Alfa-college

Informatiebeveiliging- en Privacybeleid 2020

Vastgesteld door CvB 15 juni 2020

Inhoudsopgave

Wijziging t.o.v. versie 1.0:
Op verzoek van de OR is onder reikwijdte (P5) de passage over medezeggenschap anders verwoord.

Verantwoording en richtlijnen

Inleiding

Door het toenemende belang van privacy is in de afgelopen jaren naast het informatiebeveiligingsbeleid ook privacy beleid ontstaan. Deze domeinen waren elk in een afzonderlijk beleidsstuk beschreven. Gezien de vervlechting van de beide domeinen, de overlap in de te nemen maatregelen en de wens om aan te sluiten bij de landelijke MBO standaard is er voor gekozen de beide domeinen in een informatiebeveiliging- en privacy beleid te vatten.

Aanleiding

Het onderwijs is in toenemende mate afhankelijk van informatie en ICT. De hoeveelheid informatie, waaronder persoonsgegevens, neemt toe door o.a. ontwikkelingen als gepersonaliseerd leren met ICT. Het is belangrijk om informatie goed te beschermen en veilig en verantwoord met persoonsgegevens om te gaan, met name ook van minderjarigen[1]. De afhankelijkheid van ICT en persoonsgegevens brengt nieuwe kwetsbaarheden en risico's met zich mee. Het goed regelen van informatiebeveiliging en privacy (afgekort tot IBP) in een IBP-beleid is noodzakelijk om de gevolgen van deze risico's tot een aanvaardbaar niveau te reduceren en de voortgang van het onderwijs en de bedrijfsvoering optimaal te kunnen waarborgen.

Leeswijzer

In dit hoofdstuk Verantwoording en richtlijnen zijn naast het hoe en waarom van dit beleid de beleidsuitspraken opgenomen. In het hoofdstuk Compliance zijn de relevante wet- en regelgeving en de wijze waarop we borgen dat we daar aan voldoen beschreven. In het hoofdstuk Governance is de IBP-organisatie met de relevante taken en verantwoordelijkheden beschreven.

Toelichting informatiebeveiliging

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

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

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

Toelichting privacy

Privacy gaat over persoonsgegevens. Persoonsgegevens moeten beschermd worden volgens de huidige wet- en regelgeving. Bescherming van de privacy regelt onder andere onder welke voorwaarden persoonsgegevens verwerkt mogen worden. Persoonsgegevens zijn hierbij alle

[1] Groene woorden worden in bijlage 3 (Verklarende woordenlijst) toegelicht

gegevens die een natuurlijke persoon direct of indirect kunnen identificeren. Onder verwerking wordt elke handeling met betrekking tot persoonsgegevens verstaan. De wet noemt als voorbeelden van verwerking:
Het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekking door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens[2].

Vervlechting informatiebeveiliging en privacy

Uit voorgaande blijkt dat informatiebeveiliging een belangrijke voorwaarde is voor privacy, terwijl omgekeerd de zorgvuldige omgang met persoonsgegevens noodzakelijk is voor informatiebeveiliging. Informatiebeveiliging en privacy staan naast elkaar en zijn van elkaar afhankelijk, en worden daarom samengevoegd tot één geheel: IBP. Dit beleid, verder te benoemen als IBP-beleid, vormt de basis om informatiebeveiliging en privacy binnen het Alfa-college te regelen en vormt de kapstok voor de onderliggende afspraken en procedures.

Doel

Informatiebeveiliging en privacy hebben de volgende doelen:
- Het waarborgen van de continuïteit van het onderwijs en de bedrijfsvoering.
- Het garanderen van de privacy van alle betrokkenen van wie het Alfa-college persoonsgegevens verwerkt, te weten: medewerkers, studenten, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties.
- Beveiligings- en privacy-incidenten voorkomen en de eventuele gevolgen hiervan beperken.
  Het informatiebeveiligings- en privacy beleid (IBP-beleid) is erop gericht om de kwaliteit van de verwerking van informatie en de beveiliging van persoonsgegevens te optimaliseren waarbij er een juiste balans moet zijn tussen privacy, functionaliteit en veiligheid. Het uitgangspunt is dat de persoonlijke levenssfeer van de betrokkene (o.a. medewerkers, studenten en hun ouders/verzorgers) wordt gerespecteerd en het Alfa-college voldoet aan relevante wet- en regelgeving.

