Informatiebeveiliging en privacy beleid (IBP)

Auteur:
Raymond Wannée

Datum en versie:
15 februari 2022

Classificatie

Openbaar	Dit document mag zonder beperkingen gedeeld en gepubliceerd worden
Intern	Dit document mag alleen worden ingezien door medewerkers en relevante samenwerkingspartners van de HSV
Vertrouwelijk	Dit document mag alleen worden ingezien door een beperkt aantal geautoriseerde/bevoegde medewerkers van de HSV.
Geheim	Alleen de volgende personen hebben recht op inzage: NVT.

Inhoudsopgave

Belangrijke begrippen

Algemene Verordening Gegevens Bescherming (AVG)	De AVG is een Europese Informatiebeveiliging- en privacywetgeving. De AVG zorgt onder meer voor: ▪ versterking en uitbreiding van privacyrechten; ▪ meer verantwoordelijkheden voor organisaties; ▪ dezelfde, stevige bevoegdheden voor alle Europese privacytoezichthouders, zoals de bevoegdheid om boetes tot 20 miljoen euro op te leggen.
Autoriteit persoonsgegevens (AP)	De AP is een zelfstandig bestuursorgaan en houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens.
Persoonsgegevens	Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ; als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer(BSN of personeelsnummer), locatiegegevens (adres), een online identificator (IP-adres) of van één of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.
Bijzondere persoonsgegevens	Bijzondere persoonsgegevens zijn gegevens die informatie geven over: godsdienst of levensovertuiging, ras, politieke voorkeur, gezondheid of seksuele leven. De verwerking van deze gegevens is in principe verboden tenzij kan worden aangetoond dat er wordt voldaan aan één van de uitzonderingsgrondslagen.
Datalek	Onrechtmatige toegang tot, vernietiging, wijziging en vrijkomen van persoonsgegevens.
Gegevensverwerking ‘verwerken’	Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

1. Inleiding

Om goed en eigentijds onderwijs te kunnen bieden, leerlingen te begeleiden, leermiddelen te verschaffen en de continuïteit/kwaliteit van het onderwijs en de bedrijfsvoering te kunnen waarborgen hebben we vanzelfsprekend (persoons)gegevens nodig van leerlingen, ouders en medewerkers.

Het onderwijsveld is in toenemende mate afhankelijk van informatie en (meestal geautomatiseerde) informatievoorzieningen. Ook neemt de hoeveelheid informatie toe door ontwikkelingen als gepersonaliseerd leren met ICT. 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 (verder: IBP) 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 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:

- 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 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.

1.2 Privacy

Privacy gaat over persoonsgegevens. Persoonsgegevens dienen beschermd te worden conform huidige wet – en regelgeving. Bescherming van de privacy regelt onder andere onder welke voorwaarden persoonsgegevens gebruikt mogen worden. Persoonsgegevens zijn hierbij alle gegevens/informatie die (direct of indirect) redelijkerwijs herleidbaar zijn tot een natuurlijke persoon/individu. Onder verwerking wordt verstaan elke handeling met betrekking tot persoonsgegevens. 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.*

De wet onderscheidt bijzondere persoonsgegevens van gewone persoonsgegevens. Dit zijn gegevens waar vanuit de wetgeving extra strenge eisen voor gelden vanwege de gevoelige aard van de gegevens. Voorbeelden van bijzondere persoonsgegevens zijn gegevens die iets zeggen over iemands: gezondheid, ras, godsdienst, politieke voorkeur, strafrechtelijk verleden, seksuele leven en deelname aan vakvereniging.

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. Het onderwerp informatiebeveiliging en privacy wordt afgekort tot IBP. Dit beleid ligt ten grondslag aan de aanpak van informatiebeveiliging en privacy binnen de HSV.

1.4 Privacy by Design

Privacy by Design houdt in dat wij als organisatie al tijdens de ontwikkeling van producten en diensten (zoals informatiesystemen) ten eerste aandacht besteden aan privacy verhogende maatregelen. Ten tweede houden we rekening met dataminimalisatie: we verwerken zo min mogelijk persoonsgegevens, dat wil zeggen alleen de gegevens die noodzakelijk zijn voor het doel van de verwerking. Op deze manier kunnen we een zorgvuldige en verantwoorde omgang met persoonsgegevens technisch afdwingen.

1.5 Privacy by Default

Privacy by default houdt in dat wij technische en organisatorische maatregelen moeten nemen om ervoor te zorgen dat wij, als standaard, alléén persoonsgegevens verwerken die noodzakelijk zijn voor het specifieke doel dat we willen bereiken.

1.6 Proportionaliteit en Subsidiariteit

Al onze gegevensverwerkingen dienen we te toetsen aan de eisen van (1) proportionaliteit en (2) subsidiariteit.

Dat betekent dat we moeten nagaan of:

1. het doel van de verwerking in verhouding staat tot de inbreuk voor de personen van wie we persoonsgegevens verwerken

   en

2. of we het doel niet op een voor de betrokken personen minder ingrijpende manier kunnen bereiken.

1.7 Registratie van verwerkingsactiviteiten: Dataregister

Onder de Algemene Verordening Gegevensbescherming (AVG) heeft elke onderwijsinstelling en meer expliciet elke verwerkingsverantwoordelijke een verantwoordingsplicht. Dit houdt ook in dat onderwijsinstellingen moeten kunnen aantonen dat er in overeenstemming met de AVG wordt gehandeld. Het bijhouden van een register van de verwerkingsactiviteiten (Dataregister) is een onderdeel van deze verantwoordingsplicht. Het register van de verwerkingsactiviteiten bevat informatie over de persoonsgegevens die binnen of ten behoeve van de onderwijsinstelling worden verwerkt. De HSV beschikt over een dataregister en is op aanvraag ter inzage beschikbaar voor iedereen.

