Informatiebeveiligings- en privacy beleid

Adenium

Naam	Adenium
Van	College van Bestuur
Aan	Alle betrokkenen
Datum	19 april 2023
Betreft	Informatiebeveiligings- en privacy beleid (IBP)
Document	YSKN 11001 – Versie 1.03 *190423*
Bron	Kennisnet

Versie	Datum	Auteur	Omschrijving
1.0	261022	Luuk Nicolai(kwartiermaker Flexfg)	Eerste conceptversie IBP-beleid
1.01	250123	Focusgroep	Opmerkingen
1.02	080323	Focusgroep	Wijzigingen tekstueel
1.03	190423	Focusgroep	Advies

Toelichting

Het organiseren van informatiebeveiliging en privacy op school begint met een IBP-beleid. Hierin leg je vast welke uitgangspunten je hanteert bij het beveiligen van informatie en het garanderen van privacy van medewerkers en leerlingen. Én welke maatregelen, procedures en afspraken hierbij horen. Daaronder vallen ook alle maatregelen die je moet nemen om aan de AVG te voldoen. Tot slot vermeld je in je IBP-beleid wie verantwoordelijk is voor de uitvoering van IBP binnen jouw organisatie.
Het is belangrijk dat iedereen op school weet dat er een IBP-beleid is en hoe ze het kunnen vinden. Je IBP-beleid is niet statisch. Nieuwe wet- en regelgeving, maar ook nieuwe processen en systemen kunnen betekenen dat je je beleid periodiek evalueert en zo nodig aanpast.

Advies Focusgroep:

De focusgroep adviseert het beleidsstuk “Informatiebeveiligings- en privacybeleid” YSKN 11001 te accorderen en te implementeren in alle relevante beleidsterreinen binnen Adenium. Er zijn enkele adviezen gegeven ten aanzien van de tekstuele opmaak en de interpunctie. Die zijn in dit beleidsstuk verwerkt.
Namens de Focusgroep,
Jan Hoogterp, Zwannie Boersma

Vastgesteld door

Versie	Datum	Naam	Functie
1.03	1-8-2023	J. Boomsma	Lid College van Bestuur
	1-10-2023	Benno Drenth	Voorzitter GMR OPO Furore
	1-10-2023	Wilco Scholtens	Voorzitter GMR PCBO Smallingerland e.o.

1 Het belang van informatiebeveiliging en privacy

Het onderwijs is in toenemende mate afhankelijk van informatie en ICT. Je kunt het beschouwen als een van de belangrijkste zaken naast het geven van onderwijs. Iedere dag is men bezig met persoonsgegevens en het verwerken daarvan. De hoeveelheid informatie, waaronder persoonsgegevens, neemt toe door o.a. ontwikkelingen als gepersonaliseerd leren met ICT. Het is belangrijk om informatie goed te beschermen en veilig en verantwoord met persoonsgegevens om te gaan en je ervan bewust te worden dat ieders gedrag ertoe doet. De afhankelijkheid van ICT en persoonsgegevens brengt nieuwe kwetsbaarheden en risico's met zich mee. Het goed regelen van **informatiebeveiliging en privacy** (afgekort tot IBP) in een IBP-beleid is noodzakelijk om de gevolgen van deze risico's tot een aanvaardbaar niveau te reduceren en de voortgang van het onderwijs en de bedrijfsvoering optimaal te kunnen waarborgen.

2 Toelichting informatiebeveiliging en privacy

- **Toelichting informatiebeveiliging**

Onder informatiebeveiliging wordt verstaan het nemen en onderhouden van een hoeveelheid samenhangende maatregelen zodat de betrouwbaarheid van de informatievoorziening gegarandeerd kan worden.
Informatiebeveiliging richt zich op de volgende aspecten:

- Beschikbaarheid: de mate waarin gegevens en/of functionaliteiten beschikbaar zijn op de juiste momenten.
- Integriteit: de mate waarin gegevens en/of functionaliteiten juist en volledig zijn.
- Vertrouwelijkheid: de mate waarin de toegang tot gegevens en/of functionaliteiten beperkt is tot degenen die daartoe bevoegd zijn.

