Bijlage 10 - Programma van Eisen

Onderdeel uitmakend van de aanbesteding Software voor Management & Beveiliging Digitale Toetswerkplekken met kenmerk TiU/AS08226

Algemeen

Nummer	Eis
1.	Inschrijver dient in te stemmen met de voorwaarden van de definitieve conceptovereenkomst (inclusief bijlagen), voorzien van de wijzigingen hierop die voortvloeien uit de nota van inlichtingen.
2.	Inschrijver is gelet op de aard van de opdracht een Verwerker en verwerkt alleen persoonsgegevens binnen de Europese Economische Ruimte (EER). Inschrijver dient in te stemmen met de voorwaarden van de definitieve concept verwerkersovereenkomst (inclusief bijlagen), voorzien van de wijzigingen hierop die voortvloeien uit de nota van inlichtingen.
3.	Inschrijver dient in te stemmen met de Service Level Agreement (SLA), zie bijlage 3
4.	Inschrijver dient te garanderen dat gedurende de uitvoering van de Opdracht door alle werknemers en ingezette derden welke zorg dragen voor de uitvoering van de Opdracht in de contacten met de Aanbestedende Dienst de Nederlandse of Engelse taal in woord en geschrift zal worden gebruikt. Tevens verklaart Inschrijver dat bij de uitvoering van de Opdracht alle documenten in de Nederlandse taal zijn opgesteld, met uitzondering van de technische documentatie (niet zijnde de gebruikershandleiding) welke in het Engels mag zijn opgesteld.
5.	Alle bij de uitvoering van de opdracht betrokken medewerkers conformeren zich aan de geldende huisregels van Tilburg University: https://www.tilburguniversity.edu/nl/contact/huisregels
6.	Alle bij de uitvoering van de opdracht betrokken medewerkers conformeren zich aan de geldende code of conduct van Tilburg University: https://www.tilburguniversity.edu/nl/over/gedrag-integriteit/code-conduct
7.	De Opdrachtnemer stelt zich actief op ten aanzien van de implementatie van best practices, gedragscodes, aanbevelingen of relevante standaarden van overheidsinstanties in de IT-Oplossing (verenigingen, brancheorganisaties of gebruikersgroepen). Minimaal worden de normen eduStandaard, HORA, HOSA en eduHub geïmplementeerd.

Eisen Facturering

Nummer	Eis
8.	Facturatie vindt plaats door middel van een elektronische factuur per Purchase Order. De elektrische factuur dient ontvangen te worden via: - PEPPOL of

	- UBL 2.1 versie met maximaal 1 factuur per bestand; dit bestand kan worden gestuurd naar e-invoices@tilburguniversity.edu
9.	Op de factuur dient vermeld te worden: - Purchase Ordernummer - Contractnummer - Naam besteller/opdrachtgever - Geleverde diensten - Factuurnummer - Factuurdatum - Indien van toepassing Tilburg University's VAT number (NL002791250B01)
10.	Als een Purchase Ordernummer bestaat uit meerdere regels, dient op de factuur elke regel separaat te worden opgenomen
11.	Betaling door opdrachtgever geschiedt binnen 30 dagen na ontvangst en goedkeuring van de factuur.
12.	De factuur dient te voldoen aan de wettelijke gestelde eisen en moet worden voorzien van elementen genoemd in de hiervoor opgenomen Eis. Facturen zonder deze kenmerken worden geretourneerd.
13.	Facturen op basis van alleen een budgetcode en/of een naam zullen niet geaccepteerd worden en zullen worden teruggestuurd naar de leverancier met het verzoek om alsnog de opdrachtgever een Purchase Order te laten maken.