2. Doel en reikwijdte

2.1 Doel

Dit beleid heeft als hoofddoelen:

1. *Het waarborgen van de continuïteit en kwaliteit van het onderwijs en de bedrijfsvoering;*
2. *Het waarborgen van de privacy van leerlingen, medewerkers en alle andere betrokkenen bij de HSV.*

Dit beleid is erop gericht om de kwaliteit van de verwerking van informatie en de beveiliging van persoonsgegevens 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 de HSV voldoet aan relevante wet- en regelgeving.

2.2 Reikwijdte

- Het informatiebeveiligings- en het privacy beleid binnen de HSV geldt voor alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur / outsourcing), alsmede voor alle organisatieonderdelen. Onder dit beleid vallen ook alle devices van waar geautoriseerde toegang tot het schoolnetwerk verkregen kan worden.
- De nadruk van het beleid ligt op die toepassingen, die vallen onder de verantwoordelijkheid van de HSV. 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, op (persoonlijke pagina's van) websites.
- Het beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen de HSV waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op andere betrokkenen waarvan de HSV persoonsgegevens verwerkt.
- In het beleid ligt de nadruk op de, geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens die plaatsvindt onder de verantwoordelijkheid van de HSV 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 persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.
- Het IBP-beleid binnen de HSV heeft raakvlakken met:
  - het veiligheidsbeleid;
  - personeels- en organisatiebeleid;
  - IT-beleid;
  - medezeggenschap van leerlingen, hun ouders/verzorgers en medewerkers;
  - beleid inzake aanschaf/inkoop en gebruik van digitale leermiddelen.

3. Uitgangspunten

3.1 Algemene beleidsuitgangspunten

De belangrijkste beleidsuitgangspunten bij de HSV zijn:

a. Informatiebeveiliging en het privacy dient te voldoen aan alle relevante wet- en regelgeving, in het bijzonder alle relevante Onderwijswet- en regelgeving en de Algemene Verordening Gegevensbescherming. De verwerking van persoonsgegevens is gebaseerd op één van de wettelijke grondslagen. Waarbij een goede balans tussen het belang van de HSV om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot zijn persoonsgegevens van belang is.
b. Binnen de HSV 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.
c. Het bevoegd gezag (de bestuurder) is als rechtspersoon eigenaar van de informatie die onder zijn/haar verantwoordelijkheid, op de scholen, wordt geproduceerd/opgeslagen/verwerkt en dus volgens de AVG verwerkingsverantwoordelijke. Daarnaast beheert de school informatie, waarvan het eigendom (auteursrecht) toebehoort aan derden. Medewerkers, ouders en leerlingen moeten goed geïnformeerd worden over de regelgeving rond het gebruik van informatie.
d. Informatie heeft een waarde: financieel, economisch maar zeker ook emotioneel. De waarde van informatie wordt bij de HSV 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. Bijlage 2 geeft een nadere uitwerking hiervan
e. De HSV sluit met alle externe partijen en partners overeenkomsten af als zij persoonsgegevens ontvangen van of namens de organisatie. Hierbij wordt indien mogelijk gebruik gemaakt van de meest recente versie van het convenant 'Digitale leermiddelen privacy' verwerkersovereenkomst van de PO-raad. Dit geldt ook voor overheids- en andere instellingen indien er gegevens van leerlingen of medewerkers worden verstrekt, al dan niet op wettelijke basis.
f. 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. de HSV heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.
g. Informatiebeveiliging en privacy is bij de HSV een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.
h. Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen, wordt bij de HSV vanaf de start rekening gehouden met informatiebeveiliging en privacy. In deze gevallen wordt er een Data Privacy Impact Assessment (DPIA) afgenomen.
i. Het waarborgen van informatiebeveiliging en privacy is een integraal onderdeel van de kwaliteitszorg binnen de HSV.

3.2 Uitgangspunten Informatiebeveiliging- en privacy

De zes uitgangspunten met betrekking tot de omgang van persoonsgegevens bij de HSV:

2. Grondslag: mag je de gegevens verwerken? Toestemming, overeenkomst, wet, vitaal belang, belang van het kind.

3. Dataminimalisatie: Heb ik niet teveel data? Bijvoorbeeld: Uitsluitend gegevens verzamelen die écht nodig zijn om doelen te bereiken. Mensen alleen toegang geven tot wat ze minimaal nodig hebben voor de uitvoering van hun functie.

4. Transparantie/rechten van de betrokkene: heb ik betrokkene voldoende geïnformeerd? Bijvoorbeeld: Leerlingen/ouders begrijpelijk informeren over verzamelde informatie en hun rechten.

5. Data integriteit: bevatten verzamelde persoonsgegevens geen fouten? Wij zorgen er zo goed als mogelijk voor dat de door ons verzamelde gegevens up-to-date gehouden worden en geen fouten bevatten.

6. Informatiebeveiliging: Technische en organisatorische maatregelen: Heb ik de juiste maatregelen getroffen om verlies van persoonsgegevens te voorkomen? Bijvoorbeeld: opbergen van leerlingdossiers in afsluitbare kast en lokaal op slot zetten wanneer er niemand in zit.