Onvoldoende informatiebeveiliging kan leiden tot ongewenste risico's in het onderwijsproces en bij de bedrijfsvoering van de instelling. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades en imagoverlies.

- **Toelichting privacy**

Privacy gaat over persoonsgegevens. Persoonsgegevens moeten beschermd worden volgens de huidige wet- en regelgeving. Bescherming van de privacy regelt onder andere onder welke voorwaarden persoonsgegevens verwerkt mogen worden. Persoonsgegevens zijn hierbij alle gegevens die een natuurlijke persoon direct of indirect kunnen identificeren. Onder verwerking wordt elke handeling met betrekking tot persoonsgegevens verstaan. De wet noemt als voorbeelden van verwerking:
Het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekking door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens.

- **Vervlechting informatiebeveiliging en privacy**

Uit voorgaande blijkt dat informatiebeveiliging een belangrijke voorwaarde is voor privacy, terwijl omgekeerd de zorgvuldige omgang met persoonsgegevens noodzakelijk is voor informatiebeveiliging. Informatiebeveiliging en privacy staan naast elkaar en zijn van elkaar afhankelijk, en worden

daarom samengevoegd tot één proces: IBP. Dit beleid, verder te benoemen als IBP-beleid, vormt de basis op informatiebeveiliging en privacy binnen Adenium te regelen en vormt de kapstok voor de onderliggende afspraken en procedures.

3 Doel en reikwijdte

- **Doel**

Informatiebeveiliging en privacy heeft de volgende doelen:

- Het waarborgen van de continuïteit van het onderwijs en de bedrijfsvoering.
- Het garanderen van de privacy van alle betrokkenen waarvan Adenium persoonsgegevens verwerkt, waaronder leerlingen, hun ouders/verzorgers en medewerkers
- Beveiligings- en privacy-incidenten voorkomen en de eventuele gevolgen hiervan beperken.

Het informatiebeveiligings- en privacy beleid (IBP-beleid) is erop gericht om de kwaliteit van de verwerking van informatie en de beveiliging van persoonsgegevens te optimaliseren waarbij er een juiste balans moet zijn tussen privacy, functionaliteit en veiligheid. Het uitgangspunt is dat de persoonlijke levenssfeer van de betrokkene (o.a. medewerkers, leerlingen en hun ouders/verzorgers) wordt gerespecteerd en Adenium voldoet aan relevante wet- en regelgeving.

- **Reikwijdte**

  - Het IBP-beleid binnen Adenium geldt voor alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing). Onder dit beleid vallen ook alle devices van waar geautoriseerde toegang tot het schoolnetwerk verkregen kan worden.

  - Het IBP-beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen Adenium waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op overige betrokkenen waarvan Adenium persoonsgegevens verwerkt.

  - Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van Adenium Hieronder valt tevens de gecontroleerde informatie, die door de school zelf is gegenereerd en wordt beheerd en de niet-gecontroleerde informatie waarop de school kan worden aangesproken. (b.v. uitspraken van medewerkers en leerlingen in discussies, op (persoonlijke pagina's van websites en of social media).

  - Het IBP-beleid geldt voor de geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens, die plaatsvindt onder de verantwoordelijkheid van Adenium evenals op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen. Het IBP-beleid is ook van toepassing op niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

  - IBP-beleid heeft binnen Adenium raakvlakken met:
    - *Algemeen veiligheids- en toegangsbeveiligingsbeleid;* met als aandachtspunten bedrijfshulpverlening, fysieke toegang en beveiliging, crisismanagement, huisvesting en ongevallen
    - *Personeels- en organisatiebeleid;* met als aandachtspunten in- en uitstroom van mede-

werkers, functiewisselingen, functiescheiding en vertrouwensfuncties
- *IT-beleid*; met als aandachtspunten aanschaf, beheer en gebruik van ict en (digitale) leermiddelen
- *Medezeggenschap* van leerlingen, hun ouders/verzorgers en medewerkers

4 Beleid

Adenium hanteert de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging en privacy te bereiken:

- Het bestuur van Adenium neemt de verantwoordelijkheid om ervoor te zorgen dat informatiebeveiliging en privacy geregeld wordt. Het bestuur is hierop aan te spreken en legt hier verantwoording over af. In termen van de wet is het bestuur de verwerkingsverantwoordelijke.

