Informatiebeveiliging en privacy beleid

Scholen aan Zee

INHOUDSOPGAVE

1 Inleiding

Het onderwijsveld is in toenemende mate afhankelijk van informatie en (meestal geautomatiseerde) informatievoorzieningen. Ook neemt de hoeveelheid informatie toe door ontwikkelingen in digitaal onderwijs. Deze afhankelijkheid van ICT en gegevens brengt nieuwe kwetsbaarheden en risico's met zich mee. Het is van belang om adequate maatregelen te nemen op het gebied van informatiebeveiliging en privacy 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.

1.1 Toelichting informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket aan maatregelen om de kwaliteitsaspecten van de informatievoorziening te garanderen. Deze aspecten zijn:

- **B**eschikbaarheid: de mate waarin gegevens en/of functionaliteiten beschikbaar zijn op de juiste momenten.
- **I**ntegriteit: de mate waarin gegevens en/of functionaliteiten juist en volledig zijn.
- **V**ertrouwelijkheid: de mate waarin de toegang tot gegevens en/of functionaliteiten beperkt is tot degenen die daartoe bevoegd zijn.

Deze zogenaamde BIV classificatie wordt toegepast op alle gegevens die worden verwerkt in de bedrijfs- en onderwijsapplicaties en zo nodig in dataregisters vastgelegd.

Onvoldoende informatiebeveiliging kan leiden tot onacceptabele risico's bij de uitvoering van onderwijs en bij de bedrijfsvoering van de instelling. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades en imagoverlies. Voor het onderwijs wordt door Stichting SURF jaarlijks het Cyberdreigingsbeeld rapport voor het onderwijs uitgebracht. Deze wordt gehanteerd om elk jaar het IBP beleid van Scholen aan Zee aan te toetsen.

1.2 Toelichting privacy

Privacy gaat over persoonsgegevens. Persoonsgegevens dienen beschermd te worden conform huidige wet – en regelgeving.

De Autoriteit Persoonsgegevens houdt in Nederland toezicht op de naleving van de privacywetgeving. Zij hanteren een tien stappenplan ter voorbereiding op de privacywetgeving waarop de privacyaspecten van dit beleidsplan zijn gebaseerd: bewustwording, rechten van betrokkenen, overzicht verwerkingen, gegevensbeschermingseffectbeoordeling, privacy by design & privacy by default, functionaris gegevensbescherming, meldplicht datalekken, verwerkersovereenkomsten, leidende toezichthouder en toestemming.

Bescherming van de privacy regelt onder andere onder welke voorwaarden persoonsgegevens gebruikt mogen worden. Persoonsgegevens zijn hierbij alle gegevens die herleidbaar zijn tot een bepaald individu. Onder verwerking wordt verstaan elke handeling met betrekking tot persoonsgegevens. De wet Algemene Verordening Gegevensbescherming 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.*

1.3 Vervlechting informatiebeveiliging en privacy

Uit voorgaande blijkt dat informatiebeveiliging een belangrijk onderdeel is van privacy, terwijl omgekeerd de zorgvuldige omgang met persoonsgegevens noodzakelijk is voor informatiebeveiliging. Beide begrippen staan naast elkaar, en zijn van elkaar afhankelijk. Dit beleid ligt ten grondslag aan de aanpak van informatiebeveiliging en privacy binnen Scholen aan Zee.

2 Doel en reikwijdte

2.1 Doel

Dit beleid heeft als doelen:

- Het waarborgen van de continuïteit van het onderwijs en de bedrijfsvoering.
- Het garanderen van de privacy van leerlingen en medewerkers waardoor beveiligings- en privacy incidenten en de eventuele gevolgen hiervan worden voorkomen.

Dit beleid is erop gericht om de kwaliteit van de verwerking van informatie en de beveiliging van (persoons)gegevens te optimaliseren waarbij een goede balans moet zijn tussen privacy, functionaliteit en veiligheid. Uitgangspunt is dat de persoonlijke levenssfeer van de betrokkene, met name van medewerkers en leerlingen, wordt gerespecteerd en Scholen aan Zee voldoet aan relevante wet- en regelgeving.

2.2 Reikwijdte

- Het informatiebeveiliging en privacy beleid binnen Scholen aan Zee geldt voor alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties, alsmede voor alle organisatieonderdelen. Onder dit beleid vallen ook alle devices van waar geautoriseerde toegang tot het schoolnetwerk en de applicaties verkregen kan worden.
- De nadruk van het beleid ligt op die toepassingen, die vallen onder de verantwoordelijkheid van Scholen aan Zee. Het beleid heeft zowel betrekking op gecontroleerde informatie, die door de school zelf is gegenereerd en wordt beheerd. Daarnaast is het ook van toepassing op niet-gecontroleerde informatie waarop de school kan worden aangesproken, zoals uitspraken van medewerkers en leerlingen in discussies, of op (persoonlijke pagina's van) websites.
- Het beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen Scholen aan Zee waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties, evenals op andere betrokkenen waarvan Scholen aan Zee persoonsgegevens verwerkt.
- In het beleid ligt de nadruk op de, geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van (persoons)gegevens die plaatsvindt onder de verantwoordelijkheid van Scholen aan Zee evenals op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen. Het beleid is ook van toepassing op niet-geautomatiseerde verwerking van (persoons)gegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.
- Informatiebeveiliging en privacy beleid binnen Scholen aan Zee heeft 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 medewerkers, 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
    - Beleid inzake aanschaf en gebruik van digitale leermiddelen

3 Uitgangspunten

3.1 Algemene beleidsuitgangspunten

De belangrijkste beleidsuitgangspunten bij Scholen aan Zee zijn:

- Informatiebeveiliging en het privacy dient te voldoen aan alle relevante wet- en regelgeving, in het bijzonder aan de Algemene Verordening Gegevensbescherming.
- De verwerking van persoonsgegevens is gebaseerd op wettelijke grondslagen. Hierbij is het van belang een goede balans te hebben tussen het belang van Scholen aan Zee om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot zijn persoonsgegevens.
- Scholen aan Zee sluit voor haar informatiebeveiliging en privacy beleid aan bij landelijke ontwikkelingen zoals het informatiebeveiliging en privacy framework opgesteld door Kennisnet, die een voor het voortgezet onderwijs opgesteld normen- en toetsingskader op basis van de ISO 27001 certificering hanteert om het beleid te ontwikkelen en te toetsen. Onder andere met behulp van de informatiebeveiliging en privacy monitor die jaarlijks door het merendeel van de Middelbaar Beroepsonderwijs instellingen wordt ingevuld.
- Binnen Scholen aan Zee 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 fysieke documenten.
- De school is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert de school informatie, waarvan het eigendom (auteursrecht) toebehoort aan derden. Medewerkers en leerlingen moeten goed geïnformeerd worden over de regelgeving rond het gebruik van informatie.
- Informatie heeft een waarde: financieel, economisch maar zeker ook emotioneel. De waarde van informatie wordt bij Scholen aan Zee geclassificeerd. De classificatie is het uitgangspunt voor de te nemen maatregelen. Vervolgens worden mogelijke risico's geïdentificeerd middels een risicoanalyse, waarbij gebruik gemaakt wordt van de classificatie. Er is een balans tussen de risico's van hetgeen we willen beschermen en de benodigde investeringen en maatregelen.
- Scholen aan Zee sluit met alle leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) verwerkersovereenkomsten af als zij persoonsgegevens ontvangen van de school. Hierbij wordt gebruik gemaakt van de meest recente versie van het privacyconvenant onderwijs (www.privacyconvenant.nl) en de bijbehorende model verwerkersovereenkomst. Dit geldt ook voor overheids- en andere instellingen indien er gegevens van leerlingen of medewerkers worden verstrekt, al dan niet op wettelijke basis.
- Er wordt van alle medewerkers, leerlingen, (geregistreerde) bezoekers en externe relaties verwacht 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. Scholen aan Zee heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.
- Informatiebeveiliging en privacy is bij Scholen aan Zee een continu proces, waarbij jaarlijks wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.
- Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen, wordt bij Scholen aan Zee vanaf de start rekening gehouden met informatiebeveiliging en privacy.

