

Bijlage LAS: Eisen informatiebeveiliging en privacy

DEEL 1: DOCUMENTENCLASSIFICATIE

Voor dit document hanteren wij classificatie: **TLP: AMBER**

SIVON maakt gebruik van de volgende classificaties en coderingen:

Classificatie	Toelichting
TLP: RED	Strikte toegangscontrole. Opslag op beveiligde servers met encryptie. Distributie alleen via beveiligde kanalen.
TLP: AMBER	Dit document mag gedeeld worden binnen SIVON en (externe) toegewezen belanghebbenden. Ontvanger mag niet verder delen zonder toestemming van SIVON.
TLP: GREEN	Geen restricties op toegang of distributie. Mag vrijelijk gedeeld worden binnen en buiten SIVON, maar niet via publieke kanalen.
TLP: CLEAR	Geen restricties op toegang of distributie. Mag vrijelijk gedeeld worden, ook via publieke kanalen binnen en buiten SIVON.

DEEL 2 (1/2):INFORMATIEBEVEILIGING, PRIVACY EN BEVEILIGING SERVERRUIMTE

1. De gegevens in het LAS zijn via een browser toegankelijk en dienen daarom ook dienovereenkomstig beveiligd te zijn (internet en intranet). Versleuteling van data zal plaatsvinden op basis van gangbare standaarden zoals ook vermeld op <https://www.forumstandaardisatie.nl/open-standaarden/verplicht>.
2. De online toegang tot de servers is afgeschermd door middel van een firewall met loggingsfunctionaliteiten. De technische specificaties van de firewall worden door opdrachtnemer verstrekt na het ondertekenen van een geheimhoudingsverklaring en voor aanvang van de overeenkomst.
3. Opdrachtnemer heeft en behoudt ISO/IEC 27001:2022 (RvA-geaccrediteerd), of vergelijkbaar, met een Statement of Applicability voor het garanderen van kwaliteit en veiligheid bij de serviceorganisatie en alle bij het LAS betrokken bedrijfsonderdelen en processen van opdrachtnemer.
4. Jaarlijks levert opdrachtnemer een ISAE 3000/SOC 2 Type II-rapportage (security, availability, confidentiality), of vergelijkbaar inclusief management-letter. De management-letter bevat tenminste een lijst met maatregelen waarmee de risico's die geïdentificeerd zijn beperkt en/of verkleind worden. Deze rapportage bespreekt opdrachtnemer jaarlijks met opdrachtgever en is mede bestemd ter bespreking en beoordeling van het beveiligingsbeleid van opdrachtgever, toezichthouder en/of de accountant.
5. Opdrachtnemer voldoet aantoonbaar aan de baseline van maatregelen opgenomen in het Certificeringsschema informatiebeveiliging en privacy ROSA (of vergelijkbaar, hetgeen door Opdrachtnemer moet worden aangetoond) en vult hiertoe de meest recente versie van rapportage in. Zie: (https://www.edustandaard.nl/app/uploads/2018/03/4.-Certificeringsschema_toetsingskader-v3.0.xlsx)
6. Het LAS voldoet voor wat betreft de hierin opgenomen gegevens blijvend aan de in het Certificeringsschema opgenomen recente maatregelen behorend bij de BIV-classificatie Beschikbaarheid = hoog (3), Integriteit = hoog (3), Vertrouwelijkheid = hoog (3). Classificatiemodel: https://www.edustandaard.nl/standaard_afspraken/certificeringsschema-informatiebeveiliging-en-privacy-rosa/certificeringsschema-informatiebeveiliging-en-privacy-rosa-v3-0/.
7. Opdrachtnemer heeft beveiligingsmaatregelen getroffen om cyberaanvallen tegen te gaan, die ten minste voldoen aan of beter zijn dan de basismaatregelen van het NCSC (<https://www.ncsc.nl/wat-kun-je-zelf-doen/basisprincipes>). Dit betreft de maatregelen op het gebied van logging, versleuteling opslagmedia, multifactor authenticatie, controles op toegang/bereikbaarheid (waaronder preventieve detectie- en beveiligingsmaatregelen zoals DDoS protection, IDS/IPS, en/of SOCSiem-oplossing), autorisaties volgens een vooraf ingesteld en gecontroleerd autorisatiebeleid en -matrix, maken en controleren van back-ups, segmentatie van netwerken, en patchmanagement (software updates). De procedures die opdrachtnemer hierbij hanteert zijn schriftelijk vastgelegd en beschikbaar voor inzage opdrachtgever.
8. Het LAS hanteert Role Based Access Control (RBAC) voor de authenticatie en autorisatie van gebruikers, waarbij per rol lees-, schrijf- of bewerkrechten worden toegekend tot de gegevens waarvoor toegang is verleend. Multi Factor Authenticatie wordt hierbij standaard afgedwongen op ieder niveau van authenticatie en autorisatie.
9. Authenticatiegegevens worden uitsluitend bewaard wanneer dit technisch vereist is en blijven tijdens verwerking en in alle gerelateerde processen versleuteld en niet uitleesbaar.
10. Activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen worden via audit logging bijgehouden en worden bewaard gedurende een periode die overeenkomt met wat gezien wordt als industriële standaard, gebruikelijk is voor soortgelijke systemen en door inschrijver is afgestemd met SIVON.