- Adenium voldoet aan relevante wet- en regelgeving.

- Bij Adenium is de verwerking van persoonsgegevens altijd gekoppeld aan een specifiek doel en gebaseerd op één van de wettelijke grondslagen.
  - Toestemming
  - Overeenkomst.
  - Wettelijke verplichting.
  - Bescherming vitale belangen.
  - Vervulling van een taak van algemeen belang of uitoefening van openbaar gezag.
  - Gerechtvaardigd belang.

  Een goede balans tussen het belang van Adenium om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot het gebruik van zijn/haar persoonsgegevens is essentieel. Bij alle verwerkingen van persoonsgegevens op basis van toestemming kunnen betrokkenen te allen tijde hun toestemming herzien. Om persoonsgegevens te mogen verwerken moet je voldoen aan tenminste één van de bovengenoemde zes grondslagen voor verwerking.

- Adenium zal alle betrokkenen helder en actief informeren over de verwerkingen van hun persoonsgegevens, die zowel direct als indirect zijn verkregen. Ook worden alle betrokkenen gewezen op hun rechten met betrekking tot informatie, inzage, verbetering, het wissen van gegevens, beperking van verwerking, verzet, dataportabiliteit en profilering.

- Adenium legt alle verwerkingen van persoonsgegevens vast in een dataregister en zal deze up-to-date houden. Vanuit de AVG is iedere verwerkingsverantwoordelijke (Adenium) verplicht om een verwerkingsregister aan te leggen. Dat doet Adenium in Your Safety Net. Daarin worden de verwerkersovereenkomsten geplaatst en bijgehouden welke data, waar, hoe lang etc. bewaard wordt van elke verwerker. Bij controle van de Autoriteit Persoonsgegevens kan toegang gegeven worden tot dit register. Adenium voldoet hiermee aan de documentatieplicht.

- Binnen Adenium is het veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van iedereen. Hierbij hoort niet alleen het actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie, maar ook van papieren documenten.

- Adenium is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijk-

heid wordt geproduceerd. Daarnaast beheert de school informatie, waarvan het eigendom (auteursrecht) toebehoort aan derden. Medewerkers, leerlingen en ouders worden goed geïnformeerd over de regelgeving rondom het gebruik van informatie d.m.v. de YSKN21004 Gedragscode verantwoord gebruik van bedrijfsmiddelen medewerkers en YSKN 21003A Gedragsregels voor verantwoord gebruik ICT-middelen voor leerlingen (acceptable use policy) en het ict vaardig en mediawijs maken van medewerkers en leerlingen.

- Adenium classificeert informatie en informatiesystemen. De classificatie is het uitgangspunt voor de risicoanalyse (DPIA) en de te nemen maatregelen. Er is een balans tussen de risico's die we willen afdekken en de benodigde investeringen en de te nemen maatregelen. Als er een DPIA wordt afgenomen weeg je de risico's (zijn ze aanvaardbaar en voor welke moet je passende technische/organisatorische maatregelen nemen om op een aanvaardbaar niveau te komen) en wordt de informatie op 3 classificatieniveaus ingedeeld; **B**eschikbaarheid, **I**ntegriteit en **V**ertrouwelijkheid (BIV classificatie)
    - Beschikbaarheid: hoeveel en wanneer data toegankelijk is en gebruikt kan worden.
    - Integriteit: het in overeenstemming zijn van informatie met de werkelijkheid en dat niets ten onrechte is achtergehouden of verdwenen.
    - Vertrouwelijkheid: de bevoegdheden en mogelijkheden tot muteren, kopiëren, toevoegen, vernietigen of kennisnemen van informatie voor een gedefinieerde groep van gerechtigden.

- Adenium sluit met alle leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) verwerkersovereenkomsten af als zij, in opdracht van de school, persoonsgegevens verwerken. Dit geldt ook voor andere organisaties indien er gegevens van leerlingen of medewerkers worden verstrekt.