3.2 Uitgangspunten privacy

De vijf vuistregels met betrekking tot de omgang van persoonsgegevens bij Scholen aan Zee zijn:

1. **Doelbepaling en doelbinding**: persoonsgegevens worden alleen gebruikt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden (doelbepaling). Deze doeleinden zijn concreet en voorafgaand aan de verwerking vastgesteld. Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doelen waarvoor ze zijn verkregen (doelbinding).

2. **Grondslag**: verwerking van persoonsgegevens is gebaseerd op een van de wettelijke grondslagen: toestemming, overeenkomst, de wet, publiekrechtelijke taak, vitaal belang van de betrokkene, of gerechtvaardigd belang.
3. **Dataminimalisatie**: bij de verwerking van persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt: het type persoonsgegevens moet redelijkerwijs nodig zijn om het doel te bereiken; ze staan in verhouding staan tot het doel (= proportioneel). Het doel kan niet met minder, alternatieve of andere gegevens worden bereikt. Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk.
4. **Transparantie**: de school legt aan betrokkenen (leerlingen, hun ouders en medewerkers) op transparante wijze verantwoording af over het gebruik van hun persoonsgegevens, alsmede over het gevoerde informatiebeveiliging en privacy beleid. Deze informatievoorziening vindt ongevraagd plaats. Daarnaast hebben deze betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming van hun persoonsgegevens. Ten slotte kunnen betrokkenen zich verzetten tegen het gebruik van hun gegevens.
5. **Data-integriteit**: er zijn maatregelen getroffen om te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn.

Naast de vijf vuistregels hanteert Scholen aan Zee de overige uitgangspunten:

- Persoonsgegevens moeten adequaat worden beveiligd volgens algemeen en breed geaccepteerde beveiligingsnormen.
- Bij alle registraties op basis van toestemming, zal Scholen aan Zee aan de Betrokkene een eenduidige zogenaamde Opt-out procedure worden aangeboden.
- Scholen aan Zee zal informatie die opgeslagen zit in haar systemen nooit delen, verhuren of verkopen aan (commerciele) derden anders dan niet tot een individu te herleiden gepseudonimiseerde gegevens (b.v. ten behoeve van onderzoeksdoeleinden).
- Scholen aan Zee legt geen gegevens vast m.b.t. religie, ras, biometrie, medische gezondheid, geaardheid, behalve op verzoek van de betrokkene.
- Voor gebruik van beeldmateriaal voor promotionele toepassingen wordt telkens apart toestemming gevraagd.

3.3 Privacy by design en privacy by default

Privacy by design houdt in dat Scholen aan Zee al bij het ontwerpen van producten en diensten ervoor zorgt dat persoonsgegevens goed worden beschermd. Maar ook dat er niet meer gegevens worden verzameld dan noodzakelijk voor het doel van de verwerking en dat de gegevens niet langer bewaard worden dan nodig.

Privacy by default houdt in dat Scholen aan Zee technische en organisatorische maatregelen neemt om ervoor te zorgen dat, als standaard, alléén persoonsgegevens verwerkt worden die noodzakelijk zijn voor het specifieke doel dat bereikt moet worden.

4 Wet- en regelgeving

Scholen aan Zee voldoet aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder:

- Wet voortgezet onderwijs
- Wet goed onderwijs en goed bestuur voortgezet onderwijs
- Collectieve Arbeidsovereenkomst voortgezet onderwijs
- Algemene Verordening Gegevensbescherming
- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht

Hiernaast zijn de bepalingen van het convenant ‘Digitale onderwijsmiddelen en privacy 2.0’ leidend bij het maken van afspraken met leveranciers.

Tevens is er een relatie tussen het informatie en privacy beleid en andere voorschriften die gelden bij Scholen aan Zee, te weten:

- De gedragscode
- Het IT reglement
- Het social media protocol

5 Informatiebeveiliging en privacy governance

Het goed, efficiënt en verantwoord leiden van een organisatie wordt vaak aangeduid met de term governance. Het omvat vooral ook de relatie met de belangrijkste belanghebbenden van de instelling, zoals de eigenaren, werknemers, leerlingen, andere afnemers en de samenleving als geheel. Een goed corporate governance-beleid draagt zorg voor de rechten van alle belanghebbenden.

Onderdeel van governance is dat aan alle soorten risico’s en hun onderlinge verwevenheid passende aandacht geschonken wordt. Het is om die reden dat bij Scholen aan Zee op strategisch niveau aandacht schenkt aan informatiebeveiliging en privacy beleid in afstemming met de overige beleidsterreinen en onderdeel van de (budgettaire) planningscyclus.

5.1 Organisatie

De organisatie van informatiebeveiliging en privacy 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. Er wordt daarbij onderscheid gemaakt tussen drie niveaus:

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

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

5.1.1 Richtinggevend

Eindverantwoordelijke
Het college van bestuur is eindverantwoordelijk voor informatiebeveiliging en privacy en stelt het beleid en de basismaatregelen op het gebied van informatiebeveiliging en privacy vast. De toepassing en werking van het informatiebeveiliging en privacy beleid wordt op basis van een jaarlijkse rapportage geëvalueerd en gerapporteerd aan de raad van toezicht.

Functionaris Gegevensbescherming
De Functionaris Gegevensbescherming houdt binnen Scholen aan Zee toezicht op de toepassing en naleving van de Algemene Verordening Gegevensbescherming. De wettelijke taken en bevoegdheden van de Functionaris Gegevensbescherming geven deze functionaris een onafhankelijke positie in de organisatie. De Functionaris Gegevensbescherming zorgt voor het afhandelen van vertrouwelijke informatiebeveiligingsincidenten. De Functionaris Gegevensbescherming is ook de contactpersoon voor klachten en vragen van betrokkenen.

Informatiebeveiliging en privacy coördinator
De informatiebeveiliging en privacy coördinator geeft terugkoppeling en advies aan de eindverantwoordelijke en stuurt de mensen aan op uitvoerend niveau. De informatiebeveiliging en privacy coördinator vertaalt beleid naar richtlijnen, procedures, maatregelen en documenten, bewaakt de uniformiteit en is het aanspreekpunt voor incidenten op het gebied van informatiebeveiliging en privacy.

Projectgroep informatiebeveiliging en privacy
De functionarissen met de drie bovenstaande rollen vormen de projectgroep informatiebeveiliging en privacy vanwaaruit het gehele informatiebeveiliging en privacy beleid wordt aangestuurd, vormgegeven en onderhouden.

5.1.2 Sturend

Proceseigenaar
Binnen de school zijn er verschillende processen, zoals automatisering, personeel, administratie, facilitaire- en financiële zaken, onderwijs etc. Op elk van deze processen is iemand verantwoordelijk om te bepalen op welke wijze informatiebeveiliging en privacy 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 college van bestuur stellen zij het beleid voor toegang vast.
- Samen met functioneel beheer en ICT-beheer zien zij er op toe dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.
- Samen met functioneel beheer en ICT-beheer beoordelen zij regelmatig de toegangsrechten van gebruikers.

5.1.3 Uitvoerend

Leidinggevende
Naleving van het informatiebeveiliging en privacy beleid is onderdeel van de integrale bedrijfsvoering. Iedere leidinggevende heeft op uitvoerend niveau de taak om:
- Er voor te zorgen dat zijn medewerkers op de hoogte zijn van het beveiligingsbeleid.
- Toe te zien op de naleving van het informatiebeveiliging en privacy beleid door de medewerkers, waarbij hij/zij zelf een voorbeeldfunctie heeft.
- Periodiek informatiebeveiliging en privacy onder de aandacht te brengen in werkoverleggen, beoordelingen etc.
- Als aanspreekpunt beschikbaar te zijn voor alle personeel gerelateerde informatiebeveiliging en privacy onderwerpen.

