Informatiebeveiligings- en privacy beleid

Samenwerkingsverband PO Zaanstreek

Status	Datum	auteur
Vastgesteld door BO	29-5-2018	Bernard Homans

1 Inleiding

Informatie en ict zijn noodzakelijk in de ondersteuning van beide bedrijven. Omdat we met persoonsgegevens (van onszelf, van leerlingen en van derden) werken, is privacywetgeving daarop van toepassing.

De informatie en systemen van het samenwerkingsverband wordt blootgesteld aan een groot aantal bedreigingen, al dan niet opzettelijk van aard. Alle informatie die we bewaren en verwerken kan worden bedreigd door een aanval, een vergissing, de natuur (bijv. overstroming of brand), et cetera. Het niet beschikbaar zijn van beveiling van persoonsgegevens, incorrecte administraties en het uitlekken van gegevens kan leiden tot inbreuk in de privacy en schade berokkenen aan leerlingen en aan de doelmatigheid van ons werk.

Deze bedreigingen maken het noodzakelijk om gerichte maatregelen te treffen om de risico's die gepaard gaan met deze bedreigingen tot een aanvaardbaar niveau te reduceren. Om dit structureel op te pakken is het noodzakelijk dat we duidelijk maken waar het om gaat, een doel stellen en de manier waarop we dit doel willen bereiken.

1.1 Informatiebeveiliging en privacy

Informatiebeveiliging is een proces voor het beschermen van het samenwerkingsverband tegen risico's en bedreigingen met betrekking tot informatie en ict. Het richt zicht op drie aspecten:

- Beschikbaarheid; informatie en aanverwante bedrijfsmiddelen zijn alleen toegankelijk wanneer nodig;
- Integriteit; informatie en verwerkingsmethoden bevatten zo min mogelijk fouten;
- Vertrouwelijkheid; informatie is alleen toegankelijk voor diegenen die daartoe bevoegd zijn.

Privacy gaat om de bescherming van persoonsgegevens conform de huidige wet- en regelgeving. Door het goed toepassen van informatiebeveiliging kan aan deze wetgeving worden voldaan. Vooral het aspect vertrouwelijkheid is hiervoor van belang. Informatiebeveiliging is daarom integraal onderdeel van privacy.

Om privacy goed te regelen is informatiebeveiliging nodig. Daarom zien we het als één onderwerp: informatiebeveiliging en privacy (IBP).

2 Doel en reikwijdte

Dit beleid heeft als doelen:

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

Dit beleid is een leidraad voor iedereen die betrokken is bij IBP bij het samenwerkingsverband. Het is van toepassing op medewerkers die structureel werkzaamheden voor het samenwerkingsverband verrichten, tijdelijk personeel en andere personen die een rol spelen in het samenwerkingsverband. Het is van toepassing op de hele organisatie van het samenwerkingsverband, waaronder de fysieke locaties, systemen op deze locaties en gegevensverzamelingen die gebruikt worden.

Het heeft raakvlak met andere beleidsgebieden, te weten:

- Algemeen veiligheids- en beveiligingsbeleid zoals fysieke toegang en –beveiliging en ongevallen;
- IT-beleid; met als aandachtsgebieden de aanschaf en het beheer van ict;
- Personeels- en organisatiebeleid; met als aandachtsgebieden in- en uitstroom van medewerkers, functiescheiding en vertrouwensfuncties;

Dit informatiebeveiligings- en privacybeleid maakt duidelijk waar de verantwoordelijkheden rondom informatiebeveiliging en privacy zijn belegd.

3 Uitgangspunten

De belangrijkste beleidsuitgangspunten voor het samenwerkingsverband zijn:

- Informatiebeveiliging en het privacy dient te voldoen aan alle relevante wet- en regelgeving
- Veilig en betrouwbaar omgaan met informatie is de verantwoordelijkheid van iedereen
- Er wordt van alle medewerkers, ZZP'ers, bezoekers en externe relaties verwacht dat zij zich 'fatsoenlijk' gedragen en met een eigen verantwoordelijkheid
- het samenwerkingsverband is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt gebruikt
- het samenwerkingsverband maakt met alle partijen waarmee persoonsgegevens worden uitgewisseld concrete afspraken over informatiebeveiliging en privacy
- IBP is een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is

3.1 Privacy

Het samenwerkingsverband hanteert de vijf vuistregels voor privacy:

1. **Doelbepaling en doelbinding**: persoonsgegevens worden alleen gebruikt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. 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.
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 of wettelijk is geregeld.
4. **Transparantie**: het samenwerkingsverband leggen aan klanten en medewerkers op transparante wijze verantwoording af over het gebruik van hun persoonsgegevens, alsmede over het gevoerde IBP-beleid. Deze informatievoorziening vindt ongevraagd plaats. Daarnaast hebben deze betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming van hun Persoonsgegevens. Daarnaast 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.

Persoonsgegevens moeten adequaat worden beveiligd volgens algemeen en breed geaccepteerde beveiligingsnormen.

Bij alle registraties op basis van toestemming, zal het samenwerkingsverband aan de Betrokkene een eenduidige zogenaamde Opt-out procedure worden aangeboden.

