van de volgende methoden: • HTTP basic authentication • Static API key • OAuth m.b.v. de volgende flows o Credentials Grant o Password Grant
16.8	API's beschikbaar gesteld door de IT-Oplossing werken middels REST of SOAP 1.1. De resultaten van de requests voldoen aan standaard http codes en/of conform de SOAP-standaard (Web Service/WCF Service over https) of REST XML/JSON (HTTP GET, HTTP POST, HTTP PUT, HTTP DELETE) over HTTPS.
16.9	Wanneer er een limiet is op het aantal verzoeken dat de API mag verwerken, kan de Opdrachtnemer dit kosteloos aanpassen.
16.10	Wanneer throttling wordt afgedwongen, passen de API's van de IT-Oplossing throttling per account/credential set toe. Dit betekent dat er voor elke koppeling een aparte credential wordt aangemaakt. Hierdoor heeft een piek in verzoeken op de ene interface geen invloed op de verzoeken van een andere interface. Er wordt geen throttling toegepast wanneer dit niet nodig is.
16.11	De API's van de IT-Oplossing zijn voorzien van versionering zodat bij een wijziging in de API een nieuwe versie van de API ter beschikking wordt gesteld onder een andere URL, bijvoorbeeld V1: http://systeem.leverancier.nl/api/v1/entiteit/.. V2: http://systeem.leverancier.nl/api/v2/entiteit/..
16.12	Indien de IT-Oplossing versionering op de API's ondersteunt wordt een oude versie van de API voor tenminste twee maanden ondersteund alvorens deze door de Opdrachtnemer wordt uitgefaseerd.
16.13	Indien de IT-Oplossing geen versionering van de API's ondersteunt heeft de Opdrachtgever de mogelijkheid om een wijziging voor tenminste twee maanden niet in productie te nemen zodat de wijziging in deze tijd in het integratieplatform van de Opdrachtgever kan worden geïmplementeerd.

16.14	Wijzigingen in de API's van de IT-Oplossing mogen er niet toe leiden dat functionaliteit die door Opdrachtgever wordt gebruikt (deels) niet meer beschikbaar is.
16.15	De IT-Oplossing verwerkt de statuscode en is in staat om het bericht op een later moment alsnog aan te bieden, waarbij de berichtvolgorde wordt gerespecteerd.
16.16	Wanneer een bericht van de IT-Oplossing niet kan worden afgeleverd bij het integratieplatform van Opdrachtgever, dan biedt de IT-Oplossing dit bericht op een later moment alsnog aan tot het correct is afgeleverd.
16.17	De IT-Oplossing ondersteunt het verzenden van de huidige staat van alle gegevens via de bestaande interface met het integratieplatform wanneer daarom wordt gevraagd (initiële belasting).
16.18	Als de gegevensstructuur en/of de uitgaande berichten die door de IT-Oplossing wordt verzonden verandert, wordt de Opdrachtgever hiervan ten minste twee maanden van tevoren op de hoogte gesteld, zodat de Opdrachtgever zich kan aanpassen aan de veranderingen.
16.19	De API beschikt over een heart beat service om de beschikbaarheid te monitoren.
16.20	Documentatie over het entiteitrelatiemodel (ERD) wordt beschikbaar gesteld aan de Opdrachtgever. Er is een duidelijke definitie per gegevenstabel en hoe alle tabellen aan elkaar gerelateerd zijn via primaire sleutels.
16.21	Als de IT-Oplossing de Opdrachtgever in staat stelt om vrije velden en/of aangepaste velden te gebruiken, dan moeten deze velden ook door de Opdrachtnemer beschikbaar worden gemaakt/gesteld in de API.
16.22	De IT-Oplossing kan data aanbieden op basis van geneste / hiërarchische datastructuren.
16.23	De API voor de benodigde koppelvlakken is volledig ontwikkeld door de Opdrachtnemer bij aanvang van de implementatie van de IT-Oplossing.

17. Programmamanagement

17.1	Opdrachtnemer biedt een help/service/supportdesk waar Opdrachtgever rechtstreeks contact mee kunnen opnemen en die beschikbaar is van 8 uur tot minimaal 17 uur op werkdagen.
17.2	De Opdrachtnemer biedt Opdrachtgever toegang tot zijn service managementportaal, wat de Opdrachtgever in staat stelt om incidenten te melden, feature requests in te dienen en de status van wijzigingen, problemen en incidenten te volgen. Het portaal bevat een specifiek veld wat een verwijzing naar het kenmerk van het ticketing systeem van Opdrachtgever en/of een API interface die linkt naar het ticketing Systeem van Opdrachtgever, wat het effectief tracken en bijhouden van verzoeken faciliteert.
17.3	Medewerkers van de Opdrachtnemer, die in contact treden met Opdrachtgever beheersen de Engelse en Nederlandse taal in woord en geschrift.
17.4	Onderhoud en ondersteuning op de IT-Oplossing zijn gegarandeerd gedurende de looptijd van de overeenkomst. Dit is vastgelegd in een SLA, waarbij de IT-Oplossing wordt aangeboden op minimaal de één na laatste major-release (n-1).