Eisen privacy en security

Nummer	Eis
14.	Inschrijver beschikt over een privacy statement waarmee in duidelijke taal (en in ieder geval in het Engels, maar bij voorkeur ook in het Nederlands) betrokkenen worden geïnformeerd over de verwerking van persoonsgegevens door de contractpartij.
15.	Inschrijver beschikt over een duidelijke procedure voor het behandelen van verzoeken met betrekking tot de rechten van betrokkenen.
16.	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.
17.	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.
18.	Inschrijver garandeert dat: - het te leveren product/dienst is ontworpen op basis van de 'privacy by design'-waarborgen. - het te leveren product/dienst is geconfigureerd op basis van de 'privacy by default'-waarborgen. - het uitgangspunt van het te leveren product/dienst is dat er zo min mogelijk persoonlijke data wordt verzameld.
19.	Het product/dienst maakt het mogelijk om verschillende bewaartermijnen te hanteren voor verschillende (categorieën van) persoonsgegevens.
20.	Het product/dienst heeft de mogelijkheid om geautomatiseerd de gegevens op te schonen/verwijderen zodra de bewaartermijn voor de betreffende gegevens is verstreken.
21.	Hosting vindt plaats binnen de EEA. óf Indien er sprake is van doorgifte buiten de EER (opslag buiten EER en/of toegang vanuit buiten EER), dient een juist doorgifte mechanisme van kracht te zijn voor gelijkwaardige nationale rechtsbescherming. Indien er geen internationaal adequaatheidsbesluit of certificeringsmechanisme van toepassing is, zal de Standard Contractual Clause (SCC) conform het model van de Europese Commissie vaak de meest voor de hand liggende vorm zijn voor het doorgifte mechanisme. Voorwaarde is dat contractpartij kan beargumenteren dat deze SCC kan worden nagekomen en dit toetsbaar is.
22.	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
23.	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 Overeenkomst 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
24.	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.

	Opdrachtnemer dient jaarlijks een actueel en onafhankelijk afgegeven ISAE 3402 Type II-rapport te overleggen.
25.	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. Bij data in transit is minimaal TLS versie 1.2 vereist. TLS 1.3 heeft de voorkeur. Bij data at rest is AES-256 vereist.
26.	Het autorisatiebeheer zal afdwingen dat gebruikers alleen toegang hebben tot informatie die strikt nodig is voor de uitvoering van hun werkzaamheden, met duidelijke begin- en einddatum.
27.	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.
28.	Tijdens de bouw en het onderhoud van de IT-Oplossing is de actuele OWASP top-10 meegenomen als een must have. Indien de Opdrachtnemer van de OWASP aanbevelingen afwijkt, wordt de Opdrachtgever geïnformeerd. Periodiek wordt de OWASP compliance geherevalueerd door de Opdrachtnemer.
29.	De Opdrachtnemer zal minimaal 1x per dag controleren of de verbinding voldoende veilig is en is in staat om dit, op verzoek van de Opdrachtgever, in een rapportage inzichtelijk te maken.

Eisen exit-plan

Nummer	Eis
30.	Opdrachtnemer stelt uiterlijk 6 maanden na inwerkingtreding van deze overeenkomst, een exitplan op ter goedkeuring door opdrachtgever.
31.	Het exitplan bevat ten minste bepalingen over: a) Overdracht van kennis en documentatie, waaronder systeemdocumentatie, gebruikershandleidingen, configuratiebestanden en operationele procedures; b) Informatiebeveiliging en dataprivacy, inclusief maatregelen voor het veilig overdragen, anonimiseren of verwijderen van persoonsgegevens en vertrouwelijke informatie conform de geldende wet- en regelgeving (zoals de AVG); c) Beheer en overdracht van assets, waaronder hardware, softwarelicenties, accounts, certificaten, en overige bedrijfsmiddelen die in gebruik zijn voor de dienstverlening; d) Fysieke toegang en sleutelbeheer, inclusief intrekking van toegangsrechten, retour van sleutels, badges en eventuele bedrijfseigendommen; e) Continuïteitsborging, waaronder afspraken over ondersteuning tijdens de overgangsperiode en beschikbaarheid van personeel voor kennisoverdracht;

	f) Samenwerking met de nieuwe Opdrachtnemer, inclusief verplichtingen om redelijke assistentie te verlenen bij de transitie zonder onredelijke vertraging of extra kosten (behoudens vooraf overeengekomen vergoedingen); g) Tijdsplanning en verantwoordelijkheden, met duidelijke termijnen en toewijzing van taken aan beide partijen; h) Verwijdering of vernietiging van data en materialen, met schriftelijke bevestiging aan de Opdrachtgever.
32.	Op verzoek van opdrachtgever zal opdrachtnemer het goedgekeurde exitplan uitvoeren binnen de overeengekomen termijn. Opdrachtnemer zal daarbij handelen met dezelfde zorgvuldigheid en kwaliteit als tijdens de uitvoering van de overeenkomst.
33.	Na beëindiging blijft Opdrachtnemer, gedurende een periode van drie maanden, op redelijk verzoek van opdrachtgever of de nieuwe opdrachtnemer, reageren voor toelichting of aanvullende overdracht van kennis, mits deze verzoeken redelijkerwijs verband houden met de beëindigde dienstverlening.
34.	Opdrachtgever heeft het recht om de correcte uitvoering van het exitplan te verifiëren, waaronder het recht op inzage in bewijs van verwijdering van data en intrekking van toegangsrechten.