4 Wet- en regelgeving

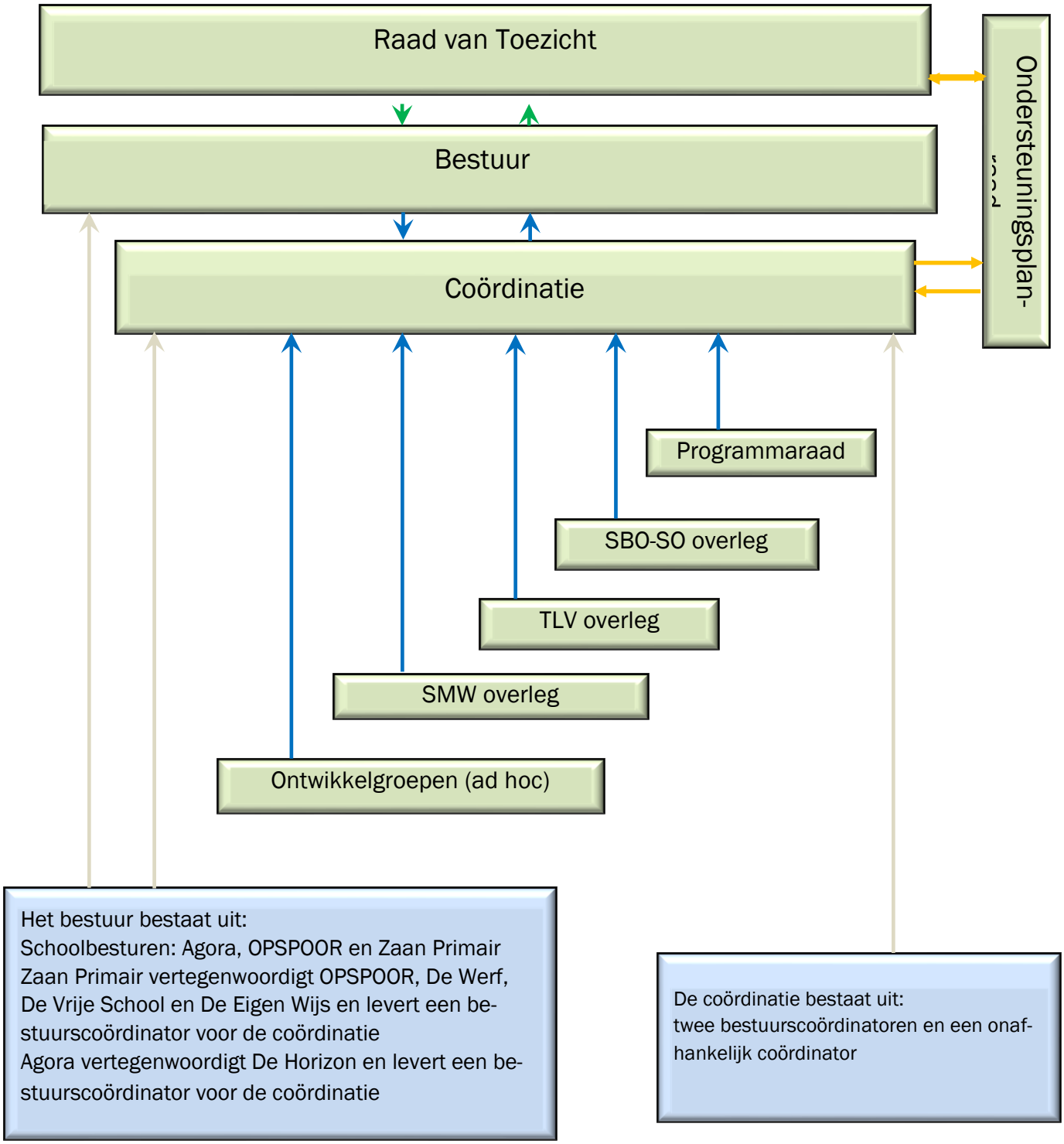
Het samenwerkingsverband voldoet aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder:

- Wet bescherming persoonsgegevens

- Algemene Verordening Gegevensbescherming (AVG)
- Specifieke wet- en regelgeving

5 Organisatie

Zo ziet onze organisatie er uit:



Dit hoofdstuk beschrijft hoe IBP in het samenwerkingsverband 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 Richtinggevend

Eindverantwoordelijke
Het bestuur van samenwerkingsverband is eindverantwoordelijk voor het IBP en stelt het beleid en de maatregelen vast op het gebied van informatiebeveiliging en privacy. De toepassing en werking van het IBP-beleid wordt op basis van regelmatige rapportages door hen geëvalueerd. De coördinatie is verantwoordelijk voor IBP.