TLP: AMBER

Deze zijn zonder tussenkomst van opdrachtnemer benaderbaar door de medewerkers bij opdrachtgever die verantwoordelijk zijn voor (het uitvoeren van) het AVG/privacy-beleid, zoals coördinator IBP, security officer en privacy officer of een door opdrachtgever aan te wijzen derde.

11. Elke poging (geslaagd of niet geslaagd) tot authenticatie en autorisatie dient gelogd te worden. Dit logbestand heeft een bewaartermijn van 3 maanden om te kunnen analyseren.
12. 1. Het LAS houdt vanaf de ingangsdatum van de naderende overeenkomst en gedurende de looptijd daarvan een registratie of logging bij van alle mutaties die nodig zijn om tenminste te voldoen aan de hierna te noemen criteria:
 - a. De normen die de Autoriteit Persoonsgegevens stelt in haar onderzoek naar leerling administratiesystemen uit 2018 (of richtlijnen of aanbevelingen die nadien zijn uitgevaardigd door de Autoriteit Persoonsgegevens).
 - b. De eisen die het NCSC (of dienst opvolger of vergelijkbare organisatie voor het onderwijs) stelt aan logging in het kader van cybersecurity.
 - c. Aansluiten bij de normen die in de (Europese) ict-sector gebruikelijk zijn voor administratiesystemen waarin bijzondere persoonsgegevens worden verwerkt.
 - d. Voor het bepalen van de wijze en inhoud van de logging wordt aangesloten bij de op het LAS van opdrachtnemer toegepaste BIV-classificatie zoals beschreven in het ROSA Certificeringsschema (dat onderdeel uitmaakt van de (model) verwerkingsovereenkomst behorende bij het Privacyconvenant 4.0)
2. De logging van deze belangrijkste gebruikersactiviteiten en informatiebeveiligingsgebeurtenissen moet interpreteerbaar zijn voor de CISO/SO/functioneel beheerders/applicatiespecialisten van of ingeschakeld door het schoolbestuur.
3. Partijen (SIVON en de opdrachtnemer) stellen na gunning in onderling overleg vast:
 - e. de belangrijkste gebruikersactiviteiten en informatiebeveiligingsgebeurtenissen die opgenomen zijn of moeten worden in de logging waarbij enerzijds de onder 1. en 2. genoemde criteria leidend zijn en anderzijds rekening wordt gehouden met de omvang van de logging, gelogde activiteiten en gebeurtenissen en techniek achter deze logging.
 - f. de wijze en tijdspad waarop de logbestanden en auditlogging beschikbaar zijn of gesteld moeten worden aan het schoolbestuur waarbij
 - i. opdrachtnemer tenminste de mogelijkheid biedt voor het schoolbestuur om (een deel van) de auditlogging zonder interactie met of actieve tussenkomst van opdrachtnemer te downloaden, ontvangen of raadplegen, en
 - ii. bepaald wordt in welk formaat of de toegang tot (audit)logbestanden beschikbaar is of wordt gesteld (export, raadplegen) aan het schoolbestuur, en
 - iii. opdrachtnemer aansluit op een aantoonbaar en voor het schoolbestuur uitvoerbaar auditplan van het schoolbestuur.
13. Het LAS is zo ingericht dat de hierin opgenomen gegevens niet ongeautoriseerd kunnen worden toegevoegd, gemuteerd, verwijderd of geraadpleegd.
14. De opdrachtnemer garandeert dat grote en/of kritieke security- en privacy-issues met hoge urgentie worden opgepakt, waarbij deze issues zowel aan de vaste contactpersoon van de opdrachtgever, als aan de functionaris gegevensbescherming van de opdrachtgever worden gemeld.
15. De opdrachtnemer garandeert dat kritische en/of grote security- en privacy-incidenten van andere klanten van de opdrachtnemer, die ook van toepassing kunnen zijn op de opdrachtgever of op enigerlei wijze