Eisen Identity and Access Management (IAM)

Nummer	Eis
35.	De IT-Oplossing ondersteunt de open SCIM-standaard ter ondersteuning van leesrollen en groepen door de IGA-applicatie.
36.	Webgebaseerde single sign-on (SSO) is mogelijk en wordt ondersteund via <OpenIDConnect (OAuth) / SAML v2-protocol> en is minimaal gekoppeld aan <SURFconext/AzureAD/of naam van een andere SAML- of openID provider in gebruik bij de Opdrachtgever>.
37.	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.
38.	Voor veilige communicatie met de IT-Oplossing <en IGA-applicatie> mogen VPN-tunnels niet vereist zijn.
39.	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.
40.	De Opdrachtnemer integreert voor two factor authenticatie (2FA) met het <SURFsecureID/EntraID/...> platform. De Opdrachtnemer is niet verplicht om 2FA-tokens of mechanismen aan te leveren, aangezien dit wordt beheerd door <SURFsecureID op het SURFconext-platform>. De IT-Oplossing moet 2FA kunnen initiëren via Levels of Assurance (LoA). De Opdrachtnemer regelt dit op verzoek van de Opdrachtgever, die hierbij de sessieduur (geldigheidsduur van het token) specificeert.
41.	De IT-Oplossing ondersteunt step up authenticatie voor specifieke, configureerbare rollen.
42.	De IT-Oplossing ondersteunt step up authentication op voor specifieke, configureerbare schermen en/of functies.

43.	De IT-Oplossing biedt een provisioning- en deprovisioning API die zowel pre-provisioning als on-demand provisioning bij eerste login ondersteunt, evenals automatische deprovisioning van on-demand geprovisioneerde accounts na een configureerbare periode.
44.	De IT-Oplossing biedt een federatief koppelvlak aan voor uitwisseling van rollen.
45.	De IT-Oplossing ondersteunt IDP (Identity Provider) initiated login.

Integraties

Nummer	Eis	Betreft
46.	De IT-Oplossing faciliteert een mechanisme om grote datasets te importeren en exporteren voor migratiedoeleinden. Indien dit via een API verloopt, moet deze server-side paginering ondersteunen om time-outs en overbelasting te voorkomen.	Initial Data
47.	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.	Integration process
48.	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 automatischverbinding 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. Indien de leverancier een API biedt, dient deze filters te ondersteunen op basis van mutatiedata en een indicator voor verwijderde records, om volledige synchronisatie te garanderen.	Integration platform
49.	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.	IP-filtering
50.	Actuele, volledige en gestructureerde documentatie van de geboden interfaces (API's) wordt beschikbaar gesteld aan de Opdrachtgever. Deze documentatie wordt aangeleverd via een machine-leesbare OpenAPI-specificatie (Swagger) of vergelijkbare industriestandaard. De documentatie bevat minimaal: • De beschikbare endpoints en URL-structuren • Het gebruikte authenticatie- en autorisatiemechanisme • De exacte datamodellen en schema's (JSON-schema's of XSD's) waarmee geautomatiseerd gevalideerd kan worden • Concrete en volledige voorbeelden van responses en een uitputtende lijst van mogelijke HTTP-foutcodes inclusief hun betekenis.	API's (documentation)