5.2 Sturend

Management IBP
Het management IBP is coördinatietaak op sturend niveau. Deze geeft terugkoppeling en advies aan de eindverantwoordelijke en stuurt de mensen aan op de uitvoerende laag. De taak houdt in:

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

Functionaris voor Gegevensbescherming
De functionaris voor gegevensbescherming (FG) houdt binnen het samenwerkingsverband toezicht op de toepassing en naleving van de privacy-wetgeving. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie. De FG zorgt voor het afhandelen van vertrouwelijke informatiebeveiligingsincidenten. FG heeft regelmatig overleg met manager IBP. De FG is meestal ook contactpersoon en voor klachten en vragen van betrokkenen met een vertrouwelijk karakter.
De rol van FG kan bij een jurist of vertrouwenspersoon van de instelling worden belegd. <het kan ook een privacy officer zijn, deze heeft geen wettelijke taken en bevoegdheden die een onafhankelijke positie garanderen>.

Domeinverantwoordelijkheid/proceseigenaar
Binnen ons samenwerkingsverband niet zinvol verschillende domeinen/processen aan te wijzen met elk een eigen verantwoordelijke. De coördinatie bepaalt op welke wijze IBP wordt vormgegeven in richtlijnen, procedures en instructies binnen alle werkzaamheden.

5.3 Uitvoerend

Security Officer
De Security Officer vormt een technisch aanspreekpunt voor incidenten en informatiebeveiliging.

Functioneel beheer door de Coördinatie
Op basis van de domeinverantwoordelijke/proceseigenaar heeft de functioneel beheerder een ingevuld werkpakket, bestaande uit richtlijnen, procedures en instructies. Op basis hiervan voert hij zijn of haar taken uit.

Medewerker
Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in het personeelshandboek en de handleiding aanvaardbaar gebruik van bedrijfsmiddelen. Daarnaast worden medewerkers in hun dagelijkse werkzaamheden, waar nodig, ondersteund met checklists en formulieren.

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

Coördinatie
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 beveiligingsbeleid;
- 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 manager IBP.

6 Controle en rapportage

Dit informatiebeveiligings- en privacybeleid wordt minimaal elke twee jaar getoetst en bijgesteld door het bestuur. 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 het samenwerkingsverband een jaarlijkse planning en control cyclus voor informatiebeveiliging en privacy. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het informatiebeveiligings- en privacybeleid wordt getoetst.

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 het samenwerkingsverband 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, deelnemers en gasten. Verhoging van het beveiligingsbewustzijn is een verantwoordelijkheid van de manager IBP / informatie manager/ Security Officer met de directies als eindverantwoordelijken.

6.2 Classificatie en risicoanalyse

Bij het samenwerkingsverband 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 voor de informatievoorziening.

6.3 Incidenten en datalekken

Alle incidenten kunnen worden gemeld bij de coördinatie. De afhandeling van deze incidenten volgt een gestructureerd proces, die ook voorziet in de juiste stappen rondom de meldplicht datalekken.

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 het samenwerkingsverband wordt actief aandacht besteed aan IBP bij de aanstelling, tijdens functioneringsgesprekken, met een instelling brede gedragscode, met periodieke bewustwordingscampagnes, et cetera.
Voor de bevordering van de naleving van de Wet bescherming persoonsgegevens vervult de Functionaris Gegevensbescherming (FG) een belangrijke rol. De FG wordt aangesteld door het bestuur van het samenwerkingsverband, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FG werkt via een door de directies vast te stellen reglement.
Mocht de naleving ernstig tekort schieten, dan kan het samenwerkingsverband de betrokken verantwoordelijke medewerkers een sanctie op leggen, binnen de kaders van overeenkomst die ten grondslag ligt aan het werkberband en de wettelijke mogelijkheden.
Bij het samenwerkingsverband is het melden van beveiligingsincidenten en datalekken vastgelegd in een protocol.

Bijlage 1: Tabel IBP rollen en taken

Niveau	Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen
Richtinggevend (strategisch)	Bestuur	• Eindverantwoordelijk • IBP-vastlegging • 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
Sturend (tactisch)	Management IBP / Coördinatie	• IBP-beleidsvorming, • Inhoudelijk verantwoordelijk voor IBP • IBP-planning en controle • Adviseert 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 klanten, ZZP'ers • Security awareness activiteiten • Sociale media reglement • Gedragscode ICT en internetgebruik • Gedragscode medewerkers en leerlingen
	Functionaris voor Gegevensbescherming / Privacy officer	• 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
	coördinatie	• **Classificatie / risicoanalyse** • Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door het bestuur • *Samen met functioneel beheer en ICT beheer* er op toezien dat 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.	• Inventariseren waar persoonsgegevens van de klanten terechtkomen (leveranciers lijst) • Classificatie- en risicoanalyse documenten. Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder: • Toegangsmatrix diverse informatiesystemen en netwerk

Niveau	Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen Vanuit de Wiki
Uitvoerend (operationeel)	coördinatie	• Incidentafhandeling (registreren en evalueren). • Technisch aanspreekpunt voor IBP-incidenten.	
	Functioneel beheerder	• Uitvoeren taken conform gegeven richtlijnen en procedures.	Communiceren, informeren en toezien op naleving van o.a.:
	Medewerker	• Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden.	• IBP in het algemeen • Regels passend onderwijs • Hoe omgaan met leerling dossiers • Wie mogen wat zien • Gedragscode • Omgaan met sociale media • Mediawijs maken
	Dagelijkse leiding / leidinggevende / directie	• 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 bestuur.	