gevolgen kunnen hebben voor de opdrachtgever, afgehandeld worden als ware het een security- en privacy-incident van de opdrachtgever zelf.

16. De opdrachtnemer volgt het software- en versiebeleid van de relevante hard- en softwareleveranciers en garandeert dat de benodigde updates, hotfixes, upgrades, enzovoorts worden uitgevoerd. De opdrachtnemer verwerkt de updates, hotfixes, upgrades enzovoorts in het LAS zo snel mogelijk en uiterlijk binnen drie maanden nadat de hard- en softwareleverancier deze updates, hotfixes, upgrades heeft doorgevoerd. Als voorbeeld bedoelen we hiermee het volgen van het Microsoft (security)patchbeleid.
17. Opdrachtnemer heeft een vestiging in de Europese Unie en voldoet aan de Algemene Verordening Gegevensbescherming (of GDPR: General Data Protection Regulation) en heeft passende technische en organisatorische (beveiligings)maatregelen genomen die zijn afgestemd op het risico van de gegevensverwerkingen in het LAS en – voor zover van toepassing – in de (interne) bedrijfs- en automatiseringsprocessen. Indien zich binnen het LAS risico's voordoen die mogelijk nadelige gevolgen hebben voor de opdrachtgever, dient de opdrachtnemer aantoonbaar inzicht te geven in de opgetreden risico's, de toegepaste behandelingsstrategieën en de genomen mitigerende maatregelen waarmee de risico's tot een acceptabel niveau zijn teruggebracht.
18. Opdrachtnemer sluit met opdrachtgever een verwerkersovereenkomst conform het meest recente model zoals wordt aangeboden in het Convenant Digitale Onderwijsmiddelen en Privacy, zie <https://www.privacyconvenant.nl/>.
19. De aangeboden applicatie, inclusief de bijdrage van eventueel ingeschakelde subverwerkers die zijn genoemd in de verwerkersovereenkomst met de opdrachtnemer, bevindt zich fysiek binnen de EER, zowel het LAS als de data.
20. Opdrachtnemer werkt onvoorwaardelijk en kosteloos mee met het uitvoeren van een door of namens opdrachtgever of SIVON uit te voeren gegevensbeschermingseffectenbeoordeling (DPIA), eventuele Data Transfer Impact Assessment (DTIA) of Fundamental Rights Impact Assessment (FRIA). Een door of namens Opdrachtnemer uitgevoerde DPIA, DTIA of FRIA volstaat niet. Onder deze verplichting is tevens begrepen het – onder nader te maken geheimhoudingsafspraken - binnen redelijke termijnen (van enkele weken) leveren van gevraagde informatie over verwerkte persoonsgegevens en datastromen, koppelingen alsmede organisatorische en technische beveiligingsmaatregelen en –beleid.
21. Het LAS voldoet aan privacy-by-design en privacy-by-default, zoals opgenomen in norm PR.06 van het Normenkader informatiebeveiliging en privacy, en uitgewerkt in het voorbeelddocument "Privacy by design en privacy by default principes – voorbeelddocument (docx): (<https://normenkaderibp.kennisnet.nl/app/uploads/Privacy-by-design-en-privacy-by-default-Voorbeelddocument.docx>). Hierbij is het LAS standaard zo ingesteld dat deze maximale privacybescherming biedt zonder dat de school of gebruiker daar iets voor hoeft te doen, en privacybescherming niet ten koste gaat van gebruiksgemak. '
22. Persoonsgegevens worden onder door de school in te stellen condities vanuit het LAS uitgewisseld via beveiligde geautomatiseerde koppelingen in plaats van handmatige in- en exports.
23. Export- of downloadfunctionaliteit staat voor medewerkers en gebruikers standaard uit en is in te stellen op basis van rol/autorisatie.
24. Het LAS faciliteert het door de school gevoerde bewaar- en vernietigingsbeleid zoals opgenomen onder norm PR.07 van het Normenkader informatiebeveiliging en privacy (<https://normenkaderibp.kennisnet.nl/privacy/domein-2-processen/pr-07-bewaar-en-vernietigingsbeleid/>). Persoonsgegevens in het LAS zijn (geautomatiseerd of op instructie van de school) gestructureerd te

verwijderen op basis de termijnen zoals opgenomen in het bewaartermijnenoverzicht (<https://normenkaderibp.kennisnet.nl/app/uploads/Bewaartermijnenoverzicht.xlsx>).