17.5	Updates en upgrades van de IT-Oplossing worden gepland door de Opdrachtnemer in overleg met Opdrachtgever, en worden niet gepusht door Opdrachtnemer. In alle gevallen dienen updates/upgrades ten minste 14 kalenderdagen (waarvan 8 werkdagen) van tevoren te worden aangekondigd en vergezeld te gaan van release notes. Uitzonderingen gelden voor updates en upgrades die nodig zijn vanwege noodsituaties op het gebied van beveiliging en privacy.
17.6	In het geval van maatwerk of configuratie van (onderdelen van) de IT-Oplossing voor de Opdrachtgever, wordt de continuïteit van dit maatwerk en/of configuratie gegarandeerd door Opdrachtnemer in releases, updates en upgrades.
17.7	Naast de productieomgeving van de IT-Oplossing dient Opdrachtnemer ten minste een dedicated ontwikkelomgeving, testomgeving en acceptatieomgeving voor Opdrachtgever te verzorgen.
17.8	Gegevens overdracht van de Productie- (P) naar de Acceptatie- (A) omgeving van de IT-oplossing moet mogelijk zijn. Gegevensoverdracht tussen de Test- (T) en Ontwikkelomgeving (O) moet mogelijk zijn. T/O en A/P moeten van elkaar gescheiden en geïsoleerd zijn om de veiligheid te verbeteren en fouten te voorkomen.
17.9	De IT-Oplossing biedt gedetailleerde logging mogelijkheden. Logging kan worden gefiltered op basis van ernst en type/categorie (bv. informatie, warning, error, security, privacy, performance etc.)
17.10	Opdrachtnemer voert periodiek, ten minste iedere twee jaar, onafhankelijke security/privacy/compliance/configuratie audits uit op zijn omgeving. Opdrachtnemer voert audits uit in overeenstemming met het door Opdrachtnemer gespecificeerde normatieve kader, zoals gedocumenteerd in de Verwerkersovereenkomst en/of Overeenkomst. Opdrachtnemer deelt de auditbevindingen met Opdrachtgever. Opdrachtnemer zal aanbevelingen van de auditor zo snel mogelijk implementeren.
17.11	De Opdrachtnemer verstrekt op verzoek van de Opdrachtgever aan Opdrachtgever een exit strategie of data retransitie plan voor de Gegevens van de Opdrachtgever. De vereisten als omschreven in de EU Data Act zijn van toepassing. De Opdrachtnemer moet aantoonbaar voldoen aan de verplichtingen van (hoofdstuk VI) Data Act, en de Opdrachtgever in staat stellen om veilig, kosteloos en interoperabel toegang te krijgen tot de Data van Opdrachtgever en over te stappen naar een andere aanbieder / leverancier.

18. Beveiliging

18.1	Indien de IT-Oplossing encryptie van informatieobjecten in ruste toepast, moet dit altijd omkeerbaar zijn, zodat het oorspronkelijke, onversleutelde informatieobject weer beschikbaar komt bij decryptie. Encryptiesleutels liggen (ook) altijd bij Opdrachtgever.
18.2	Het autorisatiebeheer kan afdwingen dat gebruikers alleen toegang hebben tot informatie die strikt nodig is voor de uitvoering van hun werkzaamheden, met duidelijke begin- en einddatum.
18.3	Alleen als de IT-Oplossing lokale usernames/passwords ondersteunt (buiten SSO): Wachtwoorden (bijvoorbeeld serviceaccounts) voldoen aan het wachtwoordbeleid van Opdrachtgever en kunnen bijvoorbeeld periodiek worden gewijzigd met beperkte impact.

18.4	Opdrachtgever zal mogelijk, bijvoorbeeld als onderdeel van de acceptatieprocedure van de IT-Oplossing, voor eigen rekening door een daartoe gecertificeerd bedrijf een attack- and penetration test uit laten voeren. Opdrachtnemer dient hieraan mee te werken. De pentest dient te worden uitgevoerd door een natuurlijk persoon, een automatisch gegenereerde attack and penetration test is onvoldoende.
18.5	De IT-Oplossing dient (t.a.v. informatiebeveiliging) aantoonbaar te voldoen aan marktconforme certificering, bijvoorbeeld ISO27001 of gelijkwaardig, of toont dit minimaal elke 2 jaar aan middels het ROSA self assessment dat correspondeert met de BIV classificatie van de IT-Oplossing.
18.6	De beveiligingsmaatregelen bij de Opdrachtnemer zijn aantoonbaar volgens de systematiek ISO 27001 of SOC 2 type II ingevoerd.
18.7	De verbinding met de IT-Oplossing is te allen tijde versleuteld. Veilige encryptie wordt beoordeeld aan de hand van de 'SSL Labs Server Test' score (https://www.ssllabs.com), waarbij een minimale score van A vereist is. Daarnaast wordt er een test uitgevoerd op http://www.internet.nl/ en worden de resultaten geëvalueerd en indien nodig besproken met de Opdrachtnemer.

