| Ref nr | Onderwerp | Vraag | Defintief antwoord |
|---|---|---|---|
| 1 | Algemeen | Welk informatiebeveiligingsrisicoprofiel heeft Scalda toegekend aan haar schoollocaties en in hoeverre verschillen de schoollocaties in dezen van elkaar? | Scalda hanteert voor alle locaties een hoog informatiebeveiligingsrisico. Dat komt door de grootschalige verwerking van privacygevoelige (student)gegevens, veel dagelijkse bezoekersstromen en het open schoolkarakter. Er zijn geen materiële verschillen per locatie in het risicoprofiel; contextfactoren (gebouw, functie en bezetting) kunnen lokaal variëren, maar het beleidsuitgangspunt is uniform: hoog risico. Het (in ontwikkeling zijnde) beveiligingsbeleid geldt organisatiebreed en is gericht op het behalen van NBA-volwassenheidsniveau 3 met een integrale, risico-gebaseerde aanpak voor preventie, detectie, reactie en rapportage. |
| 2 | Risico's en beheersmaatregelen (lees: eisen) | Welke organisatorische, mens-gerelateerde en systeemtechnische informatiebeveiligingsrisico's heeft Scalda geïdentificeerd, in relatie tot de beoogde integratie van systemen in één Cloud-gebaseerd SMS? | Voor (kantoor)ruimtes heeft Scalda fysieke beveiligingsmaatregelen vastgesteld en geïmplementeerd in overeenstemming met de bedrijfseisen, zodat de toegang tot informatiesystemen op passende wijze wordt beperkt. De fysieke beveiligingsmaatregelen zorgen er ook voor dat risico's met betrekking tot diefstal, temperatuur, brand, rook, water, trillingen, terreur, vandalisme, stroomuitval, chemicaliën of explosieven effectief worden voorkomen, gedetecteerd en beperkt. Dit zijn voor nu de belangrijkste risico's die Scalda heeft geïdentificeerd. |
| 3 | Risico's en beheersmaatregelen (lees: eisen) | Aan welke cybersecuritybeheersmaatregelen moet de beoogde opdrachtnemer, als gevolg van die risico's, de accounts, wachtwoorden, koppelvlakken, logbestanden en back-ups aantoonbaar laten voldoen? | Scalda hanteert ISO 27001 (of gelijkwaardig) als minimumnorm voor informatiebeveiliging en sluit daarbij aan bij de sectorbrede ontwikkeling richting het Normenkader Informatiebeveiliging.<br><br>Hoewel Scalda als onderwijsinstelling niet rechtstreeks onder de NIS2-richtlijn valt, is het belangrijk dat leveranciers aantoonbaar werken in lijn met de NIS2-principes. De onderwijssector maakt veel gebruik van cloudproviders, datacenters en netwerkbeheerders die wél onder NIS2 vallen; daarmee wordt de keten indirect geraakt. Leveranciers moeten dus rekening houden met deze afhankelijkheden en passende maatregelen treffen.<br><br>De NIS2-richtlijn legt niet alleen verplichtingen op aan organisaties binnen kritieke sectoren, maar benadrukt ook het belang van cybersecurity binnen de gehele toeleveringsketen. Dit betekent dat organisaties niet alleen verantwoordelijk zijn voor hun eigen cyberveiligheid, maar ook moeten zorgen dat hun ketenpartners voldoen aan bepaalde eisen. De NIS2-richtlijn wordt momenteel vertaald naar Nederlandse wetgeving. Dat gebeurt met de Cyberbeveiligingswet (Cbw). |
| 4 | Risico's en beheersmaatregelen (lees: eisen) | In hoeverre dient de beoogde opdrachtnemer, vanwege die risico's, aan te sluiten op centrale cybersecurityvoorzieningen van Scalda, bijvoorbeeld aangaande monitoring, en welke voorzieningen betreft het? | Single Sign-On via SAML 2.0 is vereist. Toegang tot het SMS en onderliggende services verloopt via centrale IAM van Scalda (MFA verplicht voor beheerders en gevoelige functies). Rollen zijn rol-gebaseerd, auditbaar en periodiek te hercertificeren. |

| | | | |
|---|---|---|---|
| 5 | Uitvoering | Met welke organisatorische en mens-gerelateerde informatiebeveiligingsmaatregelen van Scalda wordt de beoogde opdrachtnemer geconfronteerd, gedurende de uitvoering van de werkzaamheden? Welke informatiebeveiligingsprocedures zijn bijvoorbeeld van toepassing? Aan welke screeningsvereisten moet personeel van de beoogde opdrachtnemer voldoen en welke informatiebeveiligings-opleidingsvereisten zijn van kracht? | Juridisch is een verwerkersovereenkomst verplicht (art. 28 AVG) inclusief subverwerkerslijst, locaties van verwerking, beveiligingsmaatregelen en meldtermijnen datalekken. Ook wordt een VCA opgenomen als geschiktheidseis in de aanbesteding. Zie verder antwoorden vragen 3 en 4. |