De leidinggevende kan in zijn taak ondersteund worden door de informatiebeveiliging en privacy coördinator.

Functioneel beheerder
De functioneel beheerder wordt vanuit de proceseigenaar voorzien van richtlijnen, procedures en instructies. Op basis hiervan voert hij zijn of haar taken uit.

Medewerker
Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging en privacy in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in o.a. de gedragscode, het IT reglement en het protocol sociale media.

Medewerkers worden gevraagd om actief betrokken te zijn bij informatiebeveiliging en privacy. Dit kan door meldingen te maken van security incidenten, het doen van verbetervoorstellen.

5.2 Projectmatig

Bij elk project (waaronder aanbestedingen) binnen Scholen aan Zee staat informatiebeveiliging en privacy stelselmatig op de agenda en is onderdeel van het projectsjabloon. Er wordt bij elk project waarbij persoonsgegevens worden verwerkt te allen tijde een gegevensbeschermingseffectbeoordeling (GBEB) uitgevoerd om privacy risico's in kaart te brengen, om vervolgens maatregelen te treffen om de risico's te verkleinen.

5.3 Overzicht verwerkingen

Omdat Scholen aan Zee meer dan 250 medewerkers in dienst heeft wordt een overzicht van verwerkingen (dataregister) van persoonsgegevens bijgehouden. Zowel een verantwoordelijke als de door hem ingeschakelde hulppersonen (zogeheten verwerkers) moeten een register bijhouden. De verantwoordelijke is de partij die bepaalt welke persoonsgegevens worden verwerkt, voor welk doel, en met welke middelen. Een verwerker verwerkt persoonsgegevens namens een verantwoordelijke.

Het data register bevat de volgende informatie:

- De naam van de instelling.
- De naam en contactgegevens van de verantwoordelijke.
- De naam en contactgegevens van de functionaris voor gegevensbescherming.
- De doeleinden waarvoor gegevens worden verwerkt en de wettelijke grondslag.
- De categorieën gegevens (zoals NAW-gegevens, contactgegevens, betaalgegevens).
- De categorieën betrokkenen (b.v. leerlingen, medewerkers).
- De gegevens van de verwerkers.
- Informatie over eventuele doorgifte van gegevens naar landen buiten de EU.
- De van toepassing zijnde bewaar- en vernietigingstermijnen van de persoonsgegevens.
- De manieren waarop de persoonsgegevens zijn beveiligd (b.v. encryptie, logische toegangscontrole, pseudonimisering).

Scholen aan Zee hanteert het door Kennisnet ontwikkeld format en heeft dataregisters voor de volgende categorieën betrokkenen:

- (Oud) leerlingen (inclusief gegevens ouders/verzorgers en stagebedrijf begeleiders)
- (Externe) medewerkers

De primaire systemen zijn opgenomen in de dataregisters. De overige systemen zijn onder 'Overig' ondergebracht en bevatten uitsluitend een zeer beperkte gegevens-set bestaande uit naam, e-mail en organisatie-eenheid. Deze primaire systemen zijn:

1. Leerling Informatie Systeem
2. Financieel pakket
3. Personeel en relatiebeheer applicatie
4. Elektronische leeromgeving
5. Rooster applicatie
6. Management informatie systeem
7. Office programmatuur
8. Identity Management Systeem
9. Educatieve content providers
10. Formatieplanning

Er wordt hierbij voornamelijk gewerkt met "off the shelve" software van gerenommeerde leveranciers om de ondersteuning, continuïteit en beveiliging te kunnen waarborgen.

5.4 Service Level Agreements

Een Service Level Agreement is een overeenkomst tussen een software- of IT diensten leverancier en een afnemer. Dit zijn contracten met afspraken en randvoorwaarden. In deze contracten zit standaard een informatiebeveiliging en privacy paragraaf, waarin de verantwoordelijkheden van de leverancier zijn opgenomen. Met alle leveranciers van Scholen aan Zee is een Service Level Agreement afgesproken. Onderdeel van een Service Level Agreement zijn afspraken over de Service Level Rapportages die periodiek (tenminste jaarlijks) worden opgevraagd of beschikbaar gesteld en waarmee het niveau van de dienstverlening kan worden vastgesteld door de proceseigenaar. Een overzicht van de verantwoordelijkheden en afspraken die ten minste onderdeel uitmaken van een Service Level Agreement zijn opgenomen in bijlage 2.

5.5 Verwerkersovereenkomsten

Met alle leveranciers van onderwijs- en bedrijfsapplicaties en educatieve software worden verwerkersovereenkomsten afgesloten. Dit geldt ook voor overheids- en ander instellingen indien er persoonsgegevens van leerlingen of medewerkers worden verstrekt, al dan niet op wettelijke basis. Scholen aan Zee stelt als eis dat de leveranciers volgens de Algemene Verordening Gegevensbescherming handelen. Koppelingen worden uitsluitend op basis van de door Kennisnet ontwikkelde ECK-ID gerealiseerd.

Een overzicht van de verantwoordelijkheden en afspraken die ten minste onderdeel uitmaken van een verwerkersovereenkomst of de bijbehorende privacy bijsluiter zijn opgenomen in bijlage 3.

Scholen aan Zee zal leveranciers die geen verwerkersovereenkomst kunnen of willen aangaan, en daarmee niet voldoen aan de Algemene Verordening Gegevensbescherming, uitsluiten van het leveren van software en/of het uitvoeren van IT dienstverlening. Leveranciers met lopende contracten zonder verwerkersovereenkomst zijn door Scholen aan Zee geregistreerd en worden jaarlijks aangeschreven waarin leveranciers in gebreke worden gesteld. Contracten met deze leveranciers zullen niet worden verlengd.

5.6 Controle en rapportage

De projectgroep informatiebeveiliging en privacy brengt jaarlijks een jaarverslag over het afgelopen jaar en een jaarplan voor het volgende jaar uit. Het jaarplan is mede gebaseerd op:

- De resultaten van de periodieke controles / audits, incidenten, resultaten van risicoanalyses (inclusief genomen maatregelen) en andere initiatieven die het afgelopen jaar hebben plaatsgevonden.
- Controle van de gegevensbeschermingseffectbeoordelingen waarin noodzaak en evenredigheid voor het verwerken van persoonsgegevens in relatie tot het doel worden getoetst.
- De resultaten van de IBP monitor van Kennisnet in vergelijking met de sector.
- Een peer-audit door een andere onderwijsinstelling uit het IBP samenwerkingsverband van Kennisnet.
- Periodieke audit door een externe, daarvoor gecertificeerde, partij.
- Periodieke steekproeven uitgevoerd bij medewerkers op de naleving van het informatiebeveiliging en privacy beleid.

Het informatiebeveiliging en privacy beleid wordt minimaal elke twee jaar getoetst door het directieberaad. Hierbij wordt rekening gehouden met:

- De status van de informatiebeveiliging en privacy als geheel (beleid, organisatie, risico's).
- De effectiviteit van de genomen maatregelen en aantoonbare werking daarvan.

Daarnaast kent Scholen aan Zee een jaarlijkse planning en control cyclus voor informatiebeveiliging en privacy. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het informatiebeveiliging en privacybeleid wordt getoetst.

De volgende aspecten worden meegenomen:

Voor alle overlegmomenten geldt dat deze zoveel mogelijk ingepast worden in bestaande overlegvormen met hetzelfde karakter waarbij op:

- **strategisch** niveau richtinggevend wordt gesproken over organisatie en compliance, alsmede over doelen, scope en ambitie op het gebied van informatiebeveiliging en privacy.
- **tactisch** niveau wordt de strategie vertaald naar plannen, te hanteren normen, evaluatiemethoden, e.d. Deze plannen en instrumenten zijn sturend voor de uitvoering.
- **operationeel** niveau worden de onderwerpen besproken die de dagelijkse bedrijfsvoering (uitvoering) aangaan. Deze overlegvorm wordt decentraal georganiseerd, en indien nodig in elk organisatieonderdeel van Scholen aan Zee.