Reikwijdte

- Het IBP-beleid binnen het Alfa-college geldt voor alle betrokkenen, te weten: medewerkers, studenten, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur / outsourcing).
- Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van het Alfa-college. Hieronder valt tevens de gecontroleerde informatie, die door de school zelf is gegenereerd en wordt beheerd. Onder dit beleid vallen ook alle devices waarmee geautoriseerde toegang tot het schoolnetwerk verkregen kan worden.
- Het IBP-beleid geldt voor de geheel of gedeeltelijk geautomatiseerde/systematische verwerking van persoonsgegevens, die plaatsvindt onder de verantwoordelijkheid van het Alfa-college evenals op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen. Het IBP-beleid is ook van toepassing op niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.
- IBP-beleid heeft binnen het Alfa-college raakvlakken met:

[2] Bewerkt artikel 2, lid 2 van de AVG.

- *Algemeen veiligheids- en toegangsbeveiligingsbeleid;* met als aandachtspunten bedrijfshulpverlening, fysieke toegang en beveiliging, crisismanagement, huisvesting en ongevallen.
- *HRM beleid;* met als aandachtspunten in- en uitstroom van medewerkers, functiewisselingen, functiescheiding en vertrouwensfuncties.
- *Informatiebeleid*; met als aandachtspunten hoe om te gaan met proces(ketens), applicaties, gegevens en informatie, eigenaarschap en de inzet van middelen t.a.v. informatisering.
- *Medezeggenschap;* Indien aanpassingen in het IBP-beleid op enigerlei wijze impact hebben op de persoonlijke levenssfeer van studenten en/of medewerkers, dienen deze aanpassingen ter instemming te worden voorgelegd aan de Studentenraad en/of Ondernemingsraad.

Beleidsuitspraken

Het Alfa-college hanteert de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging en privacy te bereiken:

Informatiebeveiliging:

Verantwoordelijke

In termen van de wet is het bestuur de verwerkingsverantwoordelijke.
Het College van Bestuur van het Alfa-college heeft de verantwoordelijkheid te zorgen dat informatiebeveiliging en privacy geborgd zijn.

Wet- en regelgeving

Het Alfa-college voldoet aan alle relevante wet- en regelgeving. Dit wordt nader uitgewerkt in het hoofdstuk Compliance.

Continue verbeteren

Informatiebeveiliging en privacy is bij het Alfa-college een continu kwaliteitsproces, waarbij regelmatig (minimaal jaarlijks) wordt getoetst of aanpassing van beleid en/of procedures gewenst dan wel noodzakelijk is. Bij de evaluatie van IBP-beleid wordt aandacht besteed aan:

- De effectiviteit van de geïmplementeerde maatregelen;
- De aansluiting van het beleid bij de nieuwe privacy-eisen van de organisatie;
- De effectiviteit van het beleid;

Bovenstaande bevindingen kunnen leiden tot aanpassingen in maatregelen, procedures, processen of beleid.

Gedragscode en geheimhoudingsverklaring

Binnen het Alfa-college is het veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van een ieder. Hierbij hoort niet alleen het actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie, maar ook van papieren documenten.
Het Alfa-college verwacht van alle medewerkers, studenten, (geregistreerde) bezoekers en externe relaties dat zij zich ‘fatsoenlijk’ gedragen met een eigen verantwoordelijkheid. Het is niet acceptabel dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagoverlies. Het Alfa-college heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd. In deze code staat ook het sanctiebeleid beschreven.

In de CAO is een passage opgenomen waarin de geheimhouding is geregeld. Bij het inhuren van externe medewerkers wordt gevraagd een zorgvuldigheidsverklaring te tekenen.