3.3 Kwaliteitsbeheersing

Persoonsgegevens moeten adequaat en proportioneel worden beveiligd volgens algemeen en breed geaccepteerde beveiligingsnormen. Er wordt naar gestreefd om de kwaliteitseisen conform ISO/IEC 27001(2) na te streven. ISO/IEC 27001(2) is een wereldwijd erkend kwaliteitsstandaard voor informatiebeveiliging. De AVG geeft nadrukkelijk aan dat ISO/IEC 27001(2) een belangrijk hulpmiddel kan zijn voor het aantoonbaar maken van de eisen en voorschriften vanuit de AVG. Dit doen we door middel van een jaarlijkse evaluatie aan de hand van deze richtlijn.

De ISO/IEC 27001(2) is grofweg als volgt opgebouwd:

Categorie	Doelstelling
1. Informatiebeveiligingsbeleid	Het Bevoegd gezag draagt het belang van informatiebeveiliging actief uit, in overeenstemming met relevante wet- en regelgeving en speelt daar een actieve rol in, in woord en daad.
2. Organisatie van informatiebeveiliging	Het vaststellen van een kader om de implementatie en uitvoering van de informatiebeveiliging binnen de organisatie te initiëren en beheersen.
3. Bewustwording personeel	Het waarborgen dat medewerkers hun verantwoordelijkheden begrijpen, tijdens en na het dienstverband.
4. Beheer van bedrijfsmiddelen/processen	Het identificeren en classificeren van informatiesystemen in de organisatie en op basis daarvan een passend beveiligingsniveau realiseren.
5. Toegangsbeveiliging	Het voorkomen van onbevoegde toegang tot systemen en toepassingen.
6. Cryptografie (versleuteling)	Het zorgen voor correct en doeltreffend gebruik van cryptografie om de vertrouwelijkheid, authenticiteit en integriteit van informatie te beschermen.
7. Fysieke beveiliging	Het voorkomen van onbevoegde fysieke toegang tot, schade aan en interferentie met informatie en informatieverwerkende faciliteiten.
8. Beveiliging van bedrijfsvoering	Het waarborgen van een correcte en veilige bediening van informatieverwerkende faciliteiten en waarborgen van integriteit van operationele systemen.
9. Communicatiebeveiliging	Het beschermen van informatie in netwerken.
10. Acquisitie, ontwikkeling en onderhoud	Adequaat ontwerpen en onderhouden van informatiesystemen.
11. Externe –en leveranciersrelaties	Waarborgen van organisatie informatie die toegankelijk zijn voor derde.
12. Beheer van informatiebeveiligingsincidenten	Doeltreffend beleid m.b.t. tot incidenten.
13. Informatiebeveiligingsaspecten van bedrijfs-continuïteitsbeheer	Inbedden van informatiebeveiliging in de kwaliteitszorg van organisatie.
14. Naleving	Voorkomen van schendingen van wettelijke of statutaire verplichtingen.

4. Wet- en regelgeving

Bij de HSV streven we er altijd naar om zo goed als mogelijk te voldoen aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder:

- Grondwet
- Algemene Verordening Gegevensbescherming (AVG)
- Wet op het primair onderwijs en Wet Expertise Centra
- Wet goed onderwijs en goed bestuur PO/VO
- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht
- Kinderrechten verdrag (artikel 26)

Hiernaast zijn de bepalingen in het convenant 'Digitale onderwijsmiddelen en privacy 3.0 van de PO-raad leidend bij het maken van afspraken met leveranciers van educatieve software en leerling-administratiesystemen.

4.1 Bestuursbeleid

Hieronder een overzicht van ander van toepassing zijnde bestuur beleidsdocumenten die raakvlakken hebben met privacy en informatiebeveiliging:

- Informatiebeveiliging en privacybeleid (IBP);
- privacy protocol;
- Code huiselijk geweld en kindermishandeling;
- klachtenregeling;
- Klokkenluidersregeling;
- non discriminatieverklaring;
- School en veiligheidsprotocol;
- Gedragscode (voor het personeel én voor de leerlingen HSV);
- Persoonlijke en intieme verzorging protocol;
- Verzuimprotocol;
- Beleid beeldmateriaal op internet en schoolapps;
- Sociale media protocol;
- Protocol datalekken;
- COVID-19 protocol;
- Rookbeleid.

5. Organisatie

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.

Dit hoofdstuk beschrijft hoe IBP in de HSV is georganiseerd. 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

5.1 Rollen en verantwoordelijkheden

Om informatiebeveiliging en privacy gestructureerd en gecoördineerd op te pakken worden bij de HSV een aantal rollen onderkend die aan medewerkers in de bestaande organisatie zijn toegewezen.

a. Richtinggevend

Eindverantwoordelijke

Het Bestuur 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 FG en beleidsverantwoordelijke(n).

b. Sturend

Functionaris voor Gegevensbescherming
De functionaris voor gegevensbescherming (FG), houdt binnen de HSV toezicht op de toepassing en naleving van de AVG. De wettelijke taken en bevoegdheden, conform de richtlijnen van de Autoriteit Persoonsgegevens, van de FG geven deze functionaris een onafhankelijke positie in de organisatie. FG heeft regelmatig overleg met beleidsverantwoordelijken en eindverantwoordelijken. De FG is meestal ook de contactpersoon voor klachten en vragen van betrokkenen. De FG is een rol op sturend niveau.

Volgens artikel 39 van de AVG, vervult de FG ten minste de volgende taken:

1. De organisatie informeren en adviseren over hun verplichtingen ten aanzien van de wettelijke vereiste in relatie tot de bescherming van persoonsgegevens.