51.	De interfaces (API's) van de IT-Oplossing moeten beveiligd zijn middels een geautomatiseerd authenticatiemechanisme dat geen gebruikersinteractie vereist (system-to-system). De authenticatie moet gebaseerd zijn op breed gedragen, moderne beveiligingsstandaarden. Toegestane methoden zijn: • OAuth 2.0 Client Credentials Grant (met het gebruik van tijdelijke, verlopende toegangstokens) • Mutual TLS (mTLS) op basis van door Opdrachtgever goedgekeurde system-to-system certificaten • Opmerking: Het gebruik van statische API-keys of HTTP Basic Authentication is NIET toegestaan, tenzij gecombineerd met strikte IP-whitelisting en expliciete goedkeuring van de Chief Information Security Officer (CISO) van Opdrachtgever.	API's (security)
52.	De IT-oplossing moet API-limieten (rate limits) hanteren die ruim voldoende zijn voor de reguliere bedrijfsvoering, de dagelijkse delta-synchronisaties en eventuele (her)vullingen van de Opdrachtgever, zonder dat dit leidt tot aanvullende gebruikskosten. Indien er limieten actief zijn, moet de API deze via standaard HTTP-headers (zoals X-RateLimit-Limit en X-RateLimit-Remaining) communiceren, zodat het integratieplatform van Opdrachtgever de verzoeksfrequentie hierop geautomatiseerd kan afstemmen (throttling).	API's (limits)
53.	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.	API's (limits)
54.	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: https://systeem.leverancier.nl/api/v1/entiteit/.. V2: https://systeem.leverancier.nl/api/v2/entiteit/..	API's (versioning)
55.	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 leverancier wordt uitgefaseerd.	API's (versioning)
56.	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.	API's (versioning)
57.	Wijzigingen of updates in de API's (inclusief nieuwe versies) moeten de functionele continuïteit van de bestaande bedrijfsprocessen van Opdrachtgever waarborgen. Indien essentiële data-elementen of statussen wijzigen of vervallen, dient de leverancier een gelijkwaardig alternatief of migratiepad te bieden zodat de ketenintegratie niet negatief wordt beïnvloed.	API's (versioning)

58.	De Gegevens die via de API's van de IT-Oplossing worden geleverd / verzonden bestaan uit gegevens in <JSON of XML> formaat, waarbij de nadrukkelijke voorkeur van de Opdrachtgever uitgaat naar <JSON>.	API's (format)
59.	Om controle en audits op volledigheid van de gegevens mogelijk te maken biedt de IT-Oplossing metadata beschikbaar voor het totaal aantal records binnen de opgevraagde dataset en pagina.	API's (data)
60.	Bij uitwisseling van persoonsgegevens (of andere stamgegevens) biedt de IT-Oplossing de mogelijkheid om een specifieke identificatory van de Opdrachtgever op te slaan en via de interface mee te leveren, ten behoeve van de unieke identificatie en koppeling binnen de systemin van de Opdrachtgever.	API's (data)
61.	Indien de IT-oplossing de mogelijkheid biedt om vrije velden en/of aangepaste velden (custom fields) te gebruiken, moeten deze velden door de leverancier ook volledig beschikbaar worden gesteld via de geboden interfaces (API's).	API's (data)
62.	De benodigde interfaces (API's) voor de koppelvlakken moeten bij aanvang van het project volledig ontwikkeld, stabiel, in productie en algemeen beschikbaar zijn bij de leverancier.	API's (status)
63.	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, waarbij de berichtvolgorde wordt gerespecteerd.	Event driven integration

Infrastructure

Nummer	Eis	Betreft
64.	De Ict-oplossing wordt als software as a service (SAAS) oplossing geleverd.	
65.	Apparaten moeten DHCP ondersteunen (RFC2132), 802.1x (passthrough), moeten TCP/IP gebruiken (RFC9293) en minimaal 1 Gbit netwerk snelheid.	Network requirements
66.	Tussen gebouwen is laag 2-connectiviteit, broadcast/multicast-verkeer en connectiviteit naar eindpunten achter netwerkapparaten niet vereist	Network requirements
67.	Apparaten mogen geen broadcast/multicast tussen gebouwen vereisen	Network requirements
68.	De IT-Oplossing ondersteunt zowel het IPv4 als het IPv6 protocol.	Network requirements
69.	De IT-Oplossing kan volledig functioneren op een door de Opdrachtgever bepaalde FQDN (fully qualified domain name).	Network requirements
70.	Apparaten moeten geschikt zijn voor montage in racks en "Front to back" koeling ondersteunen.	Device requirements
71.	Apparaten hebben redundante netwerkaansluitingen en redundante voedingen met IEC 60320 type C14, C16, C19 of C20 ingangen.	Device requirements
72.	Bij on-premise hosting moet de IT-Oplossing een standaard database formaat ondersteunen, en voldoen aan de standaard aanwezige infrastructuur.	Hosting