| 6 | Wet- en regelgeving | Welke uit de AI Act voortvloeiende eisen legt Scalda door aan de beoogde opdrachtnemer, in het licht van de door Scalda gewenste AI-toepassingen? | Voor de beoogde AI-functionaliteiten (zoals objectdetectie en ‘smart search’) wordt uitgegaan van een laag-/beperkt-risico categorie onder de EU AI Act. Dat betekent o.a. eisen aan transparantie, logging, dataset-kwaliteit, uitlegbaarheid, risk-management en menselijk toezicht. Biometrische identificatie voor toegangsverlening of intercom is uitgesloten; gezichtsherkenning wordt niet toegepast. Leveranciers leveren een AI-risicobeoordeling, DPIA-input en documenteren trainingsdata, prestaties en beperkingen. Definitieve kwalificatie volgt bij aanbesteding. |
| 7 | Wet- en regelgeving | Welke systeemtechnische beheersmaatregelen uit de AVG dient de beoogde opdrachtnemer aantoonbaar in te vullen tijdens de ontwerp- en realisatiefase, om privacy by design mogelijk te maken, en in stand te houden gedurende de onderhoudsfase? | Systeemtechnische beheersmaatregelen volgens de AVG<br>1. Privacy by Design & Privacy by Default<br>- Ontwerp systemen zó dat privacy standaard is ingebouwd.<br>- Minimaliseer de verwerking van persoonsgegevens: verwerk alleen wat strikt noodzakelijk is.<br>- Stel standaardinstellingen zo in dat de privacy van gebruikers maximaal wordt beschermd. |

| | | | |
|---|---|---|---|
| | | | 2. Data-inventarisatie en verwerkingsregister<br>- Breng in kaart welke persoonsgegevens worden verwerkt, via welke kanalen, en met welk doel.<br>- Documenteer dit in een verwerkingsregister, verplicht voor veel organisaties.<br>3. Beveiligingsmaatregelen<br>- Implementeer technische maatregelen zoals:<br>- Encryptie van data<br>- Sterke wachtwoorden en toegangsbeheer<br>- Multi Factor Authenticatie (MFA) voor beheerders en accounts met verhoogde rechten, en waar mogelijk ook voor alle reguliere gebruikers<br>- Beveiligde verbindingen (SSL/TLS)<br>- Logging en monitoring van datatoegang<br>- Zorg voor fysieke beveiliging van servers en apparatuur.<br>4. Toegangscontrole en autorisatie<br>- Zorg dat alleen bevoegde personen toegang hebben tot persoonsgegevens.<br>- Gebruik rolgebaseerde toegang en beperk rechten tot het minimum.<br>- Pas MFA toe bij toegang tot kritieke systemen en gevoelige data.<br>5. Bewaartermijnen en opslagbeperking<br>- Stel beleid op voor bewaartermijnen van gegevens.<br>- Verwijder of anonimiseer gegevens zodra ze niet meer nodig zijn voor het oorspronkelijke doel.<br>6. Transparantie en informatievoorziening<br>- Ontwerp systemen zodat gebruikers eenvoudig inzicht krijgen in hoe hun gegevens worden verwerkt.<br>- Zorg voor duidelijke privacyverklaringen en toestemmingsmechanismen.<br>7. Risicoanalyse en DPIA (Data Protection Impact Assessment)<br>- Voer een DPIA uit bij projecten met een hoog privacyrisico.<br>- Identificeer en beoordeel risico's voor betrokkenen en neem mitigerende maatregelen.<br>8. Testen en validatie<br>- Test systemen op privacy- en beveiligingsaspecten vóór livegang.<br>- Voer penetratietests en audits uit om kwetsbaarheden op te sporen. |
| 8 | Algemeen | Gezien de structuur en detailniveau van deze marktconsultatie is het voor ons als marktpartij niet duidelijk in hoeverre dit document al als definitieve aanbestedingsvoorbereiding geldt. Kunt u verduidelijken welke onderdelen nog beïnvloedbaar zijn op basis van marktinput, en welke als vast uitgangspunt worden gezien? | Het PvE is gepubliceerd om de marktconformiteit hiervan te toetsen. Mocht uit de marktconsultatie blijken dat bepaalde eisen niet marktconform zijn, dan kunnen deze eisen worden gewijzigd. Het huidige PvE is echter wel in lijn met de behoefte van de organisatie waardoor als basis overeenkomt met het PvE dat zal worden gepubliceerd bij de aanbesteding. |