5.8 Voorlichting en bewustzijn

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging en privacy uit te sluiten. In de praktijk blijkt de mens meestal de belangrijkste speler. Daarom wordt bij Scholen aan Zee het bewustzijn van de individuele medewerkers voortdurend aangescherpt, zodat de kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. We doen dit door:

- Medewerkers, leerlingen, ouders, gasten en externe relaties structureel te informeren over informatiebeveiliging en privacy beleid en maatregelen (bewustwordingscampagnes).
- Te wijzen op het meldpunt datalekken (responsible disclosure), geheimhoudingsverklaring als onderdeel van de arbeidsovereenkomst en de clean desk/screen policy.
- Het uitvoeren van een opleidingsplan voor functionarissen die met persoonsgegevens werken waaronder met name alle proceseigenaren.
- Gebruikers op de eigen verantwoordelijkheid te wijzen als het gaat om updates van de door hen gebruikte besturingssystemen, applicaties en devices en uitleg hierover te geven.
- Periodieke toetsing op kennis en vastleggen daarvan (met name de proceseigenaren).
- De tien gouden regels voor informatie beveiliging in de scholen duidelijk herkenbaar te plaatsen en waar nodig steeds te actualiseren. Zie bijlage 4.

Verhoging van het beveiligingsbewustzijn is een verantwoordelijkheid van de proceseigenaren en de projectgroep informatiebeveiliging en privacy met het college van bestuur als eindverantwoordelijke.

5.9 Classificatie en risicoanalyse

Bij Scholen aan Zee 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 risicoanalyses. Daarbij zijn beschikbaarheid, integriteit en vertrouwelijkheid de kwaliteitsaspecten die van belang zijn voor de informatievoorziening.

We hanteren hierbij de volgende tools en werkwijzen:

- Gegegevensbeschermingseffectbeoordeling.
- Beschikbaarheid Integriteit Vertrouwelijkheid classificatie.
- Documentair Structuur Plan met daarin het archief- en vernietigingsbeleid.
- Controle op datakwaliteit.

Gegegevensbeschermingseffectbeoordeling

Er zijn verschillende methodes om een gegegevensbeschermingseffectbeoordeling uit te voeren. Scholen aan Zee hanteert de methode van NOREA. De gegegevensbeschermingseffectbeoordeling bevat in ieder geval:

- Een systematische beschrijving van de beoogde gegevensverwerkingen en de doeleinden hiervan inclusief de grondslag.
- Een beoordeling van de noodzaak en de proportionaliteit van de verwerkingen.
- Een beoordeling van de privacy risico's voor de betrokkenen.
- De beoogde maatregelen om:
    - De risico's aan te pakken (zoals waarborgen en veiligheidsmaatregelen).
    - Aan te tonen dat we aan de Algemene Verordening Gegevensbescherming voldoen.

Beschikbaarheid Integriteit Vertrouwelijkheid
Deze classificatie is per gegevenscategorie opgenomen in de dataregisters.

Document Structuur Plan
Scholen aan Zee hanteert voor haar document Structuur Plan de selectielijst van de VO-raad.

Controle op datakwaliteit
Controle op datakwaliteit wordt uitgevoerd door periodieke interne audits, jaarlijks door de accountant en door communicatie met externe instanties (DUO, belastingdienst, etc.).

5.10 Beveiligingsincidenten en datalekken

Alle incidenten dienen gemeld te worden bij datalek@scholenaanzee.nl. De afhandeling van deze incidenten volgt een gestructureerd proces, die ook voorziet in de juiste stappen rondom de meldplicht datalekken. Hierbij zijn belangrijke uitgangspunten:

- De verantwoordelijkheden en bevoegdheden in het opvolgingsproces.
- Responsible disclosure (verplichte melding voor medewerkers).
- De registratie van alle incidenten ongeacht of het uiteindelijk een datalek is.
- Bewijsmateriaal die verzamelt wordt een mogelijke rechtsgang wordt bij een externe partij belegd.

In bijlage 5 is de procedure beveiligingsincidenten en datalekken weergegeven.

5.11 Naleving en sancties

De naleving bestaat uit algemeen toezicht op de dagelijkse praktijk van het informatiebeveiliging en privacy proces. Van belang hierbij is dat leidinggevenden en proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Bij Scholen aan Zee wordt actief aandacht besteed aan informatiebeveiliging en privacy bij de aanstelling, tijdens functioneringsgesprekken, door de instelling brede gedragscode, met periodieke bewustwordingscampagnes, etc. Voor de bevordering van de naleving van de Algemene Verordening Gegevensbescherming vervult de Functionaris voor Gegevensbescherming een belangrijke rol. De Functionaris Gegevensbescherming wordt aangesteld door de college van bestuur, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De Functionaris Gegevensbescherming werkt via een door het college van bestuur vast te stellen reglement. Mocht de naleving ernstig tekort schieten, dan kan Scholen aan Zee de betrokken verantwoordelijke medewerkers een sanctie op leggen, binnen de kaders van de collectieve arbeidsovereenkomst en de wettelijke mogelijkheden. Bij Scholen aan Zee is het melden van beveiligingsincidenten en datalekken vastgelegd in een protocol.

6 Beheer en maatregelen

6.1 IT apparatuur van Scholen aan Zee

Vaste apparatuur (zoals een personal computer, monitor, printer of multifunctional) in de gebouwen van Scholen aan Zee mag niet worden verplaatst of meegenomen. Mobiele apparatuur (zoals een laptop, tablet en mobiele datadrager) wordt beheerd door daartoe aangestelde functionarissen. Gebruikers mogen deze apparatuur, na goedkeuring van die functionarissen, binnen de gebouwen gebruiken en binnen dezelfde dag weer in te leveren. Mobiele apparatuur die voor langere tijd aan een gebruiker wordt uitgegeven is voorzien van een gebruikersovereenkomst waarin afspraken staan hoe met de apparatuur om dient te worden gegaan. Zie bijlage 6. Op het moment van inleveren ontvangt de gebruiker een vrijwaringsbewijs. Zie bijlage 7. Dit geldt naast voor medewerkers ook voor leerlingen die in uitzonderlijke situaties apparatuur van Scholen aan Zee in bruikleen krijgen.

Apparatuur is voorzien van encryptie zodanig dat bij verlies of diefstal er geen (persoons)gegevens verloren gaan. Beheer van de encryptiesleutels ligt bij de helpdesk van de afdeling automatisering. Bij verlies van een sleutel kan deze alleen worden hersteld via “face to face” contact met de helpdesk.

Apparatuur is beveiligd tegen bedreigingen van buitenaf d.m.v. een virusscanner en firewall in het netwerk van Scholen aan Zee én op het apparaat zelf. Daarnaast zijn beleidsregels geactiveerd op de apparatuur die onder meer voorkomen dat software kan worden geïnstalleerd

6.2 IT apparatuur van gebruikers

Mobiele apparatuur van gebruikers zelf, zogenaamde Bring Your Own Devices, kunnen zowel via het internet als via het draadloze netwerk van Scholen aan Zee worden gebruikt om bepaalde diensten te benaderen. Om deze diensten te kunnen gebruiken worden er bepaalde beleidsmaatregelen afgedwongen op deze devices waarmee de gebruiker akkoord dient te gaan alvorens toegang te krijgen.

6.3 Toegang tot- en transport van (persoons)gegevens

Met toegang wordt bedoeld het direct opvragen of bewerken van (persoons)gegevens in de daartoe geëigende applicaties. Met transport wordt bedoeld het transporteren van (persoons)gegevens tussen twee of meer gebruikers.