73.	Wanneer de IT-Oplossing afhankelijk is van een publiek beschikbare software oplossing, dan moet bij on-premise hosting ondersteuning voor onderhoud op deze oplossing (bijvoorbeeld JAVA, OpenJDK) inbegrepen zijn.	Hosting

Specifieke eisen

Beveiligde browser (lockdown)

Nummer	Eis
74.	De Oplossing vergrendelt het apparaat van de kandidaat volledig gedurende de gehele toetssessie: toegang tot niet-toegestane websites, lokale bestanden, externe opslagmedia, communicatiemiddelen en achtergrondapplicaties is technisch geblokkeerd.
75.	De Oplossing onderdrukt meldingen en notificaties van op het apparaat geïnstalleerde software (zoals Teams, Outlook en WhatsApp) en van het besturingssysteem gedurende de toetssessie en zorgt dat deze niet zichtbaar zijn voor de kandidaat.
76.	De vergrendeling van de Oplossing is door de kandidaat niet te beëindigen of te omzeilen zonder fysieke tussenkomst van een toezichthouder (bijv. pincode/token) of reguliere beëindiging van de toetssessie door het systeem. NB. De kandidaat kan vanzelfsprekend wel het apparaat uitschakelen maar dan keert het systeem na herstart terug naar de beveiligde toetsstaat (zie ook de volgende eis).
77.	De Oplossing vergrendelt het apparaat automatisch of keert terug naar de beveiligde toetsstaat bij een verbindingsonderbreking of systeemcrash, zonder dat de kandidaat tussentijd toegang krijgt tot het reguliere besturingssysteem; de kandidaat kan de toets pas na vrijgave door een toezichthouder voorzetten.
78.	In de Oplossing is per toets exact definieerbaar welke websites, bestanden en virtuele applicaties wél toegankelijk zijn op basis van een whitelist-principe; al het overige is standaard geblokkeerd (default deny).
79.	De Oplossing functioneert met gelijkwaardige functionaliteit en gelijkwaardige beveiligingsniveau op Windows 11, macOS en ChromeOS (actuele en één voorgaande hoofdversie).
80.	De Oplossing ondersteunt zowel door Aanbestedende dienst beheerde apparaten als niet-beheerde apparaten van studenten (BYOD) met gelijkwaardig beveiligingsniveau, gelijkwaardige gebruikerservaring en identieke whitelist-mogelijkheden, zonder dat hiervoor per apparaat aanvullende configuratie, scripts, policies of registry-aanpassingen nodig zijn.
81.	De Oplossing weigert te starten binnen een virtuele machine of andere virtualisatie- of emulatieomgeving op het apparaat van de kandidaat, en blokkeert het gebruik van remote-desktop- en schermdelingssoftware tijdens de toetssessie. Naast preventieve blokkade beschikt de Oplossing over een detectielaag die manipulatiepogingen registreert die niet technisch te blokkeren zijn, waaronder ten minste: pogingen tot het starten binnen een virtuele machine die niet worden tegengehouden, aansluiten van een extern beeldscherm, pogingen tot het openen van niet-toegestane websites/applicaties en pogingen tot manipulatie van de beveiliging zelf.
82.	De Oplossing blokkeert schermafdrukken, schermopnamen en schermdeling tijdens de toets; het klembord wordt bij aanvang van de toetssessie geleegd en klembordgebruik tijdens de toets wordt gelogd.
83.	De fraudepreventie van de Oplossing berust niet op het gebruik van webcam, camera, microfoon of opnamen van het scherm of de omgeving van de kandidaat, en vereist na afloop van de toets geen menselijke beoordeling van