| | | | |
|---|---|---|---|
| 9 | Volledig cloudgebaseerd vs. lokale opslag | Kunt u verduidelijken hoe de eis van een ‘volledig cloudgebaseerd’ Securitymanagementsysteem zich verhoudt tot het gebruik van lokale opslag (zoals SD-kaarten of edge-appliances)? | Scalda verlangt een volledig cloudgebaseerd Security Management Systeem (SMS). Dat betekent dat alle videobeelden rechtstreeks en continu naar de cloud worden verzonden en daar voor 28 dagen worden bewaard, conform het Programma van Eisen.<br><br>Om de continuïteit te waarborgen bij netwerk- of cloudonderbrekingen dient het systeem zodanig ontworpen te zijn dat:<br>- Iedere locatie autonoom kan blijven functioneren;<br>- Gebruikers tijdelijk toegang houden tot live-beelden en basisfunctionaliteit;<br>- Beelden na herstel van de verbinding automatisch en volledig worden gesynchroniseerd naar de cloud;<br>- Bij calamiteiten een buffersysteem van vier (4) dagen beschikbaar is, zodat geen beelden verloren gaan en de werking van het systeem ongestoord doorloopt.<br><br>Er wordt hiermee dus primair geen lokale opslag verlangd. De cloud vormt altijd het primaire en enige opslagpunt. Dit borgt duidelijkheid, schaalbaarheid en centrale beheersbaarheid en voorkomt discussies over hybride of gedeeltelijke oplossingen. |
| 10 | Cloudgebaseerd | De term ‘volledig cloudgebaseerd’ kan op meerdere manieren worden geïnterpreteerd (bijv. met of zonder edge-opslag). Kunt u aangeven welke mate van local hardware (zoals SD-kaarten of edge-appliances) binnen deze definitie valt? En in hoeverre is er ruimte voor hybride architecturen indien dat functioneel of technisch noodzakelijk blijkt? | Zie antwoord vraag 9. |
| 11 | Open standaarden en protocollen | Kunt u aangeven welke open standaarden en/of protocollen de voorkeur hebben voor integratie van subsystemen (zoals ONVIF, SIP, OSDP)? | Voor de camera's geldt dat deze ONVIF- en NDAA compliant dienen te zijn. Voor de gegevensoverdracht is dit het RTSP-protocol. Het SMS dient een open platform te zijn en géén vendor lock-in. Voor de koppelingen dient gebruik gemaakt te worden van open API's. Voor de intercomsystemen geldt het SIP-protocol en voor de toegangscontrolesystemen geldt het OSDP-protocol. |
| 12 | Status Programma van Eisen (PvE): | Is het Programma van Eisen in deze marktconsultatiefase nog open voor wijziging op basis van marktinput, of is dit grotendeels vastgesteld? | Zie antwoord vraag 8. |
| 13 | Scope en systeemkoppelingen | Wordt er in een latere fase ook gekeken naar koppelingen met andere gebouwgebonden systemen (zoals gebouwbeheersystemen), of vallen die buiten scope van deze consultatie? | De gebouwbeheerssystemen vallen buiten de scope van deze consultatie. |
| 14 | Informatiebeveiliging en compliance | Wordt het gebruik van Europese datacenters (Tier 3) uitsluitend vanuit technische betrouwbaarheid geëist, of spelen compliance- en privacyoverwegingen (zoals AVG) ook een rol in de keuze voor cloudproviders? | Uitsluitend uit oogpunt van technische betrouwbaarheid en beschikbaarheid. Met een Tier3 datacenter kan er ongestoord onderhoud worden gepleegd en wordt er gebruik gemaakt van redundante systemen. De beschikbaarheid heeft een uptime van 99,9%. De keuze voor Tier 3 is in lijn met het organisatiebeleid van Scalda. |

| | | | |
|---|---|---|---|
| 15 | Prestatie-indicatoren en betrouwbaarheid | Wordt er in het vervolgtraject ook gedacht aan meetbare KPI's voor uptime, storingsrespons en servicekwaliteit, of blijft dit op SLA-niveau (zoals 99,7%)? | Dit blijft niet alleen op SLA-niveau. In de aanbesteding zal hier verder op in worden gegaan wat betreft meting van de afgesproken kwaliteit. |
| 16 | Betrokkenheid eindgebruikers | Worden bij de verdere uitwerking van het Programma van Eisen ook gebruikersgroepen (zoals conciërges of facilitair beheerders) betrokken voor het toetsen van gebruiksvriendelijkheid en trainingseisen? | Dit is niet relevant voor deze marktconsultatie. |