Voor beide situaties geldt dat dit zo veel mogelijk plaatsvindt middels toegang op basis van Single Sign On verkregen via Multi Factor Authenticatie en verbindingen op basis van versleuteling via Secure Socket Layer certificaten.

Gebruikers worden geacht zorgvuldig om te gaan met (persoons)gegevens en zoveel mogelijk te werken met de daartoe geëigende applicaties. Als (persoons)gegevens dienen te worden getransporteerd tussen gebruikers dan is dit uitsluitend toegestaan tussen medewerkers van Scholen aan Zee. Voor transport van (persoons)gegevens naar ontvangers buiten Scholen aan Zee is toestemming van de Functionaris Gegevensbescherming noodzakelijk en dient te worden voorzien van extra versleuteling.

6.4 Verwijdering van apparatuur

Apparatuur die niet langer gebruikt wordt dient ingeleverd te worden bij de afdeling automatisering. Deze apparatuur wordt meervoudig gewist en waar nodig gecertificeerd afgestort. Het is voor gebruikers niet mogelijk om apparatuur over te nemen met uitzondering van de laptop die gedurende de totale levensduur in bruikleen is geweest door een gebruiker.

6.5 Toegang tot IT ruimten

De toegang tot IT ruimten is beperkt. Scholen aan Zee heeft de volgende maatregelen getroffen:

- De afdeling automatisering is voorzien van een elektronische toegangsdeur waarbij alleen personeel van de afdeling automatisering toegang hebben, alleen de helpdesk is voor gebruikers toegankelijk.
- De Main Equipment Rooms zijn voorzien van een elektronische toegangsdeur waar alleen de server- en netwerkbeheerders toegang toe hebben.
- De Satellite Equipment Rooms zijn voorzien van aparte geregistreerde sleutels die alleen in het bezig zijn van personeel van de afdeling automatisering.
- De laad- en loslocatie voor IT apparatuur is direct gekoppeld aan de afdeling automatisering en alleen toegankelijk voor personeel van de afdeling automatisering.
- Toegang tot IT ruimten wordt automatisch geregistreerd in een logboek.
- Derden die in een Main Equipment Room of Satellite Equipment Room werkzaamheden verrichten worden altijd begeleid door personeel van de afdeling automatisering.
- Er zijn altijd minimaal twee personen aanwezig in de Main Equipment Room of in de afdeling automatisering.

6.6 Technische inrichting Main Equipment Room(s)

De Main Equipment Rooms van Scholen aan Zee is ingericht met de volgende uitgangspunten:

- Redundantie op de meest kritische systemen.
- Er zijn onderhoudscontract afgesloten op deze systemen.

Onderdeel van de jaarlijkse evaluatie is de afweging t.b.v. maatregelen die genomen worden met betrekking tot Single Points of Failure en redundantie in relatie tot de kosten.

Voor een uitgebreid overzicht van de getroffen maatregelen, zie bijlage 8.

6.7 Bekabeling

De volgende technische maatregelen zijn genomen in het kader van beveiliging:

- Netwerkaansluitingen in kantoren en lokalen die niet worden gebruikt worden ont-patched.
- Switchpoorten die niet worden gebruikt worden uitgeschakeld.
- Gebruikte switchpoorten zijn voorzien van poortbeveiliging en alleen de daarop aangewezen computer, laptop, access point of telefoon kan van die poort gebruik maken.
- Alle netwerkbekabeling wordt bijgehouden in een patchmanagement applicatie.

6.8 Kloksynchronisatie

De systeemklokken van alle relevante infrastructuur componenten (zoals switches, servers, pc's en appliances) worden automatisch gesynchroniseerd met een betrouwbare bron. In het beheerde netwerk is een redundant uitgevoerde Netwerk Tijd Protocol (NTP) bron geplaatst waarmee elke infrastructuur component zijn systeemklok synchroniseert. Deze NTP-bron synchroniseert op zijn beurt met een geautoriseerde NTP-bron van het internet.

6.9 Wijzigingsbeheer

Wijzigingsbeheer is één van de beheerprocessen uit de zogenaamde Information Technology Infrastructure Library (ITIL). ITIL is een gestructureerde methode voor ICT-beheer. We onderscheiden wijzigingen in twee typen applicaties:

1. Cloud applicaties / Software as a Service (SaaS).
2. Lokale applicaties / On Premise.

Voor applicaties die als SaaS worden aangeboden is het technische beheer uitbesteed aan de leverancier. Het updaten, of anderszins wijzigen van de applicatie wordt door de leverancier gedaan voor het gehele klantenbestand. In de SLA is met de leverancier afgesproken dat de releasenotes worden gedeeld met de afdeling automatisering van Scholen aan Zee voorafgaand aan de wijziging. Releasenotes worden vervolgens aan de proceseigenaren beschikbaar gesteld om medewerkers voor te bereiden op de wijzigingen. Voor de meest belangrijke applicaties is een Ontwikkel Test Acceptatie Productie (OTAP) omgeving ingericht waarin updates kunnen worden getest of op zijn minst een Test of Acceptatie omgeving.

Voor applicaties die lokaal staan wordt het technische beheer uitgevoerd door de afdeling automatisering. Wijzigingen worden uitgevoerd door de afdeling automatisering of in samenspraak met de leverancier.

Voor beide typen applicaties geldt dat het functioneel beheer, en daarmee ook de wijzigingen op dat gebied onder verantwoording van de proceseigenaren worden uitgevoerd door de functionele beheerders.

6.10 Back-up en restore procedures

We onderscheiden back-up en restore procedures in twee typen applicaties:

1. Cloud applicaties / Software as a Service.
2. Lokale applicaties / On Premise.

Voor applicaties die als Software as a Service worden aangeboden is het maken van back-ups uitbesteed aan de leverancier en onderdeel van de beschikbaarheidsafspraken in het Service Level Agreement. Optioneel kan worden overwogen om nog een extra back-up te maken. Jaarlijks wordt dit meegenomen in de evaluatie van het informatiebeveiliging en privacy beleid. NB: voor alle Office 365 onderdelen wordt een extra Cloud back-up gemaakt bij een derde partij.

Voor applicaties die lokaal staan worden back-ups gemaakt door de afdeling automatisering. Voor de back-up schema's zie bijlage 9. Er worden geen structurele restores uitgevoerd. Deze vinden ad-hoc plaats op basis van behoefte.

6.11 Updates en patches

Het uitvoeren van updates en patches is zeer belangrijk voor de beveiliging van systemen. Dagelijks worden er nieuwe kwetsbaarheden ontdekt die mogelijk tot een datalek kunnen leiden. We onderscheiden updates en patches voor twee typen systemen:

1. Cloud systemen / Software as a Service.
2. Lokale systemen / On Premise.

Voor Cloud systemen is het uitvoeren van updates en patches uitbesteed aan de leverancier. Dit is onderdeel van de Service Level Agreement. Voor lokale systemen worden de updates en patches uitgevoerd door de afdeling automatisering eventueel in samenwerking met de leverancier. Updates en patches worden eerst gecontroleerd in verband met mogelijk fouten. Binnen maximaal twee maanden na de uitlevering van een update of patch worden deze in productie doorgevoerd. Kritieke patches met een hoog risicofactor, zoals tegen ransomware worden versneld doorgevoerd.

6.12 Calamiteiten

Onder een calamiteit op het gebied van IT verstaan we een organisatie brede verstoring van de IT dienstverlening. Er zijn maatregelen genomen om de kans hierop ze klein mogelijk te maken behalve door invloeden van buitenaf die niet door Scholen aan Zee te beïnvloeden zijn.

6.13 Netwerkarchitectuur

Netwerkbeheer wordt uitgevoerd door de afdeling automatisering. De netwerkarchitectuur is opgenomen in bijlage 10.