Intellectueel eigendom
Het Alfa-college is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert de school informatie, waarvan het eigendom (auteursrecht) toebehoort aan derden. Medewerkers en studenten worden goed geïnformeerd over de regelgeving rondom het gebruik van informatie.

Awareness
Het Alfa-college bewerkstelligt dat alle medewerkers zich bewust zijn van bedreigingen en gevaren voor informatiebeveiliging, van hun verantwoordelijkheid en aansprakelijkheid, en dat ze zijn toegerust om het informatiebeveiligingsbeleid en het privacy beleid van de organisatie in hun dagelijkse werkzaamheden uit te voeren.
Medewerkers volgen een passende training voor bewustwording van informatiebeveiliging, de privacywetgeving en de geldende regelgeving van het Alfa-college.
IBP-functionarissen houden het kennisniveau op pijl door middel van relevante opleidingen en lidmaatschap van IBP-netwerken.

Inname bedrijfsmiddelen
Medewerkers leveren alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst in. In de beëindigingsprocedure is formeel het teruggeven van alle door het Alfa-college aan de medewerker verstrekte fysieke en elektronische bedrijfsmiddelen opgenomen.

Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein
Bedrijfsmiddelen die zich buiten het terrein bevinden, behoren te worden beveiligd, waarbij rekening behoort te worden gehouden met de verschillende risico's van werken buiten het terrein van de organisatie.

Clear desk en clear screen
Het Alfa-college past een "Clear Desk" en "clear screen" beleid toe voor PC's , papieren en verwijderbare opslagmedia, om het risico van onbevoegde toegang tot, verlies van en schade aan informatie te beperken.

Classificatie van informatie
Het Alfa-college classificeert informatie en informatiesystemen conform het classificatiemodel. De classificatie is het uitgangspunt voor de risicoanalyse en de te nemen maatregelen. Er is een balans tussen de risico's die we willen afdekken en de benodigde investeringen en de te nemen maatregelen.
Door middel van een risico-afhankelijkheidsanalyse wordt het beschermingsniveau vastgesteld van de processen, gegevens en informatiesystemen. Voor ieder geclassificeerd object wordt een classificatieschema ingevuld.
Het beschermingsniveau dat in het classificatieschema wordt vastgelegd komt tot stand door de eisen ten aanzien van beschikbaarheid, integriteit en vertrouwelijkheid voor de desbetreffende informatie te analyseren. Deze eisen worden vastgesteld met de waarden:
Laag / Midden / Hoog

Labeling van gegevens
Gegevens beveiligen we op gepaste wijze. Daartoe worden zakelijke - en persoonsgegevens ingedeeld in vier klassen:
1. Openbaar
2. Intern gebruik
3. Vertrouwelijk
4. Geheim
Hoe hoger de klasse, hoe stringenter de maatregelen zoals het inrichten van autorisatieniveaus. De classificatie van de gegevens en de autorisatiematrix zijn vastgelegd in het verwerkingenregister.

Informatieopslag
Persoonsgegevens mogen niet op mobiele apparatuur zoals laptops, losse harde schijven of usb sticks opgeslagen worden. Dit om te voorkomen dat bij diefstal of verlies van dit apparaat onbevoegden toegang tot de persoonsgegevens kunnen krijgen. Persoonsgegevens dienen op beschermde, beveiligde omgevingen van het Alfa-college (Het netwerk of “cloud” omgeving van het Alfa-college) te worden opgeslagen.

Informatietransport en -transacties
Er dient toezicht te worden gehouden op de uitwisseling van informatie binnen de organisatie en daarbuiten. Deze uitwisseling dient in overeenstemming te zijn met de wetgeving die van toepassing is. Dit is van toepassing voor zowel digitale als fysieke vormen van uitwisseling en overdracht. Indien mobiele apparatuur gebruikt wordt om deze informatie te transporteren zoals laptops, losse harde schijven of usb sticks moet deze apparatuur tegen onbevoegde toegang beschermd zijn door middel van encryptie. Dit is nader uitgewerkt in de richtlijn cryptografische maatregelen.
Indien mogelijk wordt gebruik gemaakt van beveiligde bestandsomgevingen en beveiligde E-mail toepassingen.
Informatie die deel uitmaakt van transacties van toepassingen behoort te worden beschermd ter voorkoming van onvolledige overdracht, foutieve routering, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen.