- Adenium verwacht van alle medewerkers, leerlingen, (geregistreerde) bezoekers en externe relaties dat zij zich 'fatsoenlijk' gedragen met een eigen verantwoordelijkheid. Het is niet acceptabel dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagoverlies. Adenium heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.

- Informatiebeveiliging en privacy is bij Adenium een continu proces, waarbij 2x per jaar wordt geëvalueerd in de Focusgroep en wordt gekeken of aanpassing gewenst is van o.a. gedragscode ICT en internetgebruik, acceptable use policy, afspraken sociale media, wachtwoordbeleid, responsible disclosure.

- Adenium kijkt bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen vóóraf naar de impact hiervan op de informatiebeveiliging en privacy, zodat tijdig de juiste maatregelen genomen kunnen worden. Het afnemen van een DPIA en privacy by design (dataminimalisatie) spelen hierbij een rol.

- Adenium neemt passende technische (beveiligings-)maatregelen om persoonsgegevens en overige data te beschermen tegen de risico's, die de voortgang van het onderwijs, de privacy en de bedrijfsvoering kunnen verstoren.
  Als de infrastructuur elders wordt beheerd en/of gegevens elders worden verwerkt legt Adenium aanvullende afspraken vast over de technische maatregelen.

- Adenium zal alle beveiligingsincidenten vastleggen en datalekken volgens een vast protocol afhandelen en melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen.

5 Uitwerking van het beleid

6 Organisatie

6.1 Rollen en verantwoordelijkheden

De organisatie van IBP gaat over processen, gewoontes, beleid, wetten en regels die van betekenis zijn voor de manier waarop mensen een organisatie sturen, besturen, beheren en controleren. Hierbij spelen de relaties tussen de verschillende betrokkenen en de doelen van de organisatie een rol. Onderstaand overzicht geeft aan welke verantwoordelijkheden en taken bij welke rollen horen bij PCBO Smallingerland e.o.

Schema Rollen en Verantwoordelijkheden

Richtinggevend	**Eindverantwoordelijk**	
	Voorzitter CvB	• Eindverantwoordelijk • IBP-beleidsvorming, -vastlegging en communiceren ervan • Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens • Organisatie IBP inrichten; toewijzen van de taken en rollen • Evalueren toepassing en werking IBP-beleid op basis van rapportages
	Uitwerken beleid / inhoudelijk verantwoordelijk	
	Werkgroep IBP • Projectleider AVG (Privacy Officer) • Functionaris Gegevensbescherming	• Voorbereiden opstellen IBP-beleid, Classificatie/risicoanalyse • Inhoudelijk verantwoordelijk voor uitwerking van het IBP-beleid • Adviseert verwerkingsverantwoordelijke (bestuur/CvB/directie) over IBP • Uitwerken algemeen IBP-beleid naar specifiek beleid op een uniforme manier • Schrijven en beheren van processen, richtlijnen en procedures om de uitvoering van het IBP-beleid te ondersteunen • Evalueren van het IBP-beleid en de maatregelen
	Focusgroep • Controller • medewerker financiële administratie • medewerker P&O/HRM • directeur basisschool • bovenschools ICT medewerker • …	• Adviseert werkgroep IBP over specifieke voorstellen rondom IBP beleid • Adviseert werkgroep IBP over voorstellen voor maatregelen rondom bewustzijn • Evalueert met werkgroep IBP het IBP beleid en maatregelen rondom bewustzijn
	Functionaris voor Gegevensbescherming (FG)	• Toezicht houden op naleving privacy wetgeving • Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoons gegevens • Voorlichting privacy geven en stimuleren van bewustwording • Afwikkeling IBP klachten en incidenten
	• afdelingshoofd	• Risicoanalyse in samenwerking met inhoudelijk verantwoordelijke