6.14 Toegangsbeleid

We onderscheiden twee typen toegang:

1. Basistoegang tot het netwerk en algemene diensten van Scholen aan Zee.
2. Toegang tot de diverse applicaties en systemen zowel in de Cloud als On Premise.

De basistoegang tot het netwerk en algemene diensten van Scholen aan Zee wordt gevoed vanuit de bronsystemen van Human Resource Management (medewerkers) en het Leerling Volg Systeem (leerlingen). Op basis van status, functie, opleiding, afdeling of groep wordt geautomatiseerd toegang verleend of ontnomen door een Identity Management systeem.

De toegang tot de diverse applicaties geschied vervolgens op basis van Single Sign On, waarbij rollen en rechten worden toegekend. In de dataregisters staan deze autorisatieschema's vermeld.

6.15 Logging

Alle relevant logbestanden van door Scholen aan Zee beheerde systemen worden verzameld in een zogenaamde Security Information & Event Monitoring systeem.

Bijlage 1: Tabel IBP rollen en taken

Niveau	Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen
Richtinggevend / strategisch **(projectgroep informatiebeveiliging en privacy)**	College van bestuur	• Eindverantwoordelijk • IBP-beleidsvorming, -vastlegging en het uitdragen ervan • Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens • Evalueren toepassing en werking IBP-beleid op basis van rapportages • Organisatie IBP inrichten	• Informatiebeveiligings- en privacy beleid • Baseline / basismaatregelen • Reglement FG vaststellen • Privacyreglement vaststellen
	IBP coördinator	• Inhoudelijk verantwoordelijk voor IBP • IBP-planning en controle • Adviseert college van bestuur/directie over IBP • Voorbereiden uitvoeren IBP-beleid, Classificatie/risicoanalyse • Hanteren IBP normen en wijze van toetsen • Evalueren IBP-beleid en maatregelen • Uitwerken algemeen beleid naar specifiek beleid op een uniforme wijze • Schrijven en beheren van processen, richtlijnen en procedures om de uitvoering te ondersteunen	Processen, richtlijnen en procedures IBP, waaronder: • Activiteitenkalender • Protocol beveiligingsincidenten en datalekken • Bewerkersovereenkomsten regelen • Brief toestemming gebruik foto's en video • Opstellen informatie documentatie richting leerlingen, ouders / verzorgers • Security awareness activiteiten • Sociale media reglement • Gedragscode ict en internetgebruik • Gedragscode medewerkers en leerlingen
	Functionaris Gegevensbescherming	• Toezicht op naleving privacy wetgeving • Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens • Afwikkeling klachten en incidenten	• Privacyreglement, • procedure IBP-incident afhandeling • Inrichten meldpunt datalekken
Sturend / tactisch **(proceseigenaren)**	Proceseigenaren waaronder: ict, personeel (HRM / P&O), Facilitair, onderwijs , financiën, inkoop en administratie	• Classificatie / risicoanalyse in samenwerking met IBP coördinator • Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door college van bestuur/directie • Samen met functioneel beheer en ICT beheer er op toezien dat	• Inventariseren waar persoonsgegevens van de school terechtkomen (leveranciers lijst) • Classificatie- en risicoanalyse documenten. Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder:

		gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn. • Samen met functioneel beheer en ICT beheer de toegangsrechten van gebruikers regelmatig beoordelen en controleren.	• Toegangsmatrix diverse informatiesystemen en netwerk
Uitvoerend / operationeel **(leidinggevenden, functioneel beheer, medewerkers)**	Leidinggevende	• Communicatie naar alle betrokkenen; er voor 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.; • Rapporteren voortgang m.b.t. doelstellingen IBP-beleid aan college van bestuur.	Communiceren, informeren en toezien op naleving van o.a.: • IBP in het algemeen • Regels passend onderwijs • Hoe omgaan met leerling dossiers • Wie mogen wat zien • Gedragscode • Omgaan met sociale media • Mediawijs maken
	Functioneel beheer	• Uitvoeren taken conform gegeven richtlijnen en procedures.	
	Medewerker	• Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden.	

Bijlage 2: Onderdelen van een SLA

1. Een beschrijving van de betrokken partijen
2. Een karakterisering van de overeenkomst
3. De functionaliteit van de diensten
4. De prestatie-eisen van de diensten (beschikbaarheid, back-up en restorebeleid, responsetijd, oplostijd, beveiliging, calamiteitenregeling, wijzigingsbeheer, updatebeleid, releasenotes, OTAP inrichting)
5. De geldende restricties (b.v. bandbreedte, aantal gebruikers, opslagruimte)
6. Technische maatregelen die de leverancier heeft getroffen op het gebied van bedrijfsvoering en continuïteit en de daarbij behorende certificeringen
7. Geldigheidsduur, verlenging, wijzigingsprocedures, beëindiging, kostenberekening
8. Escrowregeling mits beschikbaar
9. Geschillenprocedure
10. Service Level Rapportages en met welke frequentie deze beschikbaar worden gesteld
11. Geheimhoudingsclausule
12. Boeteclausule

Bijlage 3: Onderdelen van een verwerkersovereenkomst

1. Het onderwerp van de verwerkersovereenkomst
2. De duur van de verwerking
3. Aard en het doel van de verwerking
4. Het soort en categorieën persoonsgegevens
5. De rechten en verplichtingen van de verantwoordelijke en de verwerker
6. De instructie dat de verwerker alleen na uitdrukkelijke opdracht en instructie van de verantwoordelijke persoonsgegevens zal verwerken
7. De betrokken medewerkers van de verwerker verplicht zijn tot geheimhouding van de persoonsgegevens die de onderwijsinstelling met de verwerker deelt
8. Welke organisatorisch en technisch maatregelen genomen zijn om de persoonsgegevens te beveiligen
9. De contractuele bepalingen onverkort gelden voor door de verwerker ingeschakelde subverwerkers
10. De verplichting van de verwerker om medewerking te verlenen indien betrokkenen hun rechten (inzage, correctie, verwijdering) wensen uit te oefenen
11. Na afloop van de overeenkomst met de verwerker de persoonsgegevens van de verantwoordelijke worden teruggegeven of vernietigd (behoudens een op de verwerker rustende wettelijke bewaarplicht)
12. De verwerker medewerking verleent aan door de verantwoordelijke uit te voeren inspecties en audits
13. De aansprakelijkheid in geval van boetes opgelegd voor de Autoriteit Persoonsgegevens bij het niet voldoen aan de Algemene Verordening Gegevensbescherming of in geval van datalekken