Fysieke informatiebeveiliging
Het Alfa-college neemt passende maatregelen om apparatuur, ruimten en (cloud)omgevingen die Informatie en ICT middelen bevatten die kritieke of gevoelige bedrijfsactiviteiten ondersteunen te beschermen tegen interceptie, verstoring of andere schade. De geboden bescherming dient in overeenstemming te zijn met de vastgestelde risico’s.

Toegangsbeveiliging
Gebruikers behoren alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn. Rechten worden verleend en ingetrokken door middel van een formele procedure.
Identificatie, Authenticatie en Autorisatie van gebruikers zijn op netwerkniveau en applicatieniveau ingericht.
Gebruikersrechten zijn gedefinieerd en gedocumenteerd in de autorisatiematrix.
Periodieke controle op toegangsrechten wordt uitgevoerd en gedocumenteerd.

Wachtwoordbeleid

Het Alfa-college past een wachtwoordbeleid toe om het risico van onbevoegde toegang tot en verlies van en schade aan informatie te beperken. User ID en Password worden op veilige wijze verstrekt aan medewerkers en studenten.

Ontnemen van rechten
Bij het beëindigen van het dienstverband van een medewerker en de loopbaan van de student worden alle rechten ontnomen. Als een medewerker binnen het Alfa-college wijzigt van functie worden de rechten behorend bij de oude functie ontnomen.

Beveiliging van thuiswerkplekken
Verbinding met applicaties binnen het Alfa-netwerk kan alleen via een beveiligde en versleutelde VPN-verbinding plaatsvinden. Thuiswerkplekken die een verbinding met het Alfa-netwerk willen opzetten dienen adequaat beveiligd te zijn tegen schadelijke software (virussen, wormen, malware).

Verwijderen bedrijfsmiddelen
Apparatuur, informatie en programmatuur van de organisatie mogen niet zonder toestemming vooraf van de locatie worden meegenomen. (Er is duidelijk vastgesteld wie vanuit welke rol toestemming hebben om apparatuur mee te nemen of buiten de locatie te gebruiken. Er zijn tijdslimieten en bij inlevering wordt gecontroleerd op de naleving daarvan. Waar nodig wordt geregistreerd wat de locatie verlaat en wanneer het weer wordt teruggebracht.)

Technische kwetsbaarheden
Als een potentieel technische kwetsbaarheid is geïdentificeerd, stelt het Alfa-college de samenhangende risico's en de te ondernemen acties vast; een dergelijke actie kan bijvoorbeeld patching van de kwetsbare systemen inhouden. Een patch wordt ingezet om fouten in systemen op te lossen of om een systeem een update te geven.
Patches behoren te worden getest en geëvalueerd voordat ze worden geïnstalleerd om te waarborgen dat ze doeltreffend zijn en niet resulteren in bijverschijnselen. Indien geen patch beschikbaar is, behoren andere beheersmaatregelen te worden overwogen, zoals:
a) diensten of capaciteiten die de kwetsbaarheid uitschakelen;
b) toegangsbeveiligingsmaatregelen aanpassen of toevoegen;
c) vaker monitoren om werkelijke aanvallen op te sporen;
d) bewustzijn omtrent de kwetsbaarheid te kweken.

Wijzigingsbeheer
Wijzigingen in informatiesystemen en toepassingsprogrammatuur worden beheerst met strikt wijzigingsbeheer.
In het bijzonder met de volgende aspecten wordt rekening gehouden:
a) identificatie en registratie van significante veranderingen;
b) plannen en testen van veranderingen;
c) de potentiële impact van dergelijke veranderingen beoordelen, waaronder de impact voor de informatiebeveiliging.

Scheiding van ontwikkel-, test- en productieomgevingen
Ontwikkel-, test- en productieomgevingen zijn gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te voorkomen.