25. Op verzoek van de opdrachtgever, bijvoorbeeld n.a.v. een beveiligingsincident of melding van het Nationaal Cyber Security Center, kan de opdrachtnemer verzocht worden om een tussentijdse externe audit uit te laten voeren en de volledige resultaten hiervan te delen. De opdrachtnemer dient na verzoek van opdrachtgever de tussentijdse audit binnen 48 uur uit te laten voeren en de resultaten hiervan direct na ontvangst aan opdrachtgever ter beschikking te stellen. De kosten voor het uitvoeren van de externe audit zijn voor rekening van de opdrachtnemer, tenzij uit de resultaten van de audit onomstotelijk, dus zonder enige twijfel, blijkt dat opdrachtnemer adequaat heeft gehandeld met betrekking tot het onderhavige beveiligingsincident of de onderhavige melding. In een dergelijk geval worden de kosten van de externe audit door opdrachtgever vergoed.
26. Het LAS ondersteunt de school kosteloos bij het door betrokkenen uitoefenen van hun privacyrechten zoals (maar niet beperkt tot) een inzageverzoek of vragen van een kopie van alle persoonsgegevens die in het LAS-dossier van betrokkenen zijn opgenomen. Dit betekent dat de school zelf, dus zonder tussenkomst van opdrachtnemer, op snelle en eenvoudige wijze betrokkenen inzage kan geven in al hun eigen persoonsgegevens, inclusief al die velden, informatie of schermen die niet (standaard) in de gebruikers-app, -applicatie of –pagina getoond worden. Eenvoudig een kopie of inzage geven houdt tevens in dat de school niet aangewezen is op het maken van print-screens om de gevraagde informatie uit het leerlingdossier aan betrokkene te verstrekken. Opdrachtnemer biedt hier zonodig functionaliteit voor aan zoals bijvoorbeeld het bieden van een download-functie (voor AVG-doeleinden) van het gehele individuele leerlingdossier.

DEEL 2 (2/2):BEVEILIGING SERVERRUIMTE

Ten aanzien van de fysieke beveiliging van de serverruimte van het LAS zorgt opdrachtnemer voor het volgende.

- a. Het hostingbedrijf acteert binnen de vigerende AVG-regelgeving en is ISO27001/27002 gecertificeerd.
- b. De systeembeheerders van het hostingbedrijf hebben toegang tot de serverruimte waar de servers van het LAS zich bevinden. Daarnaast hebben systeembeheerders van de opdrachtnemer toegang om werkzaamheden aan de servers te kunnen uitvoeren.
- c. De systeembeheerders hebben een geheimhoudingsverklaring ondertekend.
- d. Het hostingbedrijf houdt een lijst van personen bij die toegang hebben tot de servers.
- e. Het hostingbedrijf heeft een instructie voor hun personeel waarin procedures worden beschreven voor het omgaan met persoonsgegevens en gegevensdragers.
- f. Het hosting bedrijf houdt toezicht op de handhaving van beveiliging.
- g. Wanneer de opdrachtnemer specifieke taken uitbesteedt aan derden, zal de vertrouwelijke omgang met persoonsgegevens in het contract worden vastgelegd. De toegankelijkheid van de persoonsgegevens door derden zal zoveel mogelijk worden beperkt.
- h. Het hostingbedrijf zorgt voor voldoende noodstroom en koeling voorzieningen. Daarnaast heeft het hostingbedrijf voorzieningen om brand te voorkomen en middelen om vroegtijdig in te grijpen bij brand.
- i. Het hostingbedrijf heeft een vestiging met een datacenter in de Europese Unie. De data zijn opgeslagen op dit datacenter in de Europese Unie en valt onder de Algemene Verordening Gegevensbescherming.