Activiteiten	**IBP Normenkader**	**ROSA Certificeringsschema**	**Aanvullende normen**	**Toelichting**	**Wordt aan voldaan (ja/nee)** plus onderbouwing	**Onderbouwing**
Logging die een leverancier zelf uitvoert om risico's op het gebied van cybersecurity te mitigeren. Dit betekent dat een leverancier zelf een beleid, procedure van logging en monitoring moet hebben voor het in continuïteit beschikbaar houden van de applicatie. Het gaat hier met name om netwerk, toegang via het internet om de integriteit en vertrouwelijkheid van data te garanderen.						
Security event logging **Ongebruikelijke activiteiten** worden gelogd, opgeslagen, gedocumenteerd, geanalyseerd en opgevolgd met gepaste maatregelen. De applicatie houdt een registratie of logging van alle mutaties bij die **interpretabel zijn door functioneel beheerders/applicatiespecialisten**. De logging moet beschikbaar zijn via een real-time koppeling. Deze moet beschikbaar zijn in CSV-, xlsx-, pdf-, of ander gangbaar formaat, conform vastgelegde standaarden aangeleverd en moet ook geëxporteerd kunnen worden naar een analysesysteem.	11.04 Security Management Een logregel bevat minimaal informatie over de gebeurtenis of handeling, welke gebruiker deze uitvoert, vanaf welk apparaat dit gebeurt, het resultaat van de actie en een datum en tijdstip van de handeling. Ook activiteiten van systeembeheerders worden vastgelegd in de logging. Er zijn waarborgen dat de logging niet gewijzigd kan worden. Eventuele wijzigingen in logging of pogingen tot het verwijderen van logging dienen vastgelegd te worden in de logging zelf. Er vindt periodieke controle van de logging plaats om ongebruikelijke activiteiten te ontdekken. Grotere organisaties kunnen hiervoor bijvoorbeeld een SIEM (Security Incident en Event Managementsysteem) voor inzetten zodat automatische	Integriteit / Herleidbaarheid (technisch beheer) Herleidbaar wanneer, welke onderdelen/configuraties van de toepassing gewijzigd zijn: - Het is mogelijk om wijzigingen terug te draaien - Naamloze systeemaccounts met uitgebreide rechten zijn toegestaan en (indirect) herleidbaar naar personen - Herleidbaar wanneer de toepassing gewijzigd is - Toegang tot de onderliggende systemen van de toepassing is rolgebaseerd toegewezen - Toegang met root-accounts is	Basismaatregel NCSC en 12.4.2 (p.49 BIO versie 1) BIO-normen: Beperk de **toegang** tot logbestanden en sla deze op in een apart **netwerksegment**. Incidentenonderzoek is nauwelijks mogelijk als aanvallers de logbestanden hebben kunnen aanpassen of verwijderen. Logfaciliteiten en informatie in logbestanden behoren te worden **beschermd** tegen **vervalsing** en **onbevoegde toegang** p.49 BIO versie 1) BIO-normen 12.4.1.3 De informatieverwerkende omgeving wordt **gemonitord** door een **SIEM en/ of SOC** middels detectie-voorzieningen. Deze worden ingezet op basis van een risico-inschatting, mede aan de hand van de aard van de te beschermen gegevens en	Hoe wordt hieraan voldaan? Hoe hebben scholen toegang tot de logging? Via een beheer account? Via een aanvraag proces? Lever bijvoorbeeld een voorbeeld van een log file aan. Welke vorm van logging houdt de leverancier zelf bij ten behoeve van beveiliging van de applicatie om potentiële bedreigingen te identificeren en te bestrijden. Bijvoorbeeld audit, error, security en trace logging. Welke vorm van logging is direct beschikbaar voor schoolbesturen. **Geef een opsomming van:** de in de logging vastgelegde informatiebeveiligingsgebeurtenissen. Een goede basis richtlijn is: (p.49 BIO versie 1) BIO-normen 12.4.1.1 Een logregel bevat minimaal: (a) de gebeurtenis; (b) de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te	Antwoord: Antwoord: Antwoord:	

	controle plaatsvindt en ook om na te gaan of de logging correct plaatsvindt. 6. IT heeft een overzicht van alle logbestanden binnen de organisatie.	gereguleerd, bijvoorbeeld met expliciete notificatie en logging Integriteit / Onweerlegbaarheid Gelogd wordt: inlogactiviteit technisch beheer, aanpassingen configuratie en toepassing Voor de kwaliteit van logging worden best practices gehanteerd (bijvoorbeeld OWASP Logging cheat sheet) De tijd van de applicatie is correct en consistent: wordt gesynchroniseerd met éénzelfde referentietijdbron als aanpalende systemen (binnen een netwerk of organisatie). Deze referentietijdbron is gesynchroniseerd met een publieke tijdsbron. Logging wordt periodiek (bijvoorbeeld maandelijks) gecontroleerd op afwijkende patronen	informatiesystemen, zodat aanvallen kunnen worden gedetecteerd. p.49 BIO versie 1) BIO-normen 12.4.2.3 Er is een (onafhankelijke) interne **audit** procedure die minimaal half jaarlijks toetst op het ongewijzigd bestaan van logbestanden. p.49 BIO versie 1) BIO-normen 12.4.2.4 Oneigenlijk wijzigen of verwijderen van loggegevens of pogingen daartoe worden zo snel mogelijk gemeld als **beveiligingsincident**. Op basis van de memo en het onderzoek van de Autoriteit Persoonsgegevens van januari 2018 https://autoriteitpersoonsgegevens.nl/uploads/imported/01_onderzoeksrapport_movare.pdf **Direct inzichtelijk voor de school voor periodieke controles zijn:** Foutieve inlogpogingen	herleiden tot een natuurlijk persoon; (c) het gebruikte apparaat; (d) het resultaat van de handeling; (e) een datum en tijdstip van de gebeurtenis. Aanvullend f) locatie van de apparatuur en de systeemidentificatie; g) registratie van geslaagde en geweigerde pogingen om toegang te verkrijgen tot het systeem; h) registratie van goedgekeurde en geweigerde gegevens en overige pogingen om toegang te verkrijgen tot bronnen van informatie. i) systeemconfiguratieveranderingen; j) gebruik van speciale bevoegdheden; k) gebruik van systeemhulpmiddelen en -toepassingen; l) bestanden die zijn geopend en het type toegang dat is verkregen; m) netwerkadressen en -protocollen; n) alarmen die worden afgegeven door het toegangsbeveiligingssysteem; o) activering en deactivering van beschermingssystemen, zoals antivirussystemen en inbraakdetectiesystemen; p) verslaglegging van transacties	Antwoord:

		(frequentie, oorsprong, et cetera)		die door gebruikers in toepassingen zijn uitgevoerd.	
Logging betreffende de gebruikerskant van de onderwijsinstelling. Hier ligt de nadruk op activiteiten van gebruikers en koppelingen met andere systemen.					
Activiteiten	**IBP Normenkader**	**ROSA Certificeringsschema**	**Aanvullende normen**	**Toelichting**	**Wordt aan voldaan (ja/nee)**
Audit trails e.g. data addition, modification and deletion, data exports		Integriteit / Herleidbaarheid (gebruikers) / M Herleidbaar wanneer, welke gegevens gewijzigd zijn: - Gebruikers hebben standaard (by default) niet meer rechten dan nodig: least privilege - Het is mogelijk om wijzigingen terug te draaien - Naamloze gebruikersaccounts met uitgebreide rechten zijn toegestaan maar (indirect) herleidbaar naar personen - Herleidbaar wanneer de gegevens gewijzigd zijn - Gebruikers mogen beheerdersrechten hebben	Op basis van de memo en het onderzoek van de Autoriteit Persoonsgegevens van januari 2018 https://autoriteitpersoonsgegevens.nl/uploads/imported/01_onderzoeksrapport_movare.pdf **Mutaties** van studieresultaten (indien van toepassing) Uitgevoerde **imports en exports** Acties en handelingen die gebruikers uitvoeren met persoonsgegevens, zoals raadplegen en mutaties, moeten worden gelogd. De logbestanden moeten periodiek worden gecontroleerd op indicaties van onrechtmatige toegang of onrechtmatig gebruik van gegevens. Deze controles moeten proactief, systematisch en	Lever een voorbeeld van een log file aan Welke logging is direct beschikbaar voor schoolbesturen. Indien niet direct beschikbaar, hoe kunnen schoolbesturen dan toegang krijgen? Geef een opsomming van de in de logging vastgelegde informatie	

		- Wijziging van gegevens is inzichtelijk, zodat een analyse hierop mogelijk is. Integritiet / Onweerlegbaarheid (integritiet van gegevens) / M Gelogd wordt: inlogactiviteit gebruikers en wijziging van (persoons)gegevens. Deze logging wordt alleen gebruikt voor controle of ondersteuning (doelbinding) en minimaal 13 maanden bewaard, tenzij expliciet anders is afgesproken. Voor de kwaliteit van logging lworden best practices gehanteerd (bijvoorbeeld OWASP Logging cheat sheet) Logging wordt periodiek gecontroleerd op afwijkende patronen (frequentie, oorsprong, et cetera)	consequent plaatsvinden. Worden de logbestanden **periodiek** (minstens ieder kwartaal) **gecontroleerd** op indicaties van onrechtmatige toegang. Zo ja, hoe?		

		Vertrouwelijkheid / Logging / M Toegang tot de applicatie (zowel gelukt als mislukt) en lezen van (persoons)gegevens wordt gelogd. Logging is enkel toegankelijk voor bevoegde personen en toegang ertoe wordt apart gelogd			
Log files worden 13 maanden bewaard	SM.04 Normenkader IBP	Integriteit / Onweerlegbaarheid (integriteit van gegevens) / M Deze logging wordt alleen gebruikt voor controle of ondersteuning (doelbinding) en minimaal 13 maanden bewaard, tenzij expliciet anders is afgesproken.	p.49 BIO versie 1) BIO-normen 12.4.2.2 Ten behoeve van de loganalyse is op basis van een expliciete risicoafweging de **bewaarperiode** van de logging bepaald. Binnen deze periode is de beschikbaarheid van de loginformatie gewaarborgd.	Hoelang worden security logs bewaard? Hoelang worden audit trails bewaard? Worden log file in read only bewaard?	