2. Toezien op naleving van de:

a. AVG;
b. andere Unierechtelijke (lees: Europese) of nationale gegevensbeschermingsbepalingen;

c. van het beleid van het bestuur met betrekking tot de bescherming van persoonsgegevens (inclusief van verantwoordelijkheden, bewustmaking en opleiding van de medewerkers, en de betreffende audits.

3. Gevraagd en ongevraagd advies geven met betrekking tot de gegevensbescherming

4. Met de Autoriteit Persoonsgegevens (AP) samenwerken en voor de AP optreden als contactpunt inzake met verwerking van persoonsgegevens verband houdende aangelegenheden, en – waar passend - overleg plegen over enige andere aangelegenheid aangaande privacy.

5. De FG is verplicht bij de uitvoering van zijn taken rekening te houden met de aan het gebruik van persoonsgegevens verbonden risico's, en met de aard, de omvang, de context en de doelen van het gebruik van die gegevens.

6. Bewustwording in de organisatie vergroten en op niveau houden.

De FG verzamelt informatie om:

- verwerkingsactiviteiten te identificeren;
- de naleving van verwerkingsactiviteiten analyseren en controleren;
- de organisatie te informeren, adviseren en aanbevelingen te maken;
- De uniformiteit te bewaken binnen de HSV.

De FG is:

- Het aanspreekpunt voor incidenten/klachten op het gebied van informatiebeveiliging en privacy.
- Verantwoordelijk voor de verdere afhandeling van incidenten/klachten binnen de HSV.

De AVG verplicht het bestuur om de FG toegang te geven tot alle persoonsgegevens en verwerkingen daarvan. Ook moet de FG de benodigde middelen ter beschikking hebben om zijn taken uit te kunnen voeren, en om zijn deskundigheid in stand te houden. De FG moet bij zijn werk actief ondersteund worden door het Bestuur. De volgende uitgangspunten worden aangehouden:

- Voldoende steun qua financiële middelen, infrastructuur (terrein, faciliteiten, apparatuur);

- Vereiste toegang tot andere diensten, zoals toegang tot de bestanden van personeelszaken, jurist, de ICT-afdeling etc. De FG ontvangt van deze medewerkers of afdelingen de essentiële steun, input en informatie;

- De FG moet de mogelijkheid hebben om bij te blijven op het gebied van gegevensbescherming, waarbij het uitgangspunt moet zijn dat het kennisniveau continu toeneemt;

- De FG is bevoegd om – op eigen initiatief – onderzoek uit te voeren, daarover (ongevraagd) te adviseren, en om van iedereen in de organisatie medewerking daaraan te eisen.

Beleidsverantwoordelijke(n)

De beleidsverantwoordelijken adviseren in samenwerking met de FG het Bestuur en is mede verantwoordelijk voor het organiseren van informatiebeveiliging en waarborgen van privacy binnen de HSV. Tevens zijn de beleidsverantwoordelijke(n) verantwoordelijk voor de aanpassingen in de beleidsstukken.

Schooldirecteuren

Schooldirecteuren hebben de verantwoordelijkheid om het bestuursbeleid te vertalen naar door onderwijspraktijk. Het kan bijvoorbeeld nodig zijn om aanvullende richtlijnen, procedures, maatregelen en documenten op schoolniveau te vervaardigen wanneer het IBP niet voorziet in bepaalde schoolspecifieke zaken. Ook het toezien op handhaving van het beleid op schoolniveau maakt deel uit van deze verantwoordelijkheid.

Meer in het bijzonder:
- in kaart brengen van gegevensverwerkingen/applicaties en gebruikte software.
- signaleren van nieuwe gegevensverwerkingen (bijvoorbeeld nieuwe software) en daar adequate maatregelen op nemen (checken in data register of anders melden bij Functionaris Gegevensbescherming bestuursbureau).
- aanvragen van autorisaties (rechten tot applicaties).
- signaleren en melden van datalekken binnen de school.

Domeinverantwoordelijke / proceseigenaar

Binnen het bestuursbureau zijn er verschillende domeinen/processen zoals: beleid, ICT, HRM (salaris- en personeelsadministratie, verzuim- en re-integratie), secretariaat, communicatie, inkoop en facilitair. Binnen deze domeinen zijn de medewerkers verantwoordelijk om te bepalen op welke wijze IBP daarbinnen wordt vormgegeven in de gehanteerde werkwijze. Bij twijfel dient advies te worden ingewonnen bij FG of beleidsverantwoordelijken.

Ook zijn medewerkers binnen hun domein 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 FG en ICT zien zij er op toe dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.
- Samen met FG en ICT beoordelen zij regelmatig de toegangsrechten van gebruikers.

c. Uitvoerend

ICT
De ICT vormt een technisch aanspreekpunt inzake informatiebeveiliging voor de organisatie. De ICT:

- Ontwikkelt en beheert de informatiesystemen;
- Beheert het netwerk;
- Ondersteunt en adviseert medewerkers;

Functioneel beheerders

De functioneel beheerders van applicaties (zoals YouForce) worden 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.

Medewerkers

Alle medewerkers hebben een verantwoordelijkheid met betrekking tot informatiebeveiliging in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in o.a. de akte van aanstelling, CAO, gedragscode en overig bestuursbeleid. Medewerkers worden gevraagd om actief betrokken te zijn bij informatiebeveiliging. Dit kan door meldingen te maken van (bijna) incidenten/datalekken, het doen van verbetervoorstellen en het uitoefenen van invloed op het beleid (individueel of via de MR). Alle medewerkers hebben tevens de verantwoordelijkheid om nieuwe gegevensverwerkingen te melden en toetsen bij de FG.

