Werkveld	Datum	Instemming/Advies GMR	Vastgesteld CvB
ICT	11 december 2019	A - 11 december 2019	13 januari 2020

2.8.3 | Risico analyse IBP

Inhoudsopgave

1. Risico analyse

Bij Aves heeft alle informatie waarde. Daarom worden alle gegevens waarop dit beleid van toepassing is, geclassificeerd. Het niveau van de beveiligingsmaatregelen is afhankelijk van de classificatie. De classificatie van informatie is afhankelijk van de gegevens in het informatiesysteem en wordt bepaald op basis van risico analyses. Daarbij zijn beschikbaarheid, integriteit en vertrouwelijkheid de kwaliteitsaspecten die van belang voor de informatievoorziening. Aves hanteert bij deze classificatie een tweedeling: gegevens met privacyniveau 1 en 2. Onder privacyniveau 1 vallen documenten die concrete informatie bevatten over leerlingen, hun ouders, medewerkers of derden. Privacyniveau 2 geldt daarmee automatisch voor alle documenten waar dat niet het geval is. Dit houdt de situatie werkbaar en overzichtelijk; elke andere vorm van classificeren heeft een verhoogde werkdruk tot direct gevolg, die in de ogen van de geen recht doet aan de noodzaak van nadere classificatie. Stukken die geoormerkt worden onder privacyniveau 1 worden niet openlijk gepubliceerd zonder dat daar uitdrukkelijk toestemming voor gevraagd en verkregen is van alle personen die in het document genoemd worden.

Twee maal per jaar wordt er een risico analyse gemaakt en bekeken of de maatregelen de juiste impact hebben gehad op de organisatie. We bepalen per risico de kans en impact op onze organisatie.
Kans: kans van het optreden van het risico
1. Klein: kan minder dan jaarlijks voorkomen
2. Groot: kan dagelijks voorkomen

Impact: effect als het risico waarheid wordt, de nadelige gevolgen.
1. Klein: verstoring niet-primaire proces, alleen intern merkbaar
2. Groot: verstoring primair proces, reputatieschade, langdurig

De status is;

- Nog niet gerealiseerd — Dit wordt gepland
- Gerealiseerd — Geen actie nodig
- Herhalen — Herhaaldelijk communiceren van de afspraken

Risico	Niveau	Kans	Impact	Maatregelen	Status
Niet vergrendelen van de werkplek	1	Groot	Groot	– Automatisch vergrendelen van applicaties/netwerk na bepaalde tijd. Alleen mogelijk met Windows 10 – Gebruikers bewust maken van de risico's	– Nog niet gerealiseerd – Herhalen
Achterlaten/verlies/diefstal digitale media: – USB-sticks – Externe harde schijven – Mobiele telefoons – Laptops – Tablets	1	Middel	Groot	– Verbieden van het gebruik van USB-sticks en externe harde schijven. – Goede vergrendeling van privé-apparaten ter bescherming van applicaties t.b.v. schoolwerk.	– Herhalen – Herhalen

				– Privé-apparaten hebben een eigen inlog voor privacygevoelige of schoolinformatie, waardoor andere gebruikers (gezinsleden) niet bij deze gegevens kunnen. – Externe harde schijf alleen met Bitlocker	– Herhalen - Herhalen
Printopdrachten worden direct geprint	1	Groot	Groot	– Beveiligd printen, waarbij iedere gebruiker moet inloggen om printopdrachten uit te printen. – Consumentenprinters mogen niet meer in het netwerk, vanwege de onmogelijkheden van het beheer	– Nog niet gerealiseerd – Gerealiseerd
Diefstal hardware Mobiele telefoon	1	Middel	Groot	– Goede inbraakbeveiliging	– Gerealiseerd – Nog niet gerealiseerd

				– Hardware in beheeromgeving via Intune. – BIOS-vergrendeling	– Gerealiseerd
	1	Hoog	Hoog	– Surface tablets zijn beschermd met een sterk wachtwoord. – Surface tablets worden via Microsoft Intune beheerd – Mobiele telefoon moet voorzien zijn van een inlogbeveiliging	– Herhalen – Nog niet gerealiseerd – Herhalen
Applicaties: – Office 365/Apple/MDM – Lokale kopie/synchronisatie schijven – Basispoort/Software – Leeromgevingen gekoppeld aan netwerkbeheer – ParnasSys	1	Middel	Groot	– Automatisch inloggen in applicaties mag alleen ingeschakeld worden als het apparaat vergrendeld wordt met een sterk persoonlijk wachtwoord. – Wachtwoorden zijn niet zichtbaar op papier bij de werkplek. Wachtwoorden die	– Herhalen – Herhalen