Ontwikkel- en testactiviteiten kunnen ernstige problemen veroorzaken, bijvoorbeeld ongewenste wijziging van bestanden of systeemomgeving, storingen in het systeem of datalekken. Het is nodig een bekende en stabiele omgeving te onderhouden voor het uitvoeren van zinvolle testen en om ongepaste toegang van de ontwikkelaar tot de productieomgeving te voorkomen.
In ontwikkel- en testomgevingen moet gebruik gemaakt worden van anonieme testdata

Scheiding van netwerken
Groepen van informatiediensten, -gebruikers en -systemen maken gebruik van gescheiden netwerken. Het ICT-onderwijs netwerk is virtueel gescheiden van het Alfa-college netwerk waar alle andere gebruikers op werken.

Bescherming tegen malware
Het Alfa-college maakt gebruik van software die malware opspoort en de oorspronkelijke software herstelt. Voorlichting over het herkennen van malware maakt onderdeel uit van het bewustwordingsprogramma van informatiebeveiliging.

Bedrijfscontinuïteit
Er worden maatregelen genomen om de uitwerking op de organisatie, veroorzaakt door het verlies van informatie (als gevolg van bijvoorbeeld natuurrampen, ongevallen, uitval van apparatuur en opzettelijke handelingen) en het herstellen daarvan, tot een aanvaardbaar niveau te beperken.
Ten aanzien van de informatievoorziening moeten adequate back-up en recovery faciliteiten beschikbaar zijn om te waarborgen dat alle essentiële informatie en software na een calamiteit of na falen van media kan worden hersteld. Het Alfa-college heeft dit nader uitgewerkt in het Backup en recoverybeleid.

Verslaglegging en monitoren
Het Alfa-college maakt gebruik van monitoren en logging van toegang tot en gebruik van informatiesystemen voor het ontdekken en registreren van ongewenst gebruik en het traceren van de gebruiker in geval van misbruik.
Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, worden gemaakt, bewaard en regelmatig beoordeeld. Logbestanden zijn beveiligd tegen manipulatie.

Privacy:

Basisregels bij het omgaan met persoonsgegevens
Bij het verwerken van persoonsgegevens zijn de wettelijke beginselen inzake verwerking persoonsgegevens (art.5 AVG) leidend. Deze zijn samengevat in de **vijf vuistregels** met betrekking tot de omgang met persoonsgegevens te weten:

1. **Doelbepaling en doelbinding**: persoonsgegevens worden alleen gebruikt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking vastgesteld, inclusief de bewaartermijnen. Persoonsgegevens worden niet verder verwerkt op een manier die onverenigbaar is met de doelen waarvoor ze zijn verkregen.
2. **Grondslag**: verwerking van persoonsgegevens is gebaseerd op een van de zes wettelijke grondslagen; Toestemming, Overeenkomst, Wettelijke verplichting, Vitaal belang, Algemeen belang en 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 tot het doel (proportioneel). Het doel kan niet met minder, alternatieve of andere gegevens worden bereikt (subsidiar). Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk.
4. **Transparantie**: de school legt aan betrokkenen (studenten, hun ouders 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 informatie, inzage, verbetering, aanvullen, het wissen van gegevens, beperking van verwerking, verzet, dataportabiliteit, afscherming en profilering van hun persoonsgegevens. Tevens 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 volledig, juist en actueel zijn.

Register van verwerkingen
Het Alfa-college legt alle verwerkingen van persoonsgegevens vast in een dataregister en houdt dit register up-to-date. Het Alfa-college voldoet hiermee aan de documentatieplicht, zoals benoemd in de AVG.
De volgende onderdelen worden hier in verwerkt:

- Verwerkingsdoeleinden;
- Beschrijving Categorieën betrokkenen en categorieën persoonsgegevens;
- Contactgegevens FG, verantwoordelijke en verwerker;
- Categorieën ontvangers;
- Bewaartermijnen;
- Technische en organisatorische beveiligingsmaatregelen;
- Indien van toepassing doorgifte naar derde land of internationale organisatie.