Afdelingshoofden

Naleving van het informatiebeveiligingsbeleid 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 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.

De leidinggevende kan in zijn taak ondersteund worden door de FG en beleidsverantwoordelijken.

6. Controle en rapportage

Dit informatiebeveiligings- en privacybeleid wordt minimaal elke twee jaar getoetst en bijgesteld. Hierbij wordt rekening gehouden met:

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

Daarnaast kent de HSV een jaarlijkse evaluatiecyclus voor informatiebeveiliging en privacy. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het informatiebeveiligings- en privacybeleid wordt getoetst.

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 IBP.
- **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 de HSV.

6.1 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 de HSV het bewustzijn van de individuele medewerkers voortdurend aangescherpt, zodat de kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Onderdeel van het beleid zijn de regelmatig terugkerende bewustwordingscampagnes voor medewerkers. Verhoging van het beveiligingsbewustzijn is een verantwoordelijkheid van de FG, beleidsverantwoordelijken en leidinggevende/schooldirecteuren met de bestuurder als eindverantwoordelijke. Tijdens diverse managementbijeenkomsten, teamvergaderingen, professionaliseringsbijeenkomsten en schoolbezoeken is en wordt er aandacht besteed aan informatiebeveiliging en privacy.

6.2 Classificatie en risicoanalyse

Bij de HSV heeft alle informatie waarde, daarom worden alle gegevens waarop dit beleid van toepassing is, geclassificeerd (openbaar, intern, vertrouwelijk en geheim). 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 voor de informatievoorziening. Zie bijlage 2.

6.3 Incidenten en datalekken

Alle incidenten kunnen worden gemeld bij de FG. De afhandeling van deze incidenten volgt een gestructureerd proces, die ook voorziet in de juiste stappen rondom de meldplicht datalekken. Er is een apart protocol met betrekking tot datalekken beschikbaar op het intranet.

6.4 Controle, naleving en sancties

De naleving bestaat uit algemeen toezicht op de dagelijkse praktijk van het IBP proces. Van belang hierbij is dat leidinggevenden en proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Bij de HSV wordt actief aandacht besteed aan IBP bij de aanstelling, tijdens de gesprekkencyclus, met een instellingsbrede gedragscode, met periodieke bewustwordingscampagnes, etcetera.

Voor de bevordering van de naleving van de AVG vervult de Functionaris voor Gegevensbescherming (FG) een belangrijke rol. De FG wordt aangesteld door de bestuurder, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FG zal dan ook jaarlijks onderzoek verrichten naar mogelijke onregelmatigheden in relatie tot het IBP en hierover rapporteren aan het Bestuur.

Mocht de naleving ernstig tekort schieten, dan kan de HSV de betrokken verantwoordelijke medewerkers een sanctie opleggen, binnen de kaders van de CAO en de wettelijke mogelijkheden.

Bij de HSV is het melden van beveiligingsincidenten en datalekken vastgelegd in een protocol/stappenplan. Deze is te vinden op het intranet.

6.5 Onafhankelijk Juridisch advies

De HSV laat zich bij conflicten bijstaan door de geschillencommissie. Indien er sprake is van complexere zaken dan zal de HSV bijgestaan worden door een gespecialiseerd advocatenkantoor.

6.6 Uitgelichte thema’s

In de volgende paragraaf worden enkele thema's uitgelicht die in de dagelijkse praktijk veel aan de orde komen. Om die reden wordt er hieronder extra toelichting gegeven op deze thema's.

a. Wachtwoordbeleid en -instellingen

Het verdient de aanbeveling om voor alle systemen een algemeen beleid ten aanzien van wachtwoordvereisten op te stellen conform volgende richtlijnen:

- Minimum aantal karakters: 8
- Maximale geldigheidsduur: 30-90 dagen
- Complexiteit: ingeschakeld
- Wachtwoordhistorie van 20 wachtwoorden
- Account lockout: 3
- Account lockout duur: meer dan 0 minuten

Hierna is het van belang om dit beleid door te voeren op alle relevante IT systemen, en jaarlijks checks uit te voeren waarbij geverifieerd wordt of wachtwoordvereisten nog conform het wachtwoordbeleid worden afgedwongen. Daarnaast is een adequaat wachtwoordbeheer van belang. Wachtwoorden dienen zodanig opgeslagen te worden dat alleen de geautoriseerde/bevoegde persoon er toegang toe heeft. Waar het proportioneel lijkt, kan de ICT van de HSV een two-factor authentication (extra beveiliging) doorvoeren.

b. Sociale media

Sociale media zoals Twitter, Instagram, Facebook, YouTube en LinkedIn bieden unieke mogelijkheden in relatie tot positieve profilering van onze scholen.

De HSV vertrouwt er op dat medewerkers, gastdocenten, leerlingen, ouders/verzorgers en andere betrokkenen verantwoordelijk omgaan met sociale media.

