Werkveld	Datum	Instemming/Advies GMR	Vastgesteld CvB
ICT	22 mei 2023	A - 4 oktober 2023	16-10-2023

2.8.3 | Informatiebeveiliging en privacy

Risicoanalyse

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 privacy niveau 1 en 2.

Privacy niveau 1 vallen documenten die concrete informatie bevatten over leerlingen, hun ouders, medewerkers of derden.
Privacy niveau 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 privacy niveau 1 worden niet openlijk gepubliceerd zonder dat daar uitdrukkelijk toestemming voor gevraagd en verkregen is van alle personen die in het document genoemd worden.

Een 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
Klein: kan minder dan jaarlijks voorkomen
Groot: kan dagelijks voorkomen

Impact: effect als het risico waarheid wordt, de nadelige gevolgen.
Klein: verstoring niet-primaire proces, alleen intern merkbaar
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 op het persoonlijke device na 15 minuten zonder input. – Gebruikers bewust maken van de risico's van het niet vergrendelen.	– Per 1-11-2023 – Herhalen
Achterlaten/verlies/diefstal digitale media: – USB-sticks – Externe harde schijven – Mobiele telefoons – Laptops – Tablets	1	Middel	Groot	– Medewerker van Aves maakt geen gebruik van USB-sticks en externe harde schijven. – Alle Aves apparaten vallen onder Intune en maken gebruik van Bittlocker. – Goede vergrendeling van privé-apparaten ter bescherming van applicaties t.b.v. schoolwerk. Privé-apparaten hebben	– Herhalen – Gerealiseerd – Herhalen

				een eigen inlog voor privacygevoelige of schoolinformatie, waardoor andere gebruikers (gezinsleden) niet bij deze gegevens kunnen. Op prive-apparaten wordt geen beeldmateriaal bewaard.	
Printopdrachten	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	– Per 1-11-2023 – Gerealiseerd
Diefstal hardware Mobiele telefoon	1	Middel	Groot	– Goede inbraakbeveiliging – Hardware in beheeromgeving via Intune. – BIOS-vergrendeling	– Gerealiseerd – Gerealiseerd – Gerealiseerd

Persoonlijk device Aves	1	Hoog	Hoog	– Surface tablets zijn beschermd met een sterk wachtwoord pincode of Windows Hello – Surface tablets worden via Microsoft Intune beheerd – Mobiele telefoon is voorzien zijn van een inlogbeveiliging – Buiten Aves locatie is 2fa na 12 uur noodzakelijk op Microsoft Surface – Inrichting Surface tablet door medewerker alleen via Autopilot	– Herhalen – Herhalen – Herhalen – Per 1-11-2023 - Per 1-11-2023
Cameratoezicht	1	Middel	Groot	– Opnames worden alleen gemaakt met een duidelijk omschreven doel. – Opnames worden alleen na schooltijd gemaakt. – Beelden worden beveiligd opgeslagen.	– Per 1-8-2023 Gerealiseerd

				– Toegang tot de beelden wordt door de directeur bepaald. – Externen krijgen alleen met toestemming van cvb toegang tot de beelden. – Bewaartermijn van beelden is maximaal 4 weken, tenzij een incident is vastgelegd.	
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 of Windows Hello. – Wachtwoorden zijn niet zichtbaar op papier bij de werkplek. Wachtwoorden die bewaard worden op iedere papieren vorm	– Herhalen – Herhalen

		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.	– Herhalen
		– Softwareleveranciers moeten een verwerkersovereenkomst kunnen overleggen, anders kan bij deze leverancier geen software(licentie) worden afgenomen.	– Gerealiseerd
		– ParnasSys is voorzien van twee-staps-verificatie	– Gerealiseerd

				– Microsoft365 voorzien van twee-staps-verificatie	– Gerealiseerd
				– Inloggen buiten de EU is standaard afgeschermd	– Gerealiseerd
				– Synchronisatie van de OneDrive op niet Aves computers **niet** mogelijk	– Per 1-11-2023
				– SharePoint wordt gebruikt als opslag voor documenten van de organisatie.	– Herhalen
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.	– Herhalen
				– Papieren dossiers zijn opgeborgen in afgesloten kasten en/of ruimtes.	– Herhalen
				– Papieren dossiers mogen nooit bij het oud papier, maar dienen vernietigd te worden.	– Herhalen

				– Papieren dossiers worden volgens de vastgestelde termijnen door de school bewaard. – Afspraken met Bibliotheek, Fotograaf, GGD over het delen van NAW gegevens leerlingen.	– Herhalen – Gerealiseerd
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	– Gerealiseerd – Gerealiseerd – Gerealiseerd

		gegeven toestemming voor beeldmateriaal	
		– 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.	– Gerealiseerd
		– WhattsApp wordt niet gebruikt voor het delen van privacy gevoelige informatie	– Herhalen

Aanval: – DDos – Hack – Virus – Phishing mail	2	Groot	Groot	– De netwerkbeheerder zorgt voor een gedegen beveiliging van het netwerk – Scholen waarschuwen de netwerkbeheerder indien zij het idee 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 email en kunnen deze herkennen. – Aves maakt gebruik van de standaard back-up van Microsoft. Deze is 180 dagen.	– Gerealiseerd – Herhalen – Gerealiseerd – Herhalen – Gerealiseerd

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 internetverbinding uitvallen. – Bij storingen van het netwerk wordt contact gezocht met de netwerkbeheerder, zij zullen de storing oplossen volgens de SLA	– Gerealiseerd – Gerealiseerd – Gerealiseerd – Gerealiseerd
Wachtwoorden – Om in te loggen op het netwerk – Om in te loggen in software – De pincode van het alarmsysteem	2	Groot	Groot	– Fysieke uitingen waarop wachtwoorden of pincodes zichtbaar zijn mogen in het schoolgebouw alleen	– Herhalen

– Codes van kluisjes/kluizen en kluisdeuren	opgeborgen worden in af te sluiten kasten. – Een wachtwoord bestaat tenminste uit 8 tekens, waarvan minimaal 1 hoofdletter, 1 kleine letter en 1 cijfer. – Inlog via Windows Hello op de Microsoft Surface – Wachtwoorden worden in de Cloud opgeslagen in een beveiligd document (Word, Excel, OneNote) of via speciaal daarvoor bestemde wachtwoordkluizen.	– Gerealiseerd – Per 1-1-2024 – Herhalen