DPIA (Data Protection Impact Assessment)
Om te zorgen dat alle verwerkingen blijvend aan de AVG voldoen voert het Alfa-college tijdig een DPIA uit. Een DPIA is verplicht bij:

1) Profiling
2) Grootschalige verwerking van bijzondere persoonsgegevens
3) Gegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten
4) Stelselmatige en grootschalige monitoring van openbare ruimten
5) Alle andere verwerkingen die de Autoriteit Persoonsgegevens (AP) aanwijst.

Het Alfa-college kiest er voor om alle (wijzigingen in) verwerkingen vooraf te toetsen door middel van een DPIA. Wanneer en hoe een DPIA wordt uitgevoerd is vastgelegd in de procedure DPIA.

Verwerkersovereenkomst
Het Alfa-college sluit met alle leveranciers die in opdracht van het Alfa-college persoonsgegevens verwerken een verwerkersovereenkomst af. Daarnaast zijn er anderen vormen van overeenkomsten bijvoorbeeld een gegevensuitwisselingsovereenkomst tussen verwerkingsverantwoordelijken.

Functionaris gegevensbescherming

Het Alfa-college heeft een gecertificeerde Functionaris Gegevensbescherming. De FG houdt binnen de organisatie toezicht op de toepassing en naleving van de Privacywetgeving.

Privacy bij design:
Het Alfa-college kijkt bij wijzigingen (denk ook aan uitfasering) in de infrastructuur of de aanschaf van nieuwe (informatie)systemen vóóraf naar de impact hiervan op de informatiebeveiliging en privacy, zodat tijdig de juiste maatregelen genomen kunnen worden.

Privacy bij default:
De standaardinstellingen van producten en diensten moeten zo worden ingericht dat de betrokkenen maximale privacy wordt geboden.

Verwerking t.b.v. onderzoek
Persoonsgegevens mogen worden verwerkt ten behoeve van:
• archivering in het algemeen belang (Archiefwet);
• wetenschappelijk of historisch onderzoek; of
• statistische doeleinden
indien passende technische en organisatorische maatregelen zijn genomen om de privacy van de betrokken deelnemers te garanderen. Onder deze maatregelen wordt in ieder geval verstaan dat er niet meer persoonsgegevens worden verwerkt dan strikt noodzakelijk is. Hierbij valt te denken aan pseudonimisering (in geval de data herleidbaar moet zijn tot individuen) of anonimisering (in geval data niet herleidbaar hoeft te zijn).

Bewaartermijnen
Het Alfa-college zorgt dat geldende bewaar- en vernietigingstermijnen worden gerespecteerd:
- Het Alfa-college gebruikt de selectielijst voor het MBO en het Document Structuur Plan (DSP) model) voor het bepalen van de bewaartermijnen;
- De bewaartermijnen zijn in het register van verwerkingen opgenomen;
- De betrokkenen worden geïnformeerd over de bewaartermijnen.

Technische en organisatorische maatregelen
Het Alfa-college en/of haar verwerker neemt passende organisatorische of technische (beveiligings-) maatregelen om persoonsgegevens en overige data te beschermen tegen de risico's, die de voortgang van het onderwijs, de privacy en de bedrijfsvoering kunnen verstoren. De effectieve werking van deze maatregelen kan worden aangetoond.

Beveiligingsincidenten en datalekken
Het Alfa-college zal alle beveiligingsincidenten en datalekken vastleggen en volgens het protocol datalekken afhandelen. Indien nodig worden de incidenten gemeld bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen.

Compliance

In dit hoofdstuk beschrijven we aan welke wet- en regelgeving het Alfa-college in het kader van de Informatiebeveiliging en privacy moet voldoen en hoe we borgen dat we hieraan voldoen.