Bijlage 4: 10 gouden regels voor informatiebeveiliging

1. Wachtwoorden zijn strikt persoonlijk. Geef je wachtwoord nooit aan collega's, leerlingen of anderen en bewaar ze op een veilige plek, dus niet in je agenda of op een geel briefje.
2. Het melden van beveiligingsincidenten. Melden via datalek@scholenaanzee.nl is verplicht. Voorbeelden zijn een virusmelding, inbraak of poging daartoe of als jezelf of iemand anders gegevens kan inzien als dat niet de bedoeling is er juist gegevens kwijt zijn. Eventueel kun je ook bellen met de helpdesk als er direct actie nodig is.
3. Geheimhoudingsplicht. Binnen Scholen aan Zee wordt met vertrouwelijke gegevens van onder meer collega's en leerlingen gewerkt. Hou je aan de richtlijnen hoe hiermee om te gaan.
4. Gedragscode Internet- en e-mail gebruik. Ga zorgvuldig om met internet en email, mijdt onveilige situaties en open geen e-mail van onbekenden.
5. Kennisnemen van het informatiebeveiligingsbeleid. Dit beleid met bijbehorende richtlijnen is van kracht. Neem daar kennis van via je leidinggevende.
6. Gegevensverstrekking aan derden via de telefoon. Het uitgangspunt is dat er nooit aan verzoeken om telefonische informatie over betrokkenen wordt tegemoetgekomen. Dit betekent ook dat er geen telefonische informatie over collega's, leerlingen en partners wordt verstrekt aan personen of instanties die beweren namens betrokkene te bellen.
7. Clear desk/clear screen policy. De vertrouwelijke omgang met gegevens houdt in dat elke werkplek zo is ingericht dat onbevoegden niet in jouw afwezigheid aan deze gegevens kunnen komen. Dit betekent dat jij je werkstation bewust dient te vergrendelen m.b.v. de screen-lock functie (Windowstoets + L) wanneer je je werkplek of werkstation verlaat. Ook mogen geen vertrouwelijke stukken zoals dossiers of verslagen onbeheerd op je bureau of in een niet afsluitbare kast blijven liggen. Ook de printer is een werkplek, haal vertrouwelijke gegevens direct na het afdrukken bij de printer weg.
8. Geen vertrouwelijke gegevens in de prullenbak. Zie ook punt 7. Het vernietigen van deze gegevens moet ook op een veilige manier plaatsvinden. Gebruik de papierversnipperaars en/of papiercontainers. Stop vertrouwelijke zaken in ieder geval nooit in de prullenbak of de normale oud-papier bak op je kantoor of werkplek.
9. Aanspreken van onbekende personen. Ben je al een keer in de situatie geweest dat je onbekenden tegenkwam in de met sleutels beveiligde ruimten? Spreek deze persoon of personen aan, stel jezelf voor en vraag wat hij/zij hier komt doen. Personen die niet bevoegd zijn om zich op deze plek te bevinden worden hierdoor op deze overtreding gewezen. Begeleid deze personen naar de persoon die ze willen bezoeken of begeleid ze naar het publieke gedeelte van het pand.
10. Informatiebeveiliging krijg je niet gratis. Het vraagt aandacht, neem het serieus want het is belangrijk en het hoort bij de professionele en bekwame uitvoering van het werk.

Bijlage 5: Procedure beveiligingsincidenten en datalekken

Deze procedure biedt een handleiding voor de professionele melding, beoordeling en afhandeling van beveiligingsincidenten en datalekken. Het doel hiervan is het voorkomen en leren van beveiligingsincidenten en datalekken, het voorkomen van imago schade en bescherming van het personeel, leerlingen en ouders. Gebruikte termen:

- **Beveiligingsincident**; een beveiligingsincident is een gebeurtenis die er voor zorgt of zou kunnen zorgen dat de beschikbaarheid, integriteit en/of vertrouwelijkheid van de informatievoorziening wordt aangetast.
- **Informatievoorziening;** het geheel van mensen, middelen en maatregelen, gericht op de informatiebehoefte van de organisatie.
- **Datalek**; een beveiligingsincident waarbij persoonsgegevens verloren raken of onrechtmatig worden bewerkt (opgeslagen, aangepast, verzonden, vernietigd etc.). Alle datalekken zijn beveiligingsincidenten, maar niet alle beveiligingsincidenten zijn datalekken.
- **Betrokkene**; de persoon van wie de persoonsgegevens zijn gelekt.

Wet- en regelgeving datalekken
Op 1 januari 2016 is de Wet meldplicht datalekken ingevoerd. Door deze meldplicht zijn ook scholen verplicht melding te maken van ernstige datalekken bij de Autoriteit Persoonsgegevens. Het nalaten van deze melding kan leiden tot een fikse boete.
Er is sprake van een datalek als er bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, óf waarbij het niet valt uit te sluiten dat persoonsgegevens verloren zijn gegaan. Er is persoonlijke informatie ‘gelekt’. Een klassiek voorbeeld van een datalek is een hack waarbij een database met persoonsgegevens is gestolen. Maar het verliezen van een usb-stick met daarop de adresgegevens van een klas, is ook een datalek.
De meldplicht geldt voor de verantwoordelijke voor de persoonsgegevens, het college van bestuur. Een leverancier is een bewerker voor de school, de leverancier informeert het college van bestuur direct bij het ontdekken van een datalek. De verantwoordelijke moet altijd zelf de melding doen.

Werkwijze
Uitgangssituatie

- Er is een actueel informatiebeveiliging en privacy beleid;
- Hierin staat o.a. regelgeving m.b.t. aanvaardbaar gebruik van bedrijfsmiddelen en internet.

Om een beveiligingsincident en/of datalek succesvol af te handelen worden er vier rollen erkend:

1. Ontdekker; degene die het beveiligingsincident of datalek op het spoor komt en het proces in werking stelt.
2. Meldpunt; een centrale locatie (bereikbaar via datalek@scholenaanzee.nl) waarbij alle beveiligingsincidenten worden geregistreerd en verder worden verwerkt. De projectgroep IBP opereert achter dit meldpunt onder leiding van de Functionaris Gegevensbescherming.
3. Behandelaar; degene die de oorzaak van het beveiligingsincident kan vinden en kan (laten) repareren. Aansturing vind plaats vanuit de projectgroep IBP onder leiding van de Functionaris Gegevensbescherming.
4. Melder; degene die verantwoordelijk is voor het onderzoek van het beveiligingsincident en het eventueel melden van een datalek bij de Autoriteit Persoonsgegevens. De melding zal worden gedaan door de Functionaris Gegevensbescherming.

De zeven stappen

1. Ontdekken
De Ontdekker merkt een beveiligingsincident op. Via eigen waarneming of via waarneming van een derde. De Ontdekker meldt het beveiligingsincident en bij het meldpunt. Medewerkers van Scholen aan Zee zijn verplicht om een beveiligingsincident te melden bij het meldpunt.

2. Inventariseren
Het Meldpunt bepaalt dan of er voldoende informatie omtrent het beveiligingsincident bekend is. Zo niet, dan zet hij aanvullende vragen uit bij de Ontdekker en/of de Behandelaar. De volgende informatie wordt daarna vastgelegd:

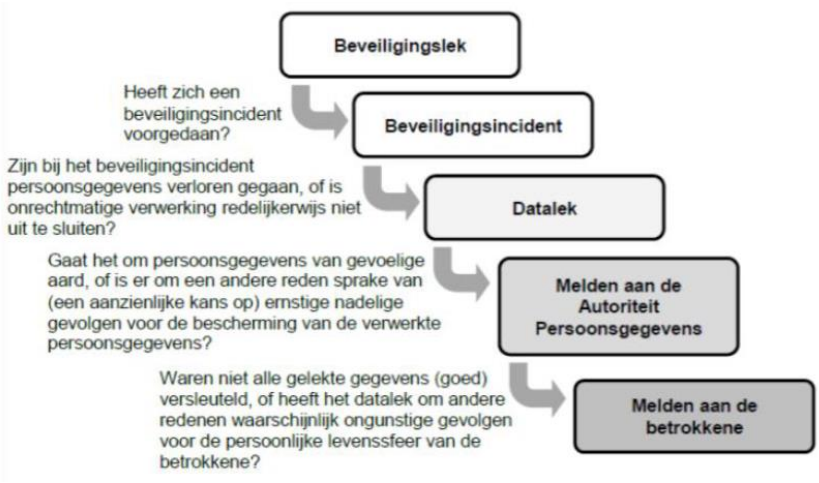
- Samenvatting van het beveiligingsincident, wat is er met de gegevens gebeurd, wat voor gegevens zijn het (bijzondere gegevens of van gevoelige aard)
- Datum/periode van het beveiligingsincident
- Aard van het beveiligingsincident
- Wanneer van toepassing (bij een potentieel datalek):
    - Omschrijving van de groep betrokkenen
    - Aantal betrokkenen
    - Type persoonsgegevens in kwestie
    - Worden de gegevens binnen een keten gedeeld

3. Beoordelen
Wanneer het Meldpunt voldoende informatie heeft verzameld, en een datalek vermoedt, stuurt deze de Melder een verzoek om de verzamelde informatie te bekijken. De Melder beoordeelt de feiten om te bepalen of een melding aan de Autoriteit persoonsgegevens en/of betrokkenen vereist is.
De volgende informatie wordt vastgelegd door de Melder:

- Mogelijke gevolgen voor de persoonlijke levenssfeer van de betrokkenen
- Wordt het datalek gemeld aan de Autoriteit Persoonsgegevens? Waarom niet?
- Wordt het datalek aan betrokkenen gemeld? Waarom niet?
- Hoe worden meldingen gedaan? Wat is de inhoud van de melding?