De HSV heeft een apart social media beleid opgesteld voor onze medewerkers om het gebruik zo goed mogelijk te laten verlopen. Daarnaast maken we afspraken met elkaar over wat niet is toegestaan. Belangrijkste uitgangspunt in onze activiteiten op het gebied van sociale media, is dat we ons net als in de ‘echte’ wereld houden aan de reguliere fatsoensnormen. Het social media beleid is gepubliceerd op het intranet.

c. Applicatie gebruik

Als applicaties persoonsgegevens verzamelen is het van belang om kritisch te zijn op de privacy vriendelijkheid van de applicatie. Relevante vragen zijn daarbij:

- Is de applicatie strikt noodzakelijk voor het geven van onderwijs, begeleiden van leerlingen, verstrekken van leermiddelen en continuïteit van het onderwijsproces?

- Is er een wettelijke grondslag voor het gebruik van de applicatie?
- Verzamelt de applicatie niet teveel gegevens?
- Is er een verwerkersovereenkomst met de leverancier van de applicatie?

Voordat er met een applicatie wordt gewerkt dient deze applicatie gecheckt te worden in het in hoofdstuk 1.7 genoemde data register. Als de applicatie er niet tussen staat dient deze applicatie gemeld te worden bij de Functionaris Gegevensbescherming van de HSV.

d. Gebruik draagbare devices

Het advies is om zo terughoudend mogelijk te zijn in het gebruik van draagbare devices, voor de verwerking van persoonsgegevens. Het verdient de aanbeveling om extra zorg te besteden aan de opslag en beveiliging van draagbare devices. Mocht er met een draagbaar device gewerkt worden, zoals een laptop, is het van belang om zo veel als mogelijk in de beveiligde Google omgeving. Draagbare devices dienen altijd versleuteld te worden met een persoonsgebonden toegangscode.

e. Gebruik van e-mail

E-mail is in onze organisatie een belangrijk communicatiemiddel. Echter, een groot deel van de datalekken wordt veroorzaakt door het gebruik van e-mail. Het is daarom van belang om goed na te denken wanneer je ervoor kiest om de mail te gebruiken voor het doorzetten van persoonsgegevens. Een alternatief is om bestanden met collega's te delen via de Google omgeving. Medewerkers dienen goed de mailadressen van de ontvangers van de mail te controleren. Bij een mail naar meerdere partijen is het aan te bevelen om de BCC te gebruiken.

f. Zorgdossiers

Zorgdossiers zijn een bron van bijzondere persoonsgegevens en bevatten dus zeer gevoelige informatie. Het is van groot belang om met extra zorg om te gaan met deze dossiers. Alleen de professionals die vanuit hun bijdrage aan de geformuleerde zorgbehoefte toegang nodig hebben tot de dossiers, mogen hier toegang tot krijgen. Het is de verantwoordelijkheid van de schooldirecteur om te bepalen wie recht heeft tot toegang van de gegevens.

g. Uitdiensttreding

Medewerkers mogen bij uitdiensttreding geen toegang meer hebben tot de gegevensverwerkingen van de HSV.

Bij uitdiensttreding dient er een signaal vanuit de betreffende school gegeven te worden richting de ICT van de HSV. De ICT zorgt dat de uitgegeven rechten met betrekking tot de toegang tot gegevensverwerkingen worden teruggetrokken door de functioneel beheerders. Dit geldt voor de gegevensverwerkingen/informatiesystemen/applicaties waarbij de rechten centraal verstrekt worden. De overige gegevensverwerkingen/informatiesystemen/applicaties dienen door de Schooldirectie geregeld te worden.

Soort gegevens	**Wettelijke basis**	**Uitleg**
1. Specifieke gevallen	Specifieke wet	Mocht de verwerking buiten de onderstaande situaties vallen is het van belang om de specifieke bewaar c.q. vernietigingstermijn terug te vinden in toepasselijke wet- en regelgeving.
2. Europese subsidie stimuleringsregeling		Tot 10 jaar na vertrek van de betreffende leerlingen moet informatie bewaard worden.
3. Financiële, fiscale en bekostigingsbescheiden	Artikel 172 lid 3 Wet PO Artikel 130a lid 3 Wet VO	7 jaar.
4. Alle gegevens in de leerlingadministratie PO / VO	Artikel 9 lid 1 (juncto artikel 6 lid 1) bekostigingsbesluit WPO Artikel 6 bekostigingsbesluit VO	Tot 5 jaar na uitschrijving betreffende leerling.
5. Leerlingdossier	Advies Autoriteit Persoonsgegevens.	2 jaar na vertrek van leerling.
6. Persoonsgegevens betreffende de gezondheid van leerlingen	Artikel 18a lid 6 (juncto lid 13) Wet PO 17a lid 14 Wet VO	3 jaar na afloop van: (a.) de beoordeling of een leerling is aangewezen op het leerwegondersteunend onderwijs of van het toelaatbaar verklaren van leerlingen tot het praktijkonderwijs of het voortgezet speciaal onderwijs (b.) de advisering over de ondersteuningsbehoefte van de leerling aan het bevoegd gezag van de school, (c.) de toewijzing van ondersteuningsmiddelen of voorzieningen aan de school.
7. Sollicitatiegegevens	Advies Autoriteit Persoonsgegevens	Het advies van de Autoriteit Persoonsgegevens (AP) is om de sollicitatiegegevens uiterlijk 4 weken na het einde van de sollicitatieprocedure te verwijderen. Met toestemming is het mogelijk om gegevens langer te bewaren. Bijvoorbeeld omdat er mogelijk op een later tijdstip een passende functie vrijkomt. Een termijn van maximaal 1 jaar na beëindiging van de sollicitatieprocedure is hiervoor redelijk volgens de AP.
8. Administratieve verzuimgegevens/re-integratie dossier	Advies Autoriteit Persoonsgegevens	De AP stelt dat een bewaartermijn van twee jaar na het einde van het dienstverband/re-integratietraject hiervoor redelijk is. Maar wanneer er bijvoorbeeld sprake is van een arbeidsconflict, dan kan de werkgever deze gegevens langer bewaren.
9. Overige gegevens tot personen herleidbaar		Vernietigen 2 jaar na uitschrijven of beëindigen relatie.
10. Als er toestemming is om na uitschrijven gegevens te bewaren met specifiek doel		Bewaren toegestaan op basis van toestemming.
11. Niet tot persoon herleidbaar		Vrij te kiezen.