	opnamen. Indien de Oplossing dergelijke (proctoring)functionaliteit wel bevat, is deze voor Aanbestedende Dienst centraal en volledig uitgeschakeld.
84.	De Oplossing biedt toezichthouders en functioneel beheer een realtime dashboard met per kandidaat: status (niet gestart / actief / afgerond), technische problemen en gedetecteerde afwijkende handelingen, chronologisch gelogd en naar ernst gecategoriseerd.
85.	Herstart van een reeds gestarte of afgeronde toetssessie door de kandidaat is geblokkeerd door de Oplossing en uitsluitend door een toezichthouder vrij te geven (bijv. via pincode of dashboard).
86.	Gedetecteerde afwijkingen worden in het dashboard van de Oplossing op ten minste twee ernstniveaus gepresenteerd (signaal ter beoordeling door surveillant versus blokkerende gebeurtenis).
87.	De Oplossing activeert een schermblokkade richting de kandidaat bij gedetecteerde afwijkingen.
88.	Een toezichthouder kan een door de Oplossing geactiveerde schermblokkade of geblokkeerde handeling ter plaatse opheffen (bijv. via pincode of dashboard), zodat de kandidaat bij een onterechte detectie de toets zonder verlies van werk kan voortzetten, zonder tussenkomst van ICT of Opdrachtnemer. Het opheffen wordt met tijdstip en betrokken toezichthouder gelogd.
89.	De Oplossing biedt bij netwerkonderbreking de mogelijkheid om lokaal in de beveiligde staat door te werken voor zover het toetstype dit toelaat, met automatische synchronisatie na herstel.

Applicatieve toetsomgeving (virtualisatie)

Nummer	Eis
90.	De Oplossing biedt een cloudgebaseerde virtuele toetsomgeving (zoals Azure Virtual Desktop of gelijkwaardig) waarmee kandidaten tijdens een toets binnen de beveiligde omgeving toegang krijgen tot desktopapplicaties, zonder dat deze applicaties lokaal op het apparaat van de kandidaat geïnstalleerd zijn of worden. NB. Hosting en beheer van deze cloudgebaseerde virtuele toetsomgeving is geen onderdeel van de gevraagde dienstverlening.
91.	De Oplossing ondersteunt aantoonbaar ten minste de volgende softwarecategorieën in een per toets instelbare, gecontroleerde configuratie: statistische software (o.a. SPSS, R/RStudio, Stata), wiskundige software (o.a. MATLAB), programmeeromgevingen (o.a. Python incl. relevante libraries, Jupyter Notebook en IDE's) en de volledige Microsoft Office-suite (Word, Excel, PowerPoint, Access).
92.	Functies binnen toegestane applicaties die de toetsintegriteit kunnen schaden (waaronder cloud-opslag, macro's, invoegtoepassingen, AI-assistenten en externe koppelingen) zijn uitschakelbaar door de Oplossing, centraal en zonder configuratie per individueel apparaat.
93.	Applicaties die niet expliciet voor een specifieke toets zijn toegestaan, zijn technisch niet bereikbaar vanuit de virtuele omgeving van de Oplossing, ook niet via omwegen zoals een terminal, bestandsbeheer, hulp-/dialoogvensters of browserextensies.
94.	De virtuele toetsomgeving van de Oplossing is volledig gescheiden van het lokale apparaat: gegevensuitwisseling (kopiëren, bestandsoverdracht, klembord) tussen virtuele omgeving en lokale machine is in beide richtingen geblokkeerd.
95.	Aanbestedende dienst beschikt over volledige beheersautonomie over de applicatie-images in de virtuele omgeving van de Oplossing: Aanbestedende

	dienst kan zelfstandig nieuwe softwareversies doorvoeren, configureren, testen en uitrollen zonder afhankelijkheid van Opdrachtnemer per wijziging.
96.	De Oplossing schaalt automatisch, op basis van de toetsplanning en zonder handmatige tussenkomst per toets, naar het verwachte aantal gelijktijdige gebruikers: bij aanvang minimaal 1.500 gelijktijdige kandidaten, groeiend naar 2.500, inclusief automatisch opstarten en afsluiten van virtuele capaciteit. De Oplossing kan het maximaal aantal kandidaten ondersteunen. NB. Hosting en beheer van de cloudgebaseerde virtuele toetsomgeving en het zorgdragen voor voldoende capaciteit, is geen onderdeel van de gevraagde dienstverlening.
97.	Licentieservers van Aanbestedende dienst (bijv. voor SPSS) kunnen op beveiligde wijze beschikbaar worden gemaakt binnen de virtuele toetsomgeving van de Oplossing.
98.	Kandidaten kunnen binnen de virtuele omgeving van de Oplossing op beveiligde wijze bestanden ontvangen (uitgereikte toetsbestanden) en inleveren, waarbij ingeleverde bestanden na afloop centraal beschikbaar zijn voor bevoegde medewerkers en niet op het lokale apparaat achterblijven.
99.	Een kandidaat kan een lopende toets bij een defect apparaat voortzetten op een ander (reserve)apparaat zonder verlies van werk in de virtuele omgeving van de Oplossing.
100.	Whitelisting van websites binnen de virtuele omgeving van de Oplossing is dynamisch per toets instelbaar zonder aanpassing van het onderliggende image.
101.	Opdrachtnemer stelt referentie-templates en tooling beschikbaar waarmee Aanbestedende dienst zelfstandig examen-images kan bouwen en aanpassen.