Bij de beoordeling of er sprake is van een ‘meldingsplichtig datalek’, houd je rekening met het type gegevens, en met de hoeveelheid gegevens. Indien het datalek leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, of als het ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens, moet er gemeld worden.
Van die ernstige nadelige gevolgen of de kans op ernstige nadelige gevolgen is bijvoorbeeld sprake wanneer er heel veel gegevens van een betrokkene of gegevens van heel veel betrokkenen gelekt zijn maar ook wanneer de gelekte gegevens “gevoelig” zijn zoals bijvoorbeeld bijzondere persoonsgegevens over gezondheid, over de financiële of economische situatie van de betrokkene, of als de gegevens kunnen leiden tot stigmatisering van de betrokkene (denk aan het lekken van een leerling die vaak kinderen pest en daarmee gezien kan worden als notoire pester).
Afhankelijk van het soort datalek kan er in deze fase contact opgenomen worden met een advocaat indien daar aanleiding voor bestaat.

De onderstaande beslisboom kan gebruikt worden



4. Repareren
De Behandelaar wordt gevraagd te achterhalen wat de oorzaak van het beveiligingsincident is, bewijzen vast te leggen, schade te beperken en de oorzaak te (laten) verhelpen. De Behandelaar legt onderstaande vast:

- Technische en organisatorische maatregelen die genomen zijn om de inbreuk te verhelpen en verdere inbreuk te voorkomen. Voorgaande voor zover de oorzaak bekend is.
- Zijn de gelekte gegevens onbegrijpelijk voor degenen die er kennis van heeft kunnen nemen? Hoe zijn de gegevens onbegrijpelijk gemaakt (versleuteld)?

5. Melden
Indien de conclusie bij stap 3 is dat er melding gedaan moet worden bij de Autoriteit Persoonsgegevens (en eventueel betrokkenen), dan zal de Melder dit binnen 72 uur in afstemming met de proceseigenaar doen. De melding bevat alle verzamelde informatie en de getroffen incidentele en structurele technische en organisatorische maatregelen. Het lek wordt gemeld bij het meldloket datalekken: https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0.
Elk Datalek wordt gemeld bij het college van bestuur. Deze informeert de raad van toezicht.

6. Vastleggen
Alle informatie, die in de voorafgaande stappen is ingewonnen of ontstaan, wordt gearchiveerd door de Functionaris Gegevensbescherming waarmee het incident is afgesloten. Het Meldpunt verstuurt een samenvatting van de afhandeling van het incident aan de Ontdekker.

7. Informeren betrokkene: leerling en/of zijn ouders
Heeft het datalek waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene? Dan moet het datalek ook aan de betrokkenen zelf worden gemeld. Dat zijn medewerkers, leerlingen (of hun ouders als zij jonger zijn dan 16 jaar). In principe kan er van worden uitgaan dat het lekken van gevoelige aard gemeld moet worden bij de betrokkenen. Let op: als er persoonsgegevens zijn gelekt maar die zijn beveiligd of versleuteld, en de gelekte data zijn onbegrijpelijk of ontoegankelijk voor anderen, dan hoeft dat toch niet aan betrokkenen te worden gemeld. Denk aan het lekken van een beveiligde én versleutelde database met gebruikersnamen en wachtwoorden.

Vastlegging en monitoring beveiligingsincidenten en datalekken
De Functionaris Gegevensbescherming van Scholen aan Zee registreert van ieder beveiligingsincident de benodigde gegevens. De Functionaris Gegevensbescherming van Scholen aan Zee maakt jaarlijks een analyse van de meldingen van beveiligingsincidenten en datalekken.
In de analyse wordt ingegaan op eventuele structurele ontwikkelingen, en of de noodzaak bestaat om maatregelen te nemen om herhaling te voorkomen.
Het collge van bestuur de raad van toezicht wordt geïnformeerd over de uitkomsten van de analyse.

Communicatie
In afstemming met de communicatieadviseur wordt er een communicatieplan opgesteld met daarin de volgende afspraken:

- Wanneer en op welke wijze wordt het college van bestuur geïnformeerd?
- Wie neemt het definitieve besluit om de melding bij de AP te doen en is hiervoor eindverantwoordelijke?
- Welke informatie moeten de betrokkene ontvangen,
    - welke gegevens op welke manier zijn blootgesteld
    - wat de gevolgen kunnen zijn
    - welke maatregelen de betrokkene eventueel zelf kan nemen
    - welke maatregelen Scholen aan Zee heeft genomen om herhaling te voorkomen
    - gegevens van contactpersoon binnen Scholen aan Zee voor het beantwoorden van vragen.
      Hiervoor wordt een standaard brief opgesteld.
- Namens wie wordt de brief ondertekend, het college van bestuur van Scholen aan Zee of namens de schooldirecteur?
- Wat wordt er door wie in de media gecommuniceerd (indien noodzakelijk)?

Rechtsgang
Op het moment dat een rechtszaak volgt uit een beveiligingsincident of datalek wordt een daarvoor gecertificeerd bedrijf ingehuurd om bewijsmateriaal uit de systemen te verzamelen en als bewijslast in te dienen.

Bijlage 6: Gebruikersovereenkomst apparatuur

[losse bijlage]

Bijlage 7: Vrijwaringsbewijs apparatuur

[losse bijlage]

Bijlage 8: Maatregelen Main Equipment Room(s)

De volgende technische maatregelen zijn genomen in het kader van beveiliging en beschikbaarheid:

- Er zijn twee Main Equipment Rooms op aparte locaties ingericht, verbonden met meervoudige glasvezelaansluitingen, waarbij één Main Equipment Room fungeert als primaire locatie en één als secundaire locatie.
- Het Storage Area Netwerk waar alle gegevens zijn opgeslagen is redundant uitgevoerd over beide Main Equipment Rooms.
- Het (virtuele) serverpark is redundant uitgevoerd over beide Main Equipment Rooms.
- De back-up voorziening is redundant uitgevoerd over beide Main Equipment Rooms.
- De primaire Main Equipment Room is voorzien van een aggregaat, no-break installaties, blus-installatie en klimaatcontrole.
- De secundaire Main Equipment Room is voorzien van no-break installatie en klimaatcontrole.
- Internet toegang is redundant uitgevoerd over beide Main Equipment Rooms.
- Telefonie is redundant uitgevoerd over beide Main Equipment Rooms.
- Onderhoudscontracten zijn afgesloten met voor alle kritieke apparatuur met minimaal een 5x8 onderhoudsvenster.

Bijlage 9: Back-up schema

Cloud applicaties / Software as a Service.

- Exchange Online : gemiddeld 2x per dag, minimaal 1x per dag
- OneDrive : gemiddeld 4x per dag
- SharePoint : gemiddeld 4x per dag
- Office groups : gemiddeld 4x per dag

Lokale applicaties / On Premise.
Voor alle lokale systemen geldt:

- Elke maandag, dinsdag, woensdag, donderdag incrementele back-up
- Wekelijks synthetisch volledig (begint vrijdag, eindigt zaterdag)
- 28 dagen retentie op dagelijkse back-up
- 180 dagen retentie op wekelijkse volledige back-up
- 365 dagen retentie op maandelijks volledige back-up
- 2555 dagen retentie op jaarlijkse volledige back-up

Bijlage 10: Netwerkarchitectuur