Bijlage 1. Plan van aanpak informatiebeveiliging en privacy

Actie	**Planning**	**Gereed**
De bestuurder weet in de basis waar informatiebeveiliging en privacybescherming over gaat.		x
De bestuurder onderschrijft het belang van Informatiebeveiliging en privacy beleid (IBP)		x
De bestuurder weet wat de AVG voor een bestuurder inhoudt.		X
Het IBP is: a. opgesteld; b. vastgesteld door de bestuurder; c. en gecommuniceerd met betrokkenen .	x	
De IBP-organisatie is ingericht waarbij verantwoordelijkheden en taken zijn belegd bij medewerkers.	x	
Privacyreglement is vastgesteld		X
Basismaatregelen IBP en toegangsbeleid gegevens en applicaties zijn goedgekeurd en vastgelegd	x	
Functionaris voor de Gegevensbescherming is benoemd		x
Evalueren toepassing en werking IBP-beleid op basis van rapportages.	x	
De bestuurder weet wat de achtergrond van de te realiseren maatregelen zijn		x
Gegevens en processen zijn geclassificeerd	Continu proces	
De huidige situatie is in beeld gebracht. Er is een Risicoanalyse gedaan.	x	
Op basis van de risicoanalyse zijn de belangrijkste te nemen maatregelen bepaald en vastgesteld	x	
Er is een Procedure melden beveiligingsincidenten (datalekken) ● Opgesteld ● Goedgekeurd ● Gecommuniceerd		X

Er is een meldpunt datalekken en beveiligingsincidenten bekendgemaakt		X
Incidentenregistratie is ingeregeld		X
Rechten betrokkenen zijn vastgelegd en gecommuniceerd naar medewerkers, leerlingen en ouders		x
Er is een procesbeschrijving hoe betrokkenen hun rechten kunnen uitoefenen		x
Privacy statement is gemaakt, vastgesteld door de bestuurder en gecommuniceerd	Update	X
Er is een geheimhoudingsovereenkomst voor medewerkers niet in vaste dienst		X
Er is een wachtwoordbeleid		X
Er zijn afspraken gemaakt met leveranciers, die persoonsgegevens verwerken (beheer en toetsing contracten) Verwerkersovereenkomsten	Continu proces	X
De Privacy bijsluiter van de verwerkers-overeenkomsten zijn gepubliceerd (transparantie)		X
Toestemming ouders/leerlingen voor gebruik beeldmateriaal is geregeld		X
Procedure om toestemming in te trekken is vastgelegd en gecommuniceerd		X
Afspraken en procedures over privacy zijn geregeld en gecommuniceerd (informatieplicht, transparantie)		X
Zijn processen rondom Informatieplicht ingericht	X	
Er is een protocol sociale media of gedragsregels vastgesteld. (met extra aandacht voor leerlingen <16 jaar)		X
Er is een Gedragscode ict en internetgebruik / Acceptable use policy		X
Afspraken over passend onderwijs zijn gemaakt en bekend bij de betrokken medewerkers	X	
Afspraken jeugdhulpverlening zijn gemaakt en bekend bij de betrokken medewerkers	X	
Er zijn afspraken over de uitwisseling van leerlingdossiers en –gegevens met andere scholen	X	
Zijn de relevante medewerkers op de hoogte van de regels over het omgaan met leerlingdossiers	X	
Afspraken leerplicht en verzuim zijn gemaakt en bekend bij de betrokken medewerkers		X
Is er een Autorisatiematrix	Behoeft Actualisatie	X
De autorisaties en rollen van medewerkers zijn vastgesteld (bijv. m.b.v. een autorisatiematrix)	Behoeft Actualisatie	X
De autorisaties en rollen van medewerkers zijn in de administratiesystemen ingevoerd en geregeld	X	
Er is een proces om autorisaties te controleren	X	
De toepassing en werking van het IBP-beleid wordt op basis van rapportages geëvalueerd.	X	
Er is een Functionaris voor Gegevensbescherming benoemd		X
Er is toezicht op naleving privacy wetgeving		X
Er wordt vooraf bij nieuwe ontwikkelingen/ technieken gekeken of een gegevensbeschermingseffectbeoordeling gedaan moet worden		X

Er is een standaard sjabloon gegevensbeschermingseffectbeoordeling aanwezig		X
Met Privacy by design, privacy by default wordt rekening gehouden		X
Alle registraties van persoonsgegevens zijn aantoonbaar (documentatieplicht, dataregister)	X	
Er is een overzicht van alle leveranciers/externen, die persoonsgegevens in opdracht van de organisatie verwerken.	X	
Er is een overzicht van alle applicaties waarin persoonsgegevens verwerkt worden (intern)		
Afspraken rondom cameratoezicht zijn geregeld en gecommuniceerd	X	
Er zijn maatregelen genomen om DDoS-aanvallen te beperken en/of voorkomen	X	
Er is een Cleardesk policy		X
Er wordt aandacht geschonken aan ict-bekwaamheid leraar	X	
Leerlingen zijn geïnformeerd over IBP op school	X	
Er wordt aandacht geschonken aan mediawijsheid en digitale geletterdheid van leerlingen		X
Sociale-mediareglement is bekend gemaakt aan alle betrokkenen		X
Gedragscode is bekend gemaakt aan alle betrokkenen		X
Ouders worden actief benaderd en geïnformeerd over IBP op school en gewezen op hun rechten		X
De (G)MR is (wordt regelmatig) geïnformeerd over IBP.		X
Security awareness training is gegeven aan alle medewerkers	X	