	• domeinverantwoordelijke • proceseigenaar	• Toegangsbeleid zowel fysieke toegang als digitale toegang vaststellen en laten goedkeuren door de verwerkings-verantwoordelijke • Regelmatig de (netwerk)toegangsrechten van gebruikers beoordelen, controleren en vastleggen.
Uitvoerend	**Uitvoeren beleid / naleven beleid**	
	• Projectleider AVG (Privacy Officer)	• Incidentafhandeling (registreren en evalueren).
	• Afdeling ICT (Security Officer)	• Technisch aanspreekpunt voor IBP-incidenten.
	• Functioneel beheer/ applicatie-beheer	• Uitvoeren taken conform gegeven richtlijnen en procedures.
	• Alle medewerkers	• Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden.
	Toezicht naleving en communicatie	
	Toezichthouders • FG • College van Bestuur • Raad van Toezicht	• Communicatie naar alle betrokkenen; ervoor zorgen dat medewerkers op de hoogte zijn van het IBP-beleid en de consequenties ervan. • Toezien op de naleving van het IBP-beleid en de daarbij behorende processen, richtlijnen en procedures door de medewerkers. • Voorbeeldfunctie met positieve en actieve houding t.a.v. IBP-beleid. • Implementeren IBP-maatregelen. • Periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen, beoordelingen etc.;
Opmerking: in een aantal gevallen is ook de (G)MR hierbij betrokken.		

De verdere uitwerking van de rollen en taken staan beschreven in bijlage 2.

7 Bijlage 1: Ondersteunende richtlijnen en procedures

Deze bijlage bevat een aantal aanvullende beleidsstukken, richtlijnen, procedures en protocollen. Een aantal zijn vanuit de Algemene Verordening Gegevensbescherming verplicht.

Documenten:	**Aandachtspunten**
Procedure toestemming gebruik beeldmateriaal	(toestemmingsbrief)
Procedure voor verwijderen van gegevens	(bewaartermijnen)
Communicatie rechten betrokkenen	(communicatie richting betrokkenen)
Procesbeschrijving rechten betrokkenen	(proces rondom aanvragen van betrokkenen)
Privacyreglement	
Autorisatiematrix	(wie mogen gegevens inzien, bewerken enz.)
Afspraken gebruik sociale media	(bewustzijn creëren)
Procedure rondom training medewerkers	
Cameratoezicht	
Wachtwoordbeleid	
Responsible disclosure	
Gedragscode ict en internetgebruik (Acceptable use policy	(verantwoord gebruik bedrijfsmiddelen)
Procedure rondom uitwisselen gegevens	(passend onderwijs, leerling dossiers, leerplicht enz.)

Verplicht vanuit de AVG:	
Procesbeschrijving melden datalekken	Infographic
Registratie beveiligingsincidenten	meldformulier YSN
Dataregister om te voldoen aan de registratieplicht Verwerkersovereenkomsten	privacy bijlage
Procedure gegevensbeschermings-effectbeoordeling Risicoanalyse	(DPIA)
Functionaris voor Gegevensbescherming	(communicatie hierover richting medewerkers)

8 Bijlage 2: Organisatie

Deze bijlage beschrijft hoe IBP op drie niveaus wordt georganiseerd.

- Richtinggevend (strategisch)
- Sturend (tactisch)
- Uitvoerend (operationeel)

Om informatiebeveiliging en privacy gestructureerd en gecoördineerd op te pakken worden bij Adenium voor elk niveau een aantal rollen onderkend die aan medewerkers in de bestaande organisatie zijn toegewezen.
Beschreven wordt welke rollen, welke verantwoordelijkheden en taken hebben en wat de documenten zijn die daarbij passen.

Richtinggevend

Eindverantwoordelijke
Het CvB is eindverantwoordelijk voor IBP en stelt het beleid en de basismaatregelen op het gebied van informatiebeveiliging en privacy vast. De toepassing en werking van het IBP-beleid wordt op basis van regelmatige rapportages geëvalueerd. De inhoudelijke verantwoordelijkheid voor IBP is gemandateerd aan de projectleider AVG (Privacy Officer).

Sturend

Werkgroep IBP
Deze groep, bestaande uit de projectleider AVG (Privacy Officer) en de Functionaris Gegevensbescherming, houdt zich op sturend niveau bezig met alles rondom aanpassen IBP.

Focusgroep
In de Focusgroep worden de voorgenomen maatregelen besproken en om advies gevraagd. Dit advies gaat daarna naar het CvB en de verschillende geledingen voor instemming.