Relevante wet- en regelgeving

De uitwerking van het beleid voldoet aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder: (zie gedetailleerde uitwerking in Bijlage 3)

- Wet Educatie en Beroepsvorming (WEB)
- Branche code Goed Bestuur MBO, MBO Raad
- Wet Inspectietoezicht
- Algemene Verordening Gegevensbescherming (AVG)
- Archiefwet
- Auteurswet
- Wetboek van Strafrecht
- Koppelingswet

Het internationale normenkader voor informatiebeveiliging NEN-ISO/IEC 27001 en 27002 (2015) is leidend voor de te nemen beveiligingsmaatregelen.
Het Alfa-college hanteert het Toetsingskader Informatiebeveiliging en Privacy dat ontwikkeld is door saMBO-ICT, Kennisnet en SURF onder verantwoordelijkheid van de regiegroep IBP in het MBO.

Ondersteunende richtlijnen en procedures

Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen geven invulling aan de uitwerking van het beleid.
Bijlage 1 geeft een overzicht van deze richtlijnen en procedures.

Voorlichting en bewustzijn

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging en privacy uit te sluiten. De mens is hier een belangrijke factor. Daarom wordt 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, leerlingen en gasten. Verhoging van het IBP-bewustzijn is een gezamenlijke verantwoordelijkheid van de FG, en/of de adviseur Informatiebeveiliging en Privacy met het College van Bestuur als eindverantwoordelijke.

Classificatie en risicoanalyse

Alle gegevens en informatiesystemen waarop dit beleid van toepassing is worden geclassificeerd. Het niveau van de te nemen 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 kwaliteitscriteria die van belang zijn.
Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen, wordt vóóraf gekeken naar de impact van de ontwikkelingen en de beoogde verwerkingen op informatiebeveiliging en privacy, zodat passende maatregelen genomen kunnen worden.

Incidenten en datalekken

Alle medewerkers die een beveiligingsincident of datalek vermoeden dienen dit te melden. Het melden van beveiligingsincidenten en datalekken is vastgelegd in een protocol. De afhandeling van deze incidenten volgt een gestructureerd proces, dat ook voorziet in de juiste stappen rondom de meldplicht datalekken. Alle (beveiligings-)incidenten worden vastgelegd in een incidentenregister. Alle (beveiligings-)incidenten kunnen worden gemeld bij het ICT servicepunt.
Periodiek zullen de beveiligingsincidenten besproken worden en waar nodig aanvullende passende beleidsmaatregelen genomen worden.
Ook naar studenten, medewerkers en externen is gecommuniceerd op welke manier zij kwetsbaarheden en incidenten moeten melden.

Accountability

Het IBP-beleid wordt jaarlijks gereviewed en eventueel bijgesteld door de Adviseur Informatiebeveiliging en Privacy en vastgesteld door het CvB. Hierbij wordt rekening gehouden met:

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

Daarnaast kent het Alfa-college een jaarlijks verbeterplan voor informatiebeveiliging en privacy. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het IBP-beleid wordt getoetst. Tevens worden hier actuele ontwikkelingen op het gebied van techniek, wet- en regelgeving et cetera meegenomen. Eén en ander leidt tot een jaarplan IBP.