Beheersbaarheid en configuratiebeheer

Nummer	Eis
102.	De Oplossing biedt een centrale, webgebaseerde beheerconsole waarmee toetsconfiguraties (toegestane applicaties, websites, bestanden en instellingen) per toets kunnen worden aangemaakt en beheerd.
103.	De Oplossing activeert automatisch lockdown- en applicatie-instellingen bij aanvang en deactiveert deze automatisch bij afsluiting van een toets door de kandidaat. Het toetsplatform bepaalt de beschikbaarheid van de toets in een specifiek tijdsvenster.
104.	De Oplossing maakt het mogelijk om direct opeenvolgend op hetzelfde apparaat verschillende toetsen met verschillende configuraties af te nemen, zonder herinstallatie of handmatige ingreep van ICT tussen de toetsen.
105.	Wijzigingen in toetsconfiguraties zijn versiebeheerd en auditeerbaar in de Oplossing: Aanbestedende dienst kan achteraf aantonen welke configuratie (incl. whitelist en applicatieset) actief was tijdens een specifieke toets.
106.	De Oplossing maakt het mogelijk voor functioneel beheerders en/of docenten van Aanbestedende dienst om zelfstandig, zonder tussenkomst van centrale ICT, de whitelist en toetsconfiguratie van een geplande toets aan te passen tenminste nog tot 1 uur voor aanvang van de toets. Het aanpassen van het aantal kandidaten (en dus de benodigde capaciteit binnen de virtuele toetsomgeving) moet mogelijk zijn ten minste nog tot 2 uur voor aanvang van de toets. Na aanvang van de toets kunnen toezichthouders of functioneel beheerders nog individuele kandidaten toelaten (bijv. laatkomers of kandidaten die op een reserve-apparaat verder werken), voor zover de reeds beschikbare capaciteit dit toelaat.

107.	De Oplossing maakt reguliere toetsafname mogelijk zonder structurele inzet van ICT-personeel van Aanbestedende dienst en zonder herinrichting van werkplekken tijdens of tussen toetsmomenten.
108.	De Oplossing ondersteunt meerdere beheerniveaus (centraal ICT-beheer, toetscoördinatoren, surveillanten) met instelbare rechtenstructuren.
109.	De beheerconsole biedt centraal realtime inzicht in alle geplande, lopende en afgelopen toetsen. Per toets worden de naam, tijdsduur, datum/tijd en het gebruikte aantal virtuele desktops getoond. Het overzicht is op al deze velden filterbaar.
110.	De Oplossing beschikt over een beheersconsole die per toets en per periode realtime inzicht geeft in het gebruik van de virtuele toetsomgeving (ten minste aantal kandidaten, gebruikte applicaties, aantal sessies en sessieduur), filterbaar op kenmerken van de toets (bijv. faculteit of opleiding, voor zover beschikbaar), exporteerbaar (bijv. CSV/XLSX) en opvraagbaar via de API.