Functionaris voor Gegevensbescherming
De functionaris voor gegevensbescherming (FG) houdt binnen Adenium toezicht op de toepassing en naleving van de AVG. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie. De FG zorgt voor het verbeteren en stimuleren van bewustwording rondom IBP, het afhandelen van informatiebeveiligingsincidenten, adviseert over het regelen van privacy, onderhoudt zo nodig de contacten met de Autoriteit Persoonsgegevens (AP) en rapporteert aan de eindverantwoordelijke (het bestuur). De FG heeft regelmatig overleg met de projectleider AVG. De FG is ook de contactpersoon voor klachten en vragen van betrokkenen.

Uitvoerend

Medewerker
Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging en privacy in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in o.a. de "YSKN21004 Gedragscode verantwoord gebruik van bedrijfsmiddelen medewerkers". Daarnaast worden medewerkers in hun dagelijkse werkzaamheden, waar nodig, ondersteund met checklists en formulieren.

Medewerkers worden gevraagd om actief betrokken te zijn bij informatiebeveiliging. Dit kan door meldingen te maken van security incidenten, het doen van verbetervoorstellen en het uitoefenen van invloed op het beleid (individueel of via de MR).

Toezichthouders (FG, College van Bestuur en Raad van Toezicht)
Naleving van het informatiebeveiligingsbeleid is onderdeel van de integrale bedrijfsvoering. Iedere toezichthouder heeft op uitvoerend niveau de taak om:

- Ervoor te zorgen dat zijn medewerkers op de hoogte zijn van het IBP-beleid;
- Toe te zien op de naleving van het IBP-beleid door de medewerkers, waarbij hij/zij zelf een voorbeeldfunctie heeft;
- Periodiek het onderwerp IBP onder de aandacht te brengen in werkoverleggen, beoordelingen etc.;
- Als aanspreekpunt beschikbaar te zijn voor alle personeel gerelateerde IBP-onderwerpen.

Toezichthouders hebben hierbij een voorbeeldrol ten opzichte van hun medewerkers.

Privacy Officer
Privacy Officer (Projectleider AVG) is een rol op sturend niveau. Hij/zij geeft terugkoppeling en advies aan de eindverantwoordelijke (het bestuur) en stuurt de mensen aan op uitvoerend niveau. De Privacy Officer moet:

- Het beleid vertalen naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling
- De uniformiteit bewaken binnen Adenium
- Het aanspreekpunt zijn voor incidenten op het gebied van informatiebeveiliging en privacy
- De verdere afhandeling van incidenten binnen Adenium coördineren

Domeinverantwoordelijke / proceseigenaar
Binnen de holding zijn er verschillende domeinen/processen, zoals ict, personeel (HRM, P&O), administratie, facilitaire- en financiële zaken, onderwijs et cetera. Op elk van deze domeinen/processen is iemand verantwoordelijk om te bepalen op welke wijze IBP daarbinnen wordt vormgegeven in richtlijnen, procedures en instructies.

Deze proceseigenaar is tevens verantwoordelijk voor de risico's die veroorzaakt worden doordat personen of applicaties ten onrechte toegang krijgen tot applicaties. Om deze risico's te verkleinen hebben proceseigenaren de volgende specifieke taken:

- Samen met het CvB/bovenschoolse ICT stellen zij het beleid voor toegang (autorisaties) vast.
- Samen met functioneel beheer en ICT-beheer zien zij erop toe dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn en voor hun werkzaamheden toegang toe moeten hebben.
- Samen met functioneel beheer en ICT-beheer beoordelen zij periodiek de toegangsrechten van de gebruikers.

Security Officer (SO)
De Security Officer vormt een technisch aanspreekpunt als het gaat over informatiebeveiliging voor het management en de medewerkers.

Functioneel beheerder of Applicatiebeheerder
Ieder softwarepakket of (web-)applicatie heeft een beheerder. Bij vragen over de software of applicatie is bekend wie daarvoor aangesproken kan worden. De functioneel beheerder wordt vanuit de domeinverantwoordelijke/proceseigenaar voorzien van een ingevuld werkpakket, bestaande uit richtlijnen, procedures en instructies. Op basis hiervan voert hij zijn of haar taken uit.