| 17 | Duurzaamheid als criterium | Wordt duurzaamheid (zoals energieverbruik, levensduur hardware of circulariteit) in het vervolg meegenomen als beoordelingscriterium of slechts als informatief onderdeel? | Duurzaamheid wordt meegenomen als gunningscriterium in de aanbesteding. |
| 18 | Eis 1: Functionele Eisen | Punt j. Hier wordt gesproken over 5-10 Mbps m.b.t. de bandbreedte. Onze vraag is op welke resolutie zou u de beelden willen weergeven? Is dit 1920x1080 of op 4K of een andere resolutie of heeft u geen specifieke resolutie in gedachte en moet de beeldkwaliteit hier alleen maar aan voldoen? Dit is meer een vraag omdat er hoogstwaarschijnlijk een mix van camera's zal zijn. | De minimumeis voor alle camera's is 5MP (=2592x1944 pixels). Zowel H.264 als H.265 voldoen aan de eisen voor wat betreft compressie, waarbij het aantal Mbps afhankelijk is van de bewegingen in het beeld. Gemiddeld gezien is dit 5-10 Mbps. |
| 19 | Eis 2: Dekkingsgebied van de camera's. | Punt a. Hier is sprake van bijlage 008, bijlage 007 en bijlage 003 Prijzenblad, Tab2. Camera's maar betreffende bijlage ontbreken. Kunt u aangeven of deze nog volgen en hoe wij hiermee om moeten gaan? | Het PvE is gepubliceerd om de marktconformiteit hiervan te toetsen. Verdere vragen over de bijbehorende bijlagen kunnen worden gesteld in de nota van inlichtingen van de aanbesteding. De referenties naar de bijlagen in het PvE komen voor deze marktconsultatie te vervallen, aangezien deze bijlagen voor nu als niet relevant worden gezien door de aanbestedende dienst. |
| 20 | Eis 3: Functionele eisen camerasysteem | Punt b. Hier is sprake van bijlage 015 maar deze is niet toegevoegd. Komt deze nog of hoe moeten wij hiermee omgaan? | Zie antwoord vraag 19. |
| 21 | Eis 4: Cloudopslag | Punt e. Een "private hosted cloud" is niet toegestaan. Wat is de reden dat dit niet is toegestaan? Heeft dit met afhankelijkheid te maken? | Uitgangspunt is cloud-tenzij. Scalda wil een standaard SaaS-oplossing op een publieke cloud met Tier-3-equivalent, om schaalbaarheid, continuïteit, portabiliteit en lifecycle-management te borgen en vendor lock-in te beperken. Een 'private hosted cloud' is daarom uitgesloten in dit traject. Deze keuze verkleint afhankelijkheden van specifieke datacenters, versnelt updates en maakt overstappen tussen regio's/providers realistischer. |
| 22 | Eis 5: Toegangscontrolesysteem | Punt a. Hier is sprake van bijlage 009, Kritische ICT ruimtes maar deze bijlage ontbreekt. Wordt deze nog ter beschikking gesteld? Hoe moeten wij hiermee om gaan? | Zie antwoord vraag 19. |
| 23 | 1.Eis 10: Turnkey oplevering. | Punt d en e. Hier is sprake van dat de tijd tussen de 1e en 2e oplevering 2 maanden is en dat dit ook geldt voor de overige schoollocaties. Betekent dit dan 1 jaar na aanvang van de 1e locaties alle locaties opgeleverd dienen te zijn? | Deze eis zal voor publicatie van de aanbesteding anders geformuleerd worden vanwege het feit dat Scalda een extra locatie heeft die momenteel wordt verbouwd. De oplevering per locatie is gedefinieëerd als: Oplevering vindt plaats nadat alle camera's voor 1 locatie zijn gemonteerd en aangesloten op het netwerk van opdrachtgever en het cloud SMS is geconfigureerd voor deze locatie en voldoet aan de gestelde eisen. De tweede oplevering is 2 maanden nadat het CCTV-systeem voor de schoollocatie in gebruik is genomen en is aangetoond dat het geheel conform de gestelde eisen functioneert. De genoemde opleveringsprocedure (10a t/m e) geldt daarna opnieuw voor alle volgende locaties. Het gaat in totaal om 7 locaties. Deze locaties dienen binnen 1 jaar opgeleverd te worden. |

| | | | |
|---|---|---|---|
| 24 | Programma van eisen | In het programma van eisen wordt verwezen naar diverse bijlagen, deze zijn echter niet gepubliceerd in de marktconsultatie. Worden deze nog gepubliceerd? | Zie antwoord vraag 19. |