		bewaard worden op iedere papieren vorm worden vernietigd als deze niet meer gebruikt worden. Ze mogen niet bij het oud papier belanden. – Het is niet toegestaan om dezelfde wachtwoorden meerdere malen te gebruiken voor privacygevoelige software zoals mail en leerling administratie- en volgsystemen. – Softwareleveranciers moeten deelnemen aan het privacy convenant en bereid zijn een verwerkersovereenkomst te tekenen, anders kan bij deze leverancier geen	– Niet gerealiseerd – Gerealiseerd – Niet gerealiseerd

				software(licentie) worden afgenomen. – ParnasSys is voorzien van twee staps verificatie – Microsoft365 voorzien van twee staps verificatie	– Niet gerealiseerd
Papieren dossiers / Adreslijsten – Leerling gegevens – Financiële zaken – Personeelsgegevens	1	Middel	Groot	– Het is niet toegestaan om zonder toestemming van ouders en medewerkers adreslijsten te verspreiden. – Papieren dossiers zijn opgeborgen in afgesloten kasten en/of ruimtes. – Papieren dossiers mogen nooit bij het oud papier, maar dienen vernietigd te worden. – Papieren dossiers worden volgens de vastgestelde termijnen door de school bewaard.	– Herhalen – Herhalen – Herhalen – Gerealiseerd

				– Afspraken met Bibliotheek, Fotograaf, GGD over het delen van NAW gegevens leerlingen.	
Ongewenst delen van content sociale media: – Ouderportalen – Facebookpagina – Twitterpagina – Schoolapp	1	Middel	Groot	– Scholen hebben een overzicht per groep waaruit blijkt of ouders bezwaar hebben gemaakt tegen het publiceren van beeldmateriaal op de website, sociale media of een ander online portaal. – Scholen vragen ouders toestemming voor het publiceren van beeldmateriaal. – Scholen informeren ouders ieder jaar over de gegeven toestemming voor beeldmateriaal	– Gerealiseerd – Gerealiseerd – Gerealiseerd – Gerealiseerd

				– Aves gebruikt alleen foto's waarvan de ouders toestemming hebben gegeven voor het gebruik van deze foto's.	– Gerealiseerd
				– Ouders die geen respons geven, hebben geen akkoord gegeven. Dit betekent dat beeldmateriaal niet gebruikt mag worden.	– Gerealiseerd
				– Bij het gebruik van een schoolapp worden er afspraken gemaakt met ouders het gebruik van de gegevens uit en in de app.	
Aanval: – DDos – Hack – Virus – Phishing mail	2	Groot	Groot	– De netwerkbeheerder zorgt voor een gedegen beveiliging van het netwerk	– Gerealiseerd
				– Scholen waarschuwen de netwerkbeheerder	– Herhalen

				indien zij het gevoel hebben dat zij een virus hebben geopend op hun pc. – De Surface tablets zijn voorzien van Windows Defender en worden door de gebruiker regelmatig geüpdate. – Medewerkers zijn bekend met phishing mail en kunnen deze herkennen.	– Gerealiseerd – Herhalen
Storing van: – Internetverbinding – Applicaties – Netwerkbeheer	2	Klein	Groot	– Eerste contact bij storingen is de netwerkbeheerder. – Internetproviders versturen een mailing om locaties op de hoogte te brengen van werkzaamheden. – Het is voor de school duidelijk wie de provider is mocht de	– Gerealiseerd – Gerealiseerd – Gerealiseerd

				internetverbinding uitvallen. – Bij storingen van het netwerk wordt contact gezocht met de netwerkbeheerder, zij zullen de storing oplossen volgens de SLA	– Gerealiseerd
Wachtwoorden – Om in te loggen op het netwerk – Om in te loggen in software – De pincode van het alarmsysteem – Codes van kluisjes/kluizen en kluisdeuren	2	Groot	Groot	– Fysieke uitingen waarop wachtwoorden of pincodes zichtbaar zijn mogen in het schoolgebouw alleen opgeborgen worden in af te sluiten kasten. – Een wachtwoord bestaat tenminste uit 8 tekens, waarvan minimaal 1 hoofdletter, 1 kleine letter en 1 cijfer. – Wachtwoorden worden in de Cloud opgeslagen in een beveiligd document (Word, Excel,	– Gerealiseerd – Gerealiseerd – Nog niet gerealiseerd

		OneNote) of via speciaal daarvoor bestemde wachtwoordkluizen.	