Scheiding toetsmodus / regulier gebruik

Nummer	Eis
111.	Apparaten waarop de toetssoftware is geïnstalleerd, zijn buiten toetsmomenten volledig regulier bruikbaar voor onderwijs en zelfstudie, zonder functionele beperkingen of merkbaar prestatieverlies veroorzaakt door de toetssoftware.
112.	De overgang tussen reguliere modus en toetsmodus (en terug) vindt plaats zonder herinstallatie, herstart of handmatige ingreep van ICT, bijvoorbeeld via automatische activering op basis van roosterkoppeling of een pincode/token van de toezichthouder.
113.	Buiten toetsmomenten is geen permanente achtergrondservice actief die prestaties, privacy of regulier gebruik van het apparaat beïnvloedt, en na afloop van een toetssessie blijven geen configuratieresten achter die het reguliere gebruik beïnvloeden. NB. Een achtergrondservice die actief is voor het periodiek downloaden van updates en voor het uploaden van eventuele relevante logs (bijv. debug- en crashlogs) is wel toegestaan.
114.	Updates en start van de toetssoftware op BYOD- en leenlaptops vereisen geen lokale beheerdersrechten van de eindgebruiker; beveiligingsupdates worden automatisch uitgerold zonder handeling van de student of van ICT. NB. Het is akkoord als voor het doen van de initiële installatie wel lokale beheerdersrechten nodig zijn.
115.	De Oplossing werkt als standaard softwareapplicatie: zonder dual boot, zonder additionele hardware (zoals USB-sticks), zonder BIOS-aanpassingen en zonder distributie van configuratiebestanden; op beheerde apparaten is silent deployment (bijv. MSI) mogelijk.
116.	De Oplossing maakt het mogelijk om te integreren met een toetsplatform, waarbij het toetsplatform zelf technisch afdwingt (bijv. Via header check) dat de toets uitsluitend binnen de beveiligde omgeving kan worden geopend.
117.	De koppeling met het toetsplatform zorgt dat de beveiligde omgeving van de Oplossing automatisch opstart vanuit het toetsplatform en de kandidaat automatisch wordt aangemeld, zonder afzonderlijke handelingen van de kandidaat om de lockdown te activeren.
118.	Whitelist- en toetsconfiguraties zijn per toets te beheren vanuit (een interface geïntegreerd met) het toetsplatform door medewerkers vanuit Aanbestedende dienst.
119.	Toetsresultaten en logdata vanuit de beveiligde omgeving van de Oplossing zijn exporteerbaar naar of direct beschikbaar in het gekoppelde toetsplatform.

Identiteitsverificatie en toegangsbeheer

Nummer	Eis
120.	De Oplossing koppelt voor authenticatie met de identity provider van Aanbestedende dienst via SURFconext, zodat kandidaten en medewerkers inloggen met hun TiU-account; buiten dit proces wordt nergens om inloggegevens gevraagd.
121.	De Oplossing staat toe dat beheer- en toezichthoudersfuncties worden beveiligd met tweefactorauthenticatie (via de identity provider van Aanbestedende dienst).
122.	De Oplossing biedt auditlogging op kandidaatniveau: tijdstip van aanmelding, relevante activiteiten en detecties tijdens de toets en tijdstip van afsluiting worden geregistreerd en zijn gedurende een instelbare periode opvraagbaar door bevoegde medewerkers, inclusief exportmogelijkheid (bijv. PDF) ten behoeve van de examencommissie.
123.	Aanvullende verificatiestappen bij aanvang van een toets zijn per toets configureerbaar (zoals een QR-code, pincode of token van een toezichthouder).

Toegankelijkheid en studentervaring

Nummer	Eis
124.	De beveiligde omgeving van de Oplossing blokkeert geen webgebaseerde toegankelijkheidsvoorzieningen die voor de toets zijn toegestaan (zoals tekstvergroting en voorleessoftware), en ondersteunt het wisselen van taal- en toetsenbordinstellingen en het aanpassen van het systeemvolume (t.b.v. luistertoetsen) tijdens de toets.
125.	Tijdens de toets kan de kandidaat, zonder de beveiligde toetsstaat van de Oplossing te verlaten: de batterijstatus zien en een melding ontvangen bij een kritiek batterijniveau; de wifi-verbinding opnieuw instellen of van netwerk wisselen; de schermhelderheid aanpassen; en het audio-uitvoerapparaat kiezen (bijv. koptelefoon).
126.	Extra toetstijd en afwijkende voorzieningen zoals deze per individuele kandidaat per toets configureerbaar zijn binnen het toetsplatform moeten automatisch worden overgenomen door de Oplossing, ook wanneer extra tijd tijdens een lopende toets wordt toegekend (bijv. na een verstoring). De beveiligde toetsstaat blijft actief tot het einde van de verlengde toetstijd.
127.	De gebruikerservaring voor de kandidaat (opstarten, inloggen, toets starten, afsluiten) is vergelijkbaar en toegankelijk op alle ondersteunde platformen en vergt geen technische kennis; het aantal handelingen tot toetsstart is minimaal.