Naleving en sancties

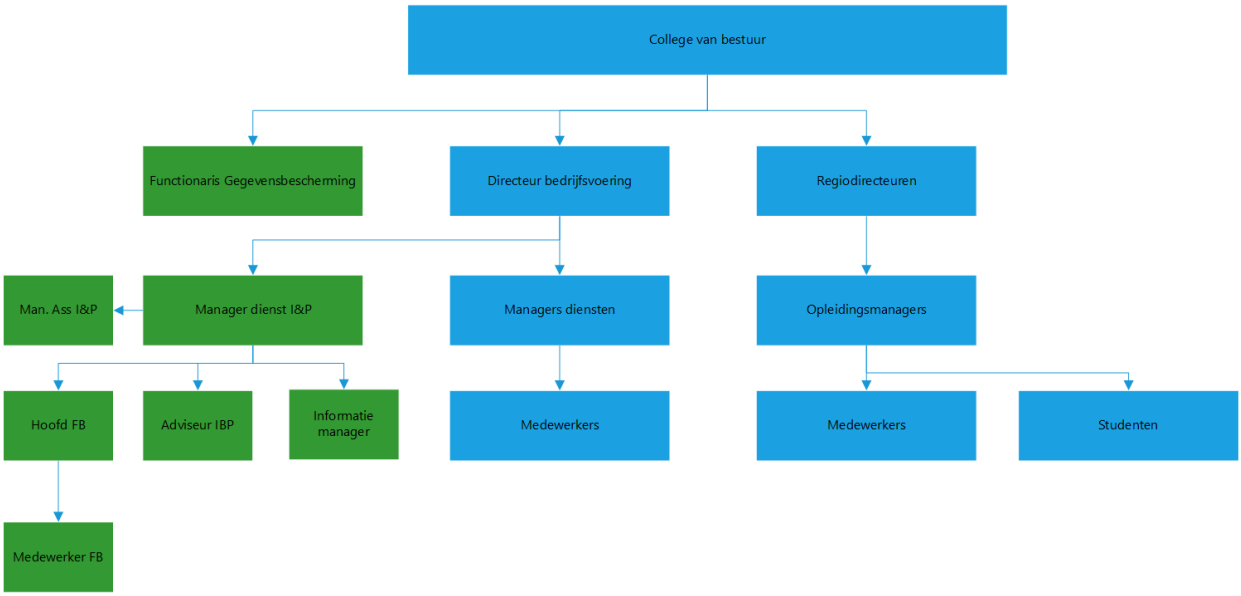
Naleving van ons IBP-beleid is een verantwoordelijkheid van alle medewerkers binnen het Alfa-college. Daarnaast nemen de leidinggevenden en proceseigenaren hun verantwoordelijkheid om hun medewerkers aan te spreken in geval van tekortkomingen. Er wordt actief aandacht besteed aan IBP-zaken bij indiensttreding, door communicatie van de gedragscode, en bewustwordingscampagnes.
Voor toezicht op de naleving van de AVG vervult de Functionaris voor Gegevensbescherming (FG) een belangrijke rol. De FG wordt aangesteld door het College van Bestuur, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak.
Mocht de naleving van dit beleid ernstig tekortschieten, dan kan het Alfa-college de betrokken verantwoordelijke medewerkers een sanctie op leggen binnen de kaders van de CAO en de wettelijke mogelijkheden.

Logging en monitoring

Door middel van logging en monitoring worden gebeurtenissen met betrekking tot geautomatiseerde systemen en toegang tot gegevens vastgelegd. Hieronder vallen onder andere het in- en uitloggen van gebruikers en (pogingen tot) ongeautoriseerde toegang tot het netwerk. Het Alfa-college beoordeelt deze logbestanden met regelmaat.

Governance

Informatiebeveiliging en Privacy organisatie



Taken en verantwoordelijkheden

College van Bestuur:
Het College van Bestuur is verantwoordelijk voor het opstellen en uitdragen van het organisatiebeleid en het Informatiebeveiliging en Privacy beleid dat daarvan is afgeleid.

Daarnaast houdt het College van Bestuur controle op de naleving van het afgesproken beleid en bijbehorende wet- en regelgeving en is de "Verwerkingsverantwoordelijke" in het kader van de Algemene Verordening Gegevensbescherming (AVG).

Directie
De directeuren zijn verantwoordelijk voor de implementatie, de uitvoering en naleving van het Informatiebeveiliging en Privacy beleid in hun organisatorische eenheid.

Manager Dienst Informatisering en Projecten
De manager van de dienst Informatisering en Projecten is verantwoordelijk voor de voorbereiding van het strategisch, tactisch en operationeel beleid op het gebied van informatisering en is verantwoordelijk voor het implementeren, de uitvoering en naleving van het Informatiebeveiliging en Privacy beleid in zijn organisatorische eenheid

Informatiemanagers en adviseur Informatiebeveiliging en Privacy
De adviseur Informatiebeveiliging en Privacy en de informatiemanagers dragen zorg voor de ontwikkeling, implementatie en uitvoering en naleving van het beleid binnen de dienst Informatisering en Projecten. Zij bewaken en evalueren dit beleid waaronder het Informatiebeveiliging en Privacy beleid.

Lijnmanagers:
De opleