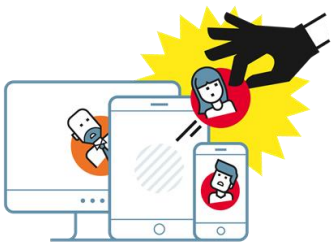
Informatiebeveiligings- en Privacybeleid 2.0

ROC van Amsterdam
ROC van Flevoland
Voortgezet Onderwijs van Amsterdam

Uitgave	: ROC van Amsterdam – ROC van Flevoland
Auteur	: M. Hoekstra en C. Klerkx
Kenmerk	: Informatiebeveiligings- en Privacybeleid 2.0
Vastgesteld door de Colleges van Bestuur op	: 22-05-2018
Beschikbaar voor OR ROCvA op	: 27-06-2018 ingestemd
Beschikbaar voor CSR ROCvA - ROCvF op	: 12-09-2018 ingestemd
Beschikbaar voor GMR VOvA op	: 04-10-2018 ingestemd



Voor:	RvB	Datum:	22-5-2018
Manager:	Rene van den Berg Rinza Kleter	Versie:	2.0
Status en vast-stelling	versie: 2.0 Instemming directeuren ICT en Bestuurs-dienst, centrale directie VOvA Vastgesteld door de RvB Ter instemming naar Platform OR, GMR VOvA en CSR ROCvA - ROCvF	Auteur(s)	C. Klerkx M. Hoekstra

Bij het opstellen van dit document is het voorbeelddocument IBPDOC18 gebruikt van

saMBO-ICT Kennisnet
TASKFORCE MBO INFORMATIEBEVEILIGING

1 Inhoudsopgave

2 Inleiding

2.1 Informatiebeveiliging beleid

In het onderwijsveld is sprake van toenemende afhankelijkheid van informatie en computersystemen, waardoor nieuwe kwetsbaarheden en risico's kunnen optreden. Het is daarom van belang hiertegen adequate maatregelen te nemen. Immers, onvoldoende informatiebeveiliging kan leiden tot onacceptabele risico's bij de uitvoering van onderwijs en bij de bedrijfsvoering van de organisatie. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades en imagoverlies.

Informatiebeveiliging is een beleidsverantwoordelijkheid van het bestuur van ROC van Amsterdam, ROC van Flevoland en Stichting Voortgezet Onderwijs van Amsterdam (ROCvA - ROCvF - VOvA). Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket aan maatregelen om de kwaliteitsaspecten beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening te garanderen.

2.2 Privacybeleid

Binnen de organisatie worden in toenemende mate persoonsgegevens van leerlingen, studenten en medewerkers verwerkt. Bovendien wordt meer en meer samenwerking gezocht met externe partijen waarbij informatie wordt gedeeld, denk bijvoorbeeld aan aanbieders van digitale lesmethoden. Misbruik van informatie kan veel schade teweegbrengen aan mensen en organisaties. De privacy van mensen komt in het geding.

2.3 Vervlechting informatiebeveiliging en privacy (IBP)

Informatiebeveiliging en privacy hebben een grote overlap. De kwaliteit van de verwerking en de beveiliging van persoonsgegevens dient te worden geoptimaliseerd waarbij een goede balans moet worden gevonden tussen privacy, functionaliteit en veiligheid. De organisatie heeft daarom gekozen voor een nieuwe versie beleidsplan waar in beide onderdelen zijn vervlochten met elkaar. De beleidsuitgangspunten die eerder zijn geformuleerd in het Informatiebeveiligingsbeleidsplan (vastgesteld door RvB d.d. 06-10-2014) zijn overgenomen en aangevuld in dit voorliggende beleidsplan waarin naast informatiebeveiliging ook privacy een plaats krijgt. Het beleidsplan is nu ook van toepassing op het VOvA. Bij het vormgeven van het beleid wordt gebruik gemaakt van het mbo-framework, standaarden en modellen. De naam van het beleidsplan is aangepast in "Informatiebeveiligings- en Privacybeleid 2.0",
Het Informatiebeveiligings- en Privacybeleid (IBP-beleid) heeft betrekking op alle medewerkers, studenten, leerlingen en gasten alsmede op alle organisatieonderdelen. Tevens vallen onder het IBP-beleid alle devices van de organisatie maar ook Bring Your Own-devices (BYOD) van waaraf geautoriseerde toegang tot het organisatienetwerk verkregen kan worden.

De organisatie heeft de ambitie om met het onderhavige beleidsdocument informatiebeveiliging en privacy structureel naar een hoger niveau te brengen en daar te houden door de doelstellingen en uitgangspunten helder te beschrijven en door aan te geven op welke wijze invulling wordt gegeven aan de realisatie van het beleid. Het beleid zal opgenomen worden in een PDCA-cyclus waarbij periodieke evaluatie en, zo nodig, bijstelling plaatsvinden. Zoals eerder vermeld vervangt dit IBP-beleidsplan het informatiebeveiligingsbeleidsplan zoals dat is vastgesteld d.d. 06-10-2014 door de Raad van Bestuur.

2.4 Doelstellingen IBP-beleid

De organisatie wil een superschool zijn waarbij de kernwaarden ambitieus, prettig, betrouwbaar en aandacht samen met vakkundigheid en daadkracht leidend zijn. Met inachtneming hiervan heeft het IBP-beleid bij de organisatie als doel het beschermen van de organisatie, onze medewerkers, onze leerlingen en onze studenten tegen onjuiste verwerking van informatie en gegevens door:

- ervoor te zorgen dat de voortgang van het onderwijs en de bedrijfsvoering niet in gevaar komt, en
- schade en gevolgen te minimaliseren door het voorkomen van beveiligings- en privacy-incidenten.

Het beleid biedt een kader om (toekomstige) maatregelen in de informatiebeveiliging en privacy te toetsen en om de taken, bevoegdheden en verantwoordelijkheden in de organisatie te beleggen. Doordat het IBP-beleid in alle processen van de organisatie een plaats krijgt, draagt dit beleid bij aan het bieden van een kwalitatief hoogwaardige onderwijsomgeving. Deze omgeving behoort veilig te zijn en te voldoen aan relevante wet- en regelgeving (zie Bijlage 2). De organisatie beschermt de persoonsgegevens die aan haar worden verstrekt en verwerkt deze zorgvuldig.

2.5 Uitgangspunten IBP-beleid

De uitgangspunten bij het IBP-beleid van de organisatie zijn:

- De organisatie is open en toegankelijk. Dit open en toegankelijk karakter heeft betrekking op gasten en op studenten, leerlingen en medewerkers. Van medewerkers, leerlingen en studenten wordt verwacht dat zij zich qua techniek en ook qua houding 'fatsoenlijk' gedragen (eigen verantwoordelijkheid). Niet acceptabel is dat, door al dan niet opzettelijk gedrag, onveilige situaties ontstaan die leiden tot schade en / of imagoverlies. Het is om deze reden dat gedragscodes zijn geformuleerd en geïmplementeerd.
- Het IBP-beleid moet voldoen aan de relevante wet- en regelgeving, in het bijzonder aan de Algemene Verordening Gegevensbescherming (AVG) die vanaf 25 mei 2018 van toepassing is en de huidige Wet Bescherming Persoonsgegevens (Wbp) vervangt.
- Hierbij dient een goede balans te worden aangebracht tussen het belang van de organisatie om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot zijn / haar persoonsgegevens.

2.6 Aanvullende uitgangspunten

- Informatiebeveiliging en privacy is een lijnverantwoordelijkheid
- Veilig en betrouwbaar omgaan met informatie in het dagelijkse werk is ieders professionele verantwoordelijkheid. Van iedereen wordt verwacht dat zij actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie. In de aanstellingsbrief, tijdens functioneringsgesprekken, met een organisatie-brede gedragscode, met periodieke bewustwordingscampagnes en dergelijke wordt hier aandacht voor gevraagd. Het opleggen van sancties na ernstige overtredingen maakt het geheel geloofwaardig.
- Informatiebeveiliging en privacy zijn continuprocessen. Regelmatige herijking van beleid en audits vinden plaats. Technologische en organisatorische ontwikkelingen binnen en buiten de instelling maken het noodzakelijk om periodiek te bezien of men nog wel op de juiste wijze bezig is de beveiliging te waarborgen. De audits maken het mogelijk het beleid en de genomen maatregelen te controleren.
- De organisatie is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd.
- Bij projecten, zoals infrastructurele wijzigingen of de aanschaf van nieuwe systemen, wordt vanaf de start rekening gehouden met informatiebeveiliging en privacy. Het is onderdeel van het ontwerpproces bij elk project.

2.7 Privacy principes

Bij bovenstaande beleidsuitgangspunten worden de volgende privacy principes in acht genomen:

- De verwerking van persoonsgegevens is gebaseerd op een van de wettelijke grondslagen zoals genoemd de Algemene Verordening Gegevensbescherming .
- Persoonsgegevens worden alleen verwerkt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking geformuleerd.
- Bij een verwerking van persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt tot de persoonsgegevens die noodzakelijk zijn voor het specifieke doeleinde. De gegevens dienen met het oog op dat doel toereikend, ter zake dienend en niet bovenmatig te zijn. Met andere woorden: niet meer gegevens worden verwerkt dan noodzakelijk (dataminimalisatie) is.
- Verwerking van persoonsgegevens gebeurt op de minst ingrijpende wijze en dient in redelijke verhouding te staan tot het beoogde doeleinde.
- Maatregelen worden getroffen om zoveel mogelijk te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn.

- Persoonsgegevens worden adequaat beveiligd volgens de geldende beveiligingsnormen.
- Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.
- Persoonsgegevens worden niet langer verwerkt dan noodzakelijk is voor de doeleinden van de Verwerking, hierbij worden de van toepassing zijnde bewaar- en vernietigtermijnen in acht genomen.
- Iedere betrokkene heeft het recht op inzage, verbetering, aanvulling, verwijdering en overdraagbaarheid van zijn persoonsgegevens alsmede het recht om bezwaar te maken tegen de verwerking.
- Studenten en leerlingen onder 16 jaar worden door de ouders / verzorgers vertegenwoordigd in het kader van privacy.
- Op transparante wijze wordt verantwoording afgelegd aan betrokkenen over welke gegevens worden verwerkt en waarom deze verwerking plaatsvindt. Hiertoe worden dataregisters bijgehouden waarin ook wordt aangegeven met welke instellingen gegevens worden uitgewisseld, welke gegevens dat zijn en met welk doel dit gebeurt. Betrokkenen worden geïnformeerd over de dataregisters die op de website van de organisatie worden gepubliceerd.
- Een Functionaris voor gegevensbescherming (FG) is aangesteld om regelmatige observatie en toetsing uit te voeren.

3 Realisatie IBP-beleid

Om de doelstellingen van dit beleid te realiseren en de hiervoor beschreven principes na te leven moeten rollen bij medewerkers worden belegd, overlegstructuren worden bepaald, maatregelen worden getroffen en middelen beschikbaar gesteld.

3.1 Functionele inpassing IBP

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

3.1.1 Raad van Bestuur

De Raad van Bestuur (RvB) is eindverantwoordelijk voor de informatiebeveiliging en privacy binnen de organisatie en stelt het beleid en de basismaatregelen op het gebied van informatiebeveiliging en privacy vast. De inhoudelijke verantwoordelijkheid voor informatiebeveiliging en privacy is gemandateerd aan de IBP-manager. Deze heeft de opdracht om voor de informatiebeveiliging en privacy voor de gehele instelling zorg te dragen.

3.1.2 Portefeuillehouder informatiebeveiliging

Het RvB-lid dat informatiebeveiliging en privacy in de portefeuille heeft is eindverantwoordelijk voor informatiebeveiliging en privacy binnen de organisatie.

3.1.3 IBP-manager

De IBP-manager is een rol op strategisch en tactisch niveau. Hij adviseert samen met de Directeur ICT en Directeur Bestuursdienst aan de RvB. De IBP-manager bewaakt de uniformiteit binnen de instelling en formuleert het IBP-beleid.

3.1.4 Functioneel beheerder

De rol van functioneel beheerder van de centraal beheerde onderwijs- of bedrijfsapplicaties is belegd op centraal stafniveau. De functioneel beheerder vervult een rol bij de vertaling van de strategie naar tactische (en operationele) plannen. Dit gebeurt samen met de IBP-manager en met de eigenaren van de technische platforms.

3.1.5 Proceseigenaar

Een proceseigenaar is iemand die verantwoordelijk is voor een van de primaire of ondersteunende processen zoals inkoop, HRM en onderwijs.

3.1.6 Systeemeigenaar

De systeemeigenaar is ervoor verantwoordelijk dat de applicatie een goede ondersteuning biedt aan het proces waarvoor deze verantwoordelijk is. Dit betekent dat de systeemeigenaar zorgt dat zowel nu als in de toekomst de applicatie blijft beantwoorden aan de eisen en wensen van de gebruikers en aan wet- en regelgeving. Uiteraard moet de applicatie voldoen aan het IBP-beleid.

3.1.7 Security specialist

De security specialist adviseert over specifieke informatiebeveiligingsmaatregelen in projecten en bewaakt de consistentie van de maatregelen. Deze rol is belegd binnen Dienst ICT.

3.1.8 Leidinggevende

Naleving van het IBP-beleid is onderdeel van de integrale bedrijfsvoering. Iedere leidinggevende heeft de taak om:

- ervoor te zorgen dat zijn medewerkers op de hoogte zijn van het IBP-beleid;
- toe te zien op de naleving van het IBP-beleid door zijn medewerkers;
- periodiek het onderwerp informatiebeveiliging en privacy onder de aandacht te brengen in werkoverleggen;
- als aanspreekpunt beschikbaar te zijn voor alle personeel gerelateerde informatiebeveiliging en privacyzaken.

De leidinggevende kan hierin ondersteund worden door de IBP-manager.

3.1.9 Functionaris Gegevensbescherming

De Functionaris voor gegevensbescherming (FG) houdt binnen de organisatie toezicht op de toepassing en naleving van de Algemene Verordening Gegevensbescherming. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie.

3.2 De overlegstructuren

Om de samenhang van informatiebeveiliging en privacy binnen de organisatie goed tot uitdrukking te laten komen en de initiatieven en activiteiten op dit gebied binnen de verschillende onderdelen op elkaar af te stemmen wordt bij de organisatie gestructureerd overleg gevoerd over dit onderwerp op verschillende niveaus.

Op strategisch niveau wordt richtinggevend gesproken over governance en compliance alsmede over doelen, scope en ambitie op het gebied van informatiebeveiliging en privacy. Dit gebeurt in de regiegroep Veiligheid.

Op tactisch niveau wordt de strategie vertaald naar plannen, te hanteren normen, evaluatiemethoden e.d.. Deze plannen en instrumenten zijn sturend voor de uitvoering.

Op operationeel niveau worden de zaken besproken die de dagelijkse bedrijfsvoering (uitvoering) aangaan. Deze overlegvorm is decentraal georganiseerd, indien nodig binnen elk organisatieonderdeel.

Voor alle drie de typen overleg geldt dat dit zoveel mogelijk ingepast moet worden in bestaande overlegvormen met hetzelfde karakter. Zo zal op strategisch niveau niet alleen over informatiebeveiliging en privacy gesproken worden maar ook over andere risico's waarmee de organisatie te maken kan krijgen, zoals bijvoorbeeld financieel, personeel en commercieel.

SCHEMATISCH WEERGEGEVEN:

	Richtinggevend	*Sturend*	*Uitvoerend*
Wat?	• Bepalen IBP-strategie • Organisatie t.b.v. IBP inrichten • IBP-planning en control vaststellen	Planning & Control IBP: • voorbereiden • normen en wijze van toetsen • evalueren beleid en maatregelen • begeleiding externe audits	• Implementeren IBP-maatregelen • registreren en evalueren incidenten • communicatie eindgebruikers
Wie?	• CvB, i.c. portefeuillehouder IB, o.b.v. advies manager IBP • Directeur Onderwijs • Directeur HRM • Directeur ICT • Directeur Bestuursdienst	• Proces eigenaren • Manager IBP • Functioneel beheerders • Functionaris voor de Gegevensbescherming	• Functioneel Beheerder • ICT
Overleg	• RvB stelt vast • Regiegroep veiligheid adviseert	• Tactisch IBP-overleg	• Operationeel IBP-overleg
Documenten	• IBP-beleidsplan • IBP-baseline (basis • maatregelen	• Risicoanalyses en audits • Jaarplan en verslag	• contracten (security paragraaf) • Incident registratie, incl. evaluatie

3.3 Maatregelen

Voor informatiebeveiliging en privacy wordt bij de organisatie dezelfde managementcyclus gevolgd die ook voor andere onderwerpen geldt: beleid, analyse, plan implementatie, uitvoering, controles en evaluatie. De maatregelen die getroffen moeten worden om het beleid vorm te geven worden in documenten en in concrete acties vertaald.

3.3.1 IBP-beleidsplan

Het informatiebeveiligings- en privacybeleid 2.0 ligt ten grondslag aan de aanpak van informatiebeveiliging en privacy binnen de organisatie. In het IBP-beleid worden de randvoorwaarden en uitgangspunten vastgelegd en de wijze waarop het beleid wordt vertaald in concrete maatregelen. Om ervoor te zorgen dat het beleid gedragen wordt binnen de organisatie en de organisatie daarnaar handelt, wordt het uitgedragen door (of namens) de RvB. Het IBP-beleid wordt opgesteld door de IBP-manager, afgestemd met OBV en MT-ICT, goedgekeurd door DvD ICT en DvD Bestuursdienst en vastgesteld door de RvB.

3.3.2 Normenkader MBO (basisniveau maatregelen)

Dit kader, dat ook wordt gehanteerd bij het vo / po, bevat de basismaatregelen die minimaal nodig zijn om organisatie-breed een minimaal niveau van informatiebeveiliging en privacy te kunnen waarborgen. Dit vloeit voort uit het beleid of uit besluiten die door het tactisch overleg genomen zijn. Deze basismaatregelen dienen dus overal binnen de organisatie ingevoerd te worden. De baseline wordt gemaakt door de IBP-manager en goedgekeurd door de RvB. Wanneer systemen na een risicoanalyse hogere beveiligingseisen nodig hebben, dan worden deze bovenop de minimale maatregelen genomen.

De basismaatregelen vloeien voort uit het Normenkader informatiebeveiliging MBO zoals dat door saMBO-ICT en Kennisnet is opgesteld en waar de organisatie invulling aan geeft (Bijlage 1). Het streven is ieder statement van de normenkaders in de organisatie naar een gewenst en mogelijk hoger volwassenheidsniveau te brengen. De organisatie heeft hiertoe een eigen IBP-monitor ingericht waar, per statement onderbouwd, inzichtelijk wordt gemaakt op welk volwassenheidsniveau de organisatie zich bevindt.

3.3.3 Jaarplan / verslag

Elk jaar levert de IBP-manager een jaarverslag en een jaarplan voor het volgende jaar. Het jaarplan is mede gebaseerd op de resultaten van periodieke controles / audits. In het jaarverslag wordt o.a. ingegaan op incidenten, resultaten van risicoanalyses (incl. genomen maatregelen) en andere initiatieven die het afgelopen jaar hebben plaatsgevonden. Dergelijke verslagen kunnen opgenomen worden in de bestuurlijke Planning & Control-cyclus.

3.3.4 Verwerkersovereenkomsten applicaties en educatieve software

Met alle leveranciers van onderwijs- en bedrijfsapplicaties en educatieve software worden verwerkersovereenkomsten afgesloten. De organisatie maakt gebruik van het privacy convenant Kennisnet. Dit privacy convenant zorgt dat het gebruik van digitale onderwijsmiddelen in lijn is met de AVG. Een model verwerkersovereenkomst is onderdeel van dit convenant.

3.3.5 Gedragscodes

Gedragscodes en richtlijnen worden opgesteld voor medewerkers, studenten, leerlingen en derden, al dan niet voor specifieke doelgroepen, op het gebied van informatiebeveiliging en privacy zoals:

- Gedragscode ICT;
- Wachtwoordbeleid;
- Toepassing van crypto grafische hulpmiddelen;
- Classificatierichtlijnen (Bijlage 4);
- Protocol ICT-medewerkers;
- Protocol social media;
- Privacyreglementen voor studenten, leerlingen en medewerkers.

Jaarlijks vindt een review plaats op deze gedragscodes en richtlijnen door de IBP-manager.

3.4 Inrichten meldpunt voor registratie en afhandeling incidenten

Het is van belang om te leren van incidenten. Incidentregistratie en periodieke rapportage over opgetreden incidenten horen thuis in een volwassen informatiebeveiligingsomgeving. Bij de organisatie is daarom een meldpunt ingericht, de ICT Servicedesk, en is op Portaal voor Talent aangegeven wanneer en hoe dat meldpunt is te benaderen. Voor het afhandelen van datalekken is een apart proces ingericht waarin de FG de afhandeling en waar nodig melding naar de Autoriteit Persoonsgegevens (AP) verzorgt.

3.5 Informatiebeveiliging en Privacy Team (IBP-team) aanwijzen

Een IBP-team is georganiseerd met als doel: organisatie-brede preventie en zorg voor informatiebeveiliging en privacy incidenten. Het team signaleert en registreert beveiligingsincidenten en datalekken en zorgt voor een juiste afhandeling volgens vastgesteld proces. Het IBP-team houdt zich ook bezig met beveiligingsincidenten buiten de organisatie als daar eigen medewerkers of deelnemers in enige rol bij betrokken zijn. Binnen het team zijn verschillende rollen belegd en het team kan per calamiteit van samenstelling wijzigen. Voor meer informatie over het IBP-team wordt verwezen naar bijlage 5.

3.6 Bewustwording en training

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 organisatie het bewustzijn voortdurend aangescherpt, zodat kennis van risico's wordt verhoogd en het (veilig en verantwoord) gedrag wordt aangemoedigd. Onderdeel van het beleid zijn de regelmatig terugkerende bewustwordingscampagnes voor medewerkers en onderwijsdeelnemers. Zulke campagnes kunnen aansluiten bij landelijke campagnes in het vo / po, het mbo en het hbo, zo mogelijk in afstemming met beveiligingscampagnes voor Arbo, milieu en fysiek. Verhoging van het beveiligingsbewustzijn is een verantwoordelijkheid van de IBP-manager; uiteindelijk is ook hiervoor de RvB eindverantwoordelijk.

3.7 Controle, naleving en sancties

Bij de organisatie initieert de IBP-manager in samenwerking met de interne auditor de controle op de uitvoering van het IBP-beleid en de jaarplannen. De IBP-monitor biedt handvatten voor deze interne controle.
De externe controle wordt in de toekomst uitgevoerd door onafhankelijke accountants. Dit is gekoppeld aan het jaarlijkse accountantsonderzoek en wordt zoveel mogelijk gecoördineerd met de normale Planning & Control cyclus. Steeds vaker is ook sprake van branche audits, zoals de MBO-audit (afgeleid van de HO-audit en bewerkt door Kennisnet en saMBO-ICT). De bevindingen van de interne en externe audits zijn input voor de nieuwe jaarplannen van de organisatie.

De naleving bestaat uit algemeen toezicht op de dagelijkse praktijk van het informatiebeveiliging en privacy proces. Van belang hierbij is dat lijnmanagers en proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Mocht de naleving ernstig tekort schieten dan kan de organisatie de betrokken verantwoordelijke medewerkers een sanctie op leggen, binnen de kaders van de Cao en de wettelijke mogelijkheden.
Ter bevordering van de naleving van de wetgeving vervult de FG een belangrijke rol. De FG heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FG werkt volgens een door de RvB vast te stellen reglement.

3.8 Middelen IBP-beleid

De financiering van informatiebeveiliging en privacy wordt bij de organisatie als volgt geregeld:

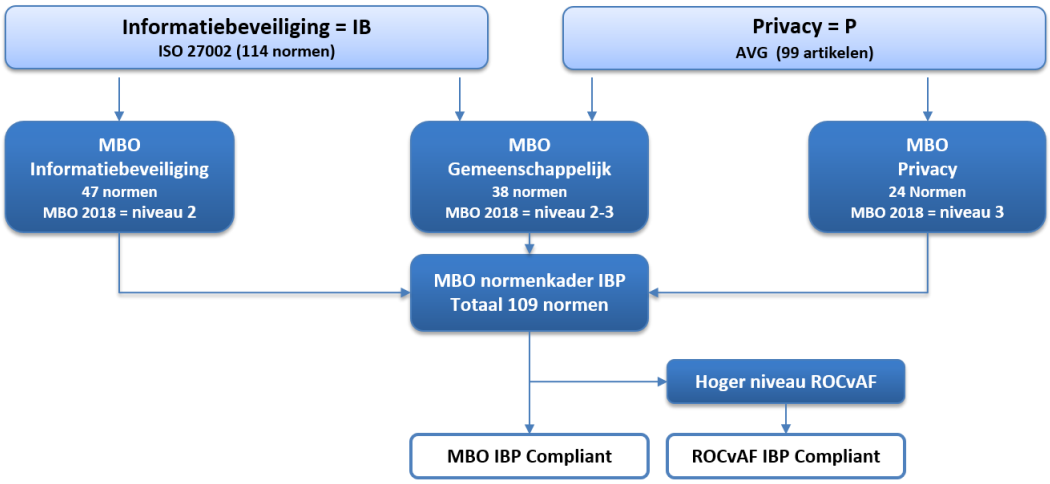
- Algemene zaken, zoals het opstellen van een IBP-plan voor de gehele instelling of een externe audit, worden uit het centrale ICT-budget betaald. De FG wordt uit het budget van de Bestuursdienst betaald.
- De beveiliging van informatiesystemen komen ten laste van het informatiesysteem zelf.
- Beveiligingskosten van werkplekken maken integraal onderdeel uit van de werkplekkosten. Hetzelfde geldt voor awareness en training: dit kunnen organisatie-brede bewustwordingscampagnes zijn (centraal gefinancierd) en lokale voorlichting en training voor specifieke toepassingen of doelgroepen (decentraal gefinancierd).

3.9 Bijlagen.

3.9.1 Bijlage 1: MBO Toetsingskader voor ROCvA -ROCvF -VOvA

Alle mbo's en steeds meer po / vo- scholen richten zich op genoemde ontwikkelingen vanuit een gezamenlijke aanpak rond informatiebeveiliging en privacy (IBP). Binnen de sector is vanuit SURF, saMBO-ICT en Kennisnet een toetsingskader geformuleerd om informatiebeveiliging en privacy te meten en te borgen binnen de onderwijsinstellingen.

Het IBP-toetsingskader bestaat uit 109 normen die voor het mbo zijn geformuleerd en ook toepasbaar zijn voor po / vo en die zijn gebaseerd op de ISO 27002 regels en op de wettelijke eisen. Per norm zijn vijf volwassenheidsniveaus gedefinieerd met de bijbehorende maatregelen. Vanuit de mbo-branche is gesteld dat het wenselijk is om ten aanzien van de informatiebeveiliging (IB) normen dusdanige maatregelen te treffen dat in ieder geval volwassenheidsniveau 2 wordt behaald. Ten aanzien van de privacy (P) normen wordt volwassenheidsniveau 3 minimaal als wenselijk gezien. Per norm kan de organisatie echter haar eigen koers varen en een hoger dan wel lager volwassenheidsniveau aanhouden / nastreven.



Het IBP vormt, samen met het hiervoor beschreven toetsingskader, het kader van waaruit wordt gewerkt. Een pragmatische aanpak wordt gehanteerd met de bewustwording (awareness) van medewerkers als rode draad. Het doel is de organisatieonderdelen IBP-compliant te maken en te behouden en de awareness te vergroten. Vooralsnog sluiten wij aan bij het wenselijk geachte niveau zoals de mbo-branche dat heeft geformuleerd en is het doel om ten aanzien van de IB-normen volwassenheidsniveau 2 te behalen en ten aanzien van de P-normen niveau 3 te bereiken.

3.9.2 Bijlage 2: Toelichting beschikbaarheid, integriteit, vertrouwelijkheid.

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.

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.

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.

3.9.3 Bijlage 3. Wet- en regelgeving

Bij de organisatie wordt op de volgende wijze omgegaan met relevante wet- en regelgeving.

3.9.3.1 De Wet Educatie Beroepsonderwijs

De organisatie heeft een kwaliteitszorgsysteem, waarin (onder meer) het zorgvuldig omgaan met gegevens in de studentenadministratie en met de studieresultaten is gewaarborgd.

3.9.3.2 Wet Bescherming Persoonsgegevens (Wbp)

De organisatie heeft de wettelijke vereisten (juistheid en nauwkeurigheid van gegevens en passende technische en organisatorische maatregelen tegen verlies en onrechtmatige verwerking) geïmplementeerd via het IBP- beleid. Met ingang van 25 mei 2018 wordt de Wbp vervangen door de reeds in werking getreden Algemene Verordening Gegevensbescherming (AVG).

3.9.3.3 Algemene Verordening Gegevensbescherming

De organisatie heeft de wettelijke vereisten (juistheid en nauwkeurigheid van gegevens en passende technische en organisatorische maatregelen tegen verlies en onrechtmatige verwerking) geïmplementeerd via het IBP-beleid. Met ingang van 25 mei 2018 vervangt de AVG de Wbp.

3.9.3.4 Archiefwet

De organisatie houdt zich aan de voorschriften uit de Archiefwet en het Archiefbesluit over de wijze waarop omgegaan moet worden met informatie vastgelegd in (gedigitaliseerde) documenten, informatiesystemen, websites e.d.. Dit is onderdeel van de jaarlijkse externe accountantsrapportages. Het basis selectiedocument voor de mbo-sector wordt gevolgd.

3.9.3.5 Auteurswet

De organisatie verspreidt geen originele werken zonder dat daarvoor toestemming is verkregen van de eigenaar van de auteursrechten. Dit impliceert ook dat de organisatie het gebruik van software zonder het bezitten van de juiste licenties tegengaat.

3.9.3.6 Specifiek po / vo

Specifiek voor het po / vo bestaat aanvullende relevante wet- en regelgeving in de wet Goed onderwijs en goed bestuur po / vo, Wet onderwijstoezicht en de Leerplichtwet.

3.9.3.7 Telecommunicatiewet

Zolang het netwerk van de organisatie niet openbaar is, is de Telecommunicatiewet niet van toepassing. Instellingen die wel (ten dele) een openbaar netwerk aanbieden moeten aan de Telecommunicatiewet voldoen. De maatregelen die de organisatie genomen heeft om aan de privacywetgeving te voldoen zijn tevens toereikend om de bescherming van de persoonlijke levenssfeer van gebruikers op onze openbare netwerken te waarborgen.

3.9.3.8 Wetboek van Strafrecht

In het Wetboek van Strafrecht is de laatste decennia een aantal specifieke bepalingen opgenomen over de strafrechtelijke probleemgebieden in relatie tot het computergebruik. De wet schrijft voor dat “enige beveiliging” vereist is alvorens sprake *kan zijn* van het eventueel strafrechtelijk vervolgen van delicten jegens de onderwijsinstelling en het eventueel vrijwaren van bestuurders van de instelling.
Naleving van dit informatiebeveiligings- en privacybeleid en implementatie van de basismaatregelen bij de organisatie moet leiden tot een niveau van beveiliging dat als voldoende mag worden gezien in het kader van het Wetboek van Strafrecht.

3.9.3.9 Overige regelgeving, richtlijnen en landelijke afspraken

Zoals eerder gesteld is het IBP-beleid bij de organisatie gebaseerd op het normenkader zoals dat voor de mbo-sector binnen het Framework is opgesteld. De organisatie houdt zich voorts aan (o.a.) de volgende regelgeving, richtlijnen en landelijke afspraken:

- DUO afspraken Bron e.d.;
- Aansluitvoorwaarden SURFnet;
- De vigerende Cao’s;
- Het Convenant Digitale Onderwijsmiddelen en Privacy.

3.9.4 Bijlage 4. Classificatie

Bij de organisatie zijn alle gegevens waarop dit informatiebeveiligingsbeleid van toepassing is, geclassificeerd. Het niveau van de beveiligingsmaatregelen is afhankelijk van de klasse.
De classificatie van informatie is afhankelijk van de gegevens in het informatiesysteem en wordt bepaald op basis van risicoanalyses.
Daarbij zijn de volgende kwaliteitsaspecten van informatievoorziening van belang:

a. **beschikbaarheid:** de mate waarin de beheersmaatregelen de beschikbaarheid en ongestoorde voortgang van de ICT-dienstverlening waarborgen.
b. **integriteit:** de mate waarin de beheersmaatregelen (organisatie, processen en technologie) de juistheid, volledigheid en tijdigheid van de IT-dienstverlening waarborgen.
c. **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.

A. Beschikbaarheid

Ten aanzien van de beschikbaarheidseisen is voor de volgende classificatie indeling gekozen:

Classificatie indeling	Classificatie gevolg
Beschikbaarheid **Laag**	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan **1 week** brengt geen merkbare (meetbare) schade toe aan de belangen van de instelling, haar medewerkers of haar studenten of klanten.
Beschikbaarheid **Midden**	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan **48 uur** brengt merkbare schade toe aan de belangen van de instelling, haar medewerkers of haar studenten of klanten.
Beschikbaarheid **Hoog**	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan **4 uur** brengt merkbare schade toe aan de belangen van de instelling, haar medewerkers of haar studenten of klanten.

B. Integriteit

Voor integriteit wordt de volgende classificatie indeling gehanteerd:

Classificatie indeling	Classificatie gevolg
Integriteit **Laag**	Het bedrijfsproces staat **enkele** integriteitsfouten toe.
Integriteit **Midden**	Het bedrijfsproces staat **zeer weinig** integriteitsfouten toe. Bescherming van integriteit is absoluut noodzakelijk.
Integriteit **Hoog**	Het bedrijfsproces staat **geen** integriteitsfouten toe.

C. **Vertrouwelijk**

Vertrouwelijkheid is als volgt geclassificeerd:

Classificatie indeling	Classificatie gevolg
Vertrouwelijkheid **Laag**	Informatie die toegankelijk mag of moet zijn voor **alle of grote groepen** medewerkers of studenten. Vertrouwelijkheid is gering.
Vertrouwelijkheid **Midden**	Informatie die alleen toegankelijk mag zijn voor een **beperkte groep** gebruikers. De informatie is vertrouwelijk.
Vertrouwelijkheid **Hoog**	Dit betreft zeer vertrouwelijke informatie, alleen bedoeld voor **specifiek benoemde personen**, waarbij onbedoeld bekend worden buiten deze groep grote schade kan toe brengen.

Welk beveiligingsniveau geschikt is voor een bepaald informatiesysteem hangt af van de classificatie van de informatie die het systeem verwerkt. De classificatie dient door de proceseigenaar te worden bepaald.

3.9.5 Bijlage 5: Het IBP-team

Het IBP-team van de organisatie heeft de volgende opdracht:

- Het signaleren en registreren van alle beveiligingsincidenten en datalekken, het coördineren van de bestrijding en het toezien op de oplossing van problemen die tot incidenten hebben geleid of door de incidenten zijn veroorzaakt (of het bieden van ondersteuning daarbij);
- Het geven van voorlichting en het doen van algemene aanbevelingen aan netwerkbeheerders, systeembeheerders, ontwikkelaars en eindgebruikers door het verspreiden van informatie;
- Het leveren van managementrapportages aan Directeur ICT en directeur Bestuursdienst over de beveiligingsincidenten en het doen van voorstellen tot betere preventie van incidenten.

Het IBP-team bij de organisatie levert de volgende diensten bij calamiteiten:

- Afhandelen van binnenkomende e-mails;
- Afhandelen van binnenkomende telefoongesprekken;
- Inrichten en operationeel houden van een meldpunt voor alle beveiligingsincidenten en het coördineren en bewaken van een adequate afhandeling daarvan;
- De bereikbaarheid van het IBP-team (tijden / middelen) wordt bekend gemaakt aan alle betrokkenen;
- Geven van voorlichting aan IT-gebruikers, -ontwikkelaars en -beheerders over preventie van incidenten en actuele bedreigingen;
- Adviseren over instelling brede beveiligingsaspecten;
- Periodiek opstellen van managementrapportages;
- Onderhouden van contacten met SURFcert.

Het IBP-team kent de rollen:

- Coördinator Frontoffice;
- Coördinator IAM;
- Coördinator Infrastructuur;
- Security specialist;
- Functioneel beheerder;
- Functionaris Gegevensbescherming;
- IBP-manager;
- MT lid.

Bij grote calamiteiten worden de Veiligheidscoördinator en Dienst PRC&M betrokken

Het IBP-team bij de organisatie behandelt meldingen vertrouwelijk en verstrekt alleen informatie over beveiliging en privacy incidenten als dat noodzakelijk en relevant is voor de oplossing van een incident.

De rol van IBP-teamcoördinator wordt belegd bij de IBP-manager.