Bijlage 2. BIV-classificatie

De kwaliteitsaspecten die worden toegepast op informatiebeveiliging zijn Beschikbaarheid, Integriteit, en Vertrouwelijkheid. Deze termen worden hier inclusief de deelaspecten beschreven. Alle aspecten kunnen worden geclassificeerd in laag, midden en hoog.

Beschikbaarheid:

de mate waarin beheersmaatregelen de beschikbaarheid en ongestoorde voortgang van de ict-dienstverlening waarborgen.

Deelaspecten hiervan zijn:

- Continuïteit: de mate waarin de beschikbaarheid van de ict-dienstverlening gewaarborgd is;
- Portabiliteit: de mate waarin de overdraagbaarheid van het informatiesysteem naar andere gelijksoortige technische infrastructuren gewaarborgd is;
- Herstelbaarheid: de mate waarin de informatievoorziening tijdig en volledig hersteld kan worden.

Niveau 1: **Laag** Beschikbaarheid is onbelangrijk.	**Niveau 2:** **Midden** Beschikbaarheid is belangrijk	**Niveau 3:** **Hoog** Beschikbaarheid is noodzakelijk
Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende meerdere dagen brengt geen merkbare (meetbare) schade toe aan de belangen van de instelling, haar medewerkers of haar leerlingen.	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende een dag brengt merkbare schade toe aan de belangen van de instelling, haar medewerkers of haar leerlingen.	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende een werkdag brengt merkbare schade toe aan de belangen van de instelling, haar medewerkers of haar leerlingen.

Integriteit:

De mate waarin de beheersmaatregelen (organisatie, processen en technologie) de juistheid, volledigheid en tijdigheid van de IT-dienstverlening waarborgen.

Deelaspecten hiervan zijn:

- Juistheid: de mate waarin overeenstemming van de presentatie van gegevens/informatie in IT-systemen ten opzichte van de werkelijkheid is gewaarborgd;
- Volledigheid: de mate van zekerheid dat de volledigheid van gegevens/informatie in het object gewaarborgd is;
- Waarborging: de mate waarin de correcte werking van de IT-processen is gewaarborgd.

Niveau 1: **Laag** Integriteit is onbelangrijk.	**Niveau 2:** **Midden** Integriteit is beschermd.	**Niveau 3:** **Hoog** Integriteit is noodzakelijk.
Blijvende juistheid van informatie (vanaf de bron tot het laatste gebruik) is gewenst, maar hoeft niet gegarandeerd te zijn. Indien informatie niet correct is, leidt dit tot beperkte schade.	Blijvende juistheid van informatie moet gewaarborgd zijn. Sommige toleranties zijn toelaatbaar. Juistheid van informatie is belangrijk, maar niet kritisch. Het is niet noodzakelijk dat correctheid onbetwistbaar aangetoond kan worden. Indien informatie niet correct is kan de organisatie substantiële schade lijden.	Informatie moet gegarandeerd correct zijn. Informatie waarbij het noodzakelijk is dat de correctheid niet betwist kan worden, zoals de uitslagen van toetsen, examens, onomkeerbare financiële transacties. Indien informatie niet correct is, kan de organisatie ernstige schade lijden.

Vertrouwelijkheid:

De mate waarin uitsluitend geautoriseerde personen, programmatuur of apparatuur gebruik kunnen maken van de gegevens of programmatuur, al dan niet gereguleerd door (geautomatiseerde) procedures en/of technische maatregelen.

Deelaspecten hiervan zijn:

- Autorisatie: de mate waarin de adequate inrichting van bevoegdheden gewaarborgd is;
- Authenticiteit: de mate waarin de adequate verificatie van geïdentificeerde personen of apparatuur gewaarborgd is;
- Identificatie: de mate waarin de mechanismen ter herkenning van personen of apparatuur gewaarborgd zijn;
- Periodieke controle op de bestaande bevoegdheden. Het (geautomatiseerd) vaststellen of geïdentificeerde personen of apparatuur de gewenste handelingen mogen uitvoeren.

Niveau 1: **Laag** Informatie is voor intern gebruik	**Niveau 2:** **Midden** Informatie is vertrouwelijk.	**Niveau 3:** **Hoog** Informatie is geheim.
Openbaar worden van gegevens leidt tot weinig of geen schade voor een instelling of betrokkene.	De organisatie, instelling of betrokkene kan substantiële schade lijden indien informatie toegankelijk is voor ongeautoriseerde personen. Informatie mag alleen toegankelijk zijn voor personen die hier vanuit hun functie toegang toe moeten hebben (need-to-know basis). Hieronder vallen onder andere persoonsgegevens.	De organisatie, instelling of betrokkene kan ernstige schade lijden indien informatie toegankelijk is voor ongeautoriseerde personen. Informatie mag uitsluitend toegankelijk zijn voor een zeer geselecteerde groep personen. Hieronder vallen onder andere bijzondere persoonsgegevens.