19. **Eisen ten aanzien van facturering**

19.1	Facturatie vindt plaats door middel van één elektronische factuur per geleverde bestelling via PEPPOL, of in UBL 2.1 versie in .xml met maximaal 1 factuur per bestand. De factuur dient gestuurd te worden naar e-invoices@tilburguniversity.edu.
19.2	Op de factuur dient vermeld te worden: a. Proactis ordernummer. b. Budgetcode/naam besteller c. Contractnummer d. Geleverde Diensten e. Contactpersoon Tilburg University Indien van toepassing, Tilburg University's BTW nummer (NL002791250B01)
19.3	Betaling door Opdrachtgever geschiedt binnen 30 dagen na ontvangst en goedkeuring van de factuur.
19.4	De factuur dient te voldoen aan de wettelijke gestelde eisen en moet worden voorzien van elementen genoemd in de hiervoor opgenomen eis 20.2. Facturen zonder deze kenmerken worden geretourneerd.

Naast bovenstaande minimum eisen voor een elektronisch sluitsysteem heeft de Opdrachtgever een drietal optionele wensen; een online elektronisch sluitsysteem, smartphone comptabiliteit en een batterijloos sluitsysteem. Onderstaande minimum eisen zijn alleen van toepassing als de desbetreffende optie door de Opdrachtnemer wordt aangeboden.

20. **Smartphone comptabiliteit (optioneel)**

20.1	Tijdelijke toegangsrechten kunnen op een smartphone met een Android en Apple IOS besturingssysteem gezet worden.
20.2	De mobiele applicatie is gratis verkrijgbaar in de appstore van Apple en Google.
20.3	Elke gebruiker heeft een unieke identificatie en kan individueel worden ontgrendeld en vergrendeld.
20.4	Autorisatielezers zijn beveiligd tegen manipulatie van tijd op smartphone.
20.5	Toegangsrechten zijn tijdgebonden.
20.6	Toegangsrechten zijn niet overdraagbaar naar andere smartphones.

21. **Online toegangscontrolesysteem (optioneel)**

21.1	Het toegangscontrolesysteem dient geschikt te zijn om zowel online als offline toepassingen (binnen één systeem) toe te passen.
21.2	Het online deel werkt via WiFi of 4G/5G en heeft dus geen gebouwgebonden data-aansluiting nodig om volledig te functioneren.
21.3	Bij uitval van de communicatie met de centrale server dient lokaal de toegangscontrole ongehinderd te blijven functioneren voor tenminste 3 uur. Deurcontrollers dienen zelfstandig op basis van de laatst geladen autorisaties voor uitval van het toegangscontrolesysteem toegang te kunnen geven of weigeren voor de gecontroleerde doorgangen.
21.4	Bij toepassing van computers voor de beveiligingssystemen dienen de interne systeemklokken allemaal gelijk te lopen d.m.v. radiografisch gestuurde tijdcorrectie, zodat de logfiles gegarandeerd de juiste tijd vermelden.
21.5	Het dient mogelijk te zijn om vluchtwegen, aanvalswegen en vluchtplannen ook vanuit het TCS te openen in geval van calamiteiten.
21.6	Op de plattegrond in de interface zullen minimaal de volgende statusmeldingen van een doorgang van het toegangscontrolesysteem kunnen worden getoond: a. Deur status (geopend / gesloten) b. Naam en personeelsnummer van autorisatiemiddelhouder die op basis van een autorisatiemiddel toegang is verleend. c. Lijst van overbrugde toegangen, toegangen in storing, en dergelijke.
21.7	Het zal mogelijk zijn om vanuit de interface: a. Een autorisatiemiddel te blokkeren b. Een deur te openen, te sluiten en/of te overbruggen

21.8	Het toegangscontrolesysteem moet programmeerbaar zijn en de volgende mogelijke bedrijfsstanden kennen: a. Tijden van alertheid, tijdens deze periode zijn bepaalde, vooraf aangewezen autorisatielezers bij de betreffende deuren uitgeschakeld voor bepaalde autorisatiegroepen. Voor het verkrijgen van toegang is dan tussenkomst van de meldkamer noodzakelijk.

22. **Batterijloos (optioneel)**

22.1	Het slot genereert zelfstandig de benodigde energie, zonder hulp van een stroomaansluiting of batterij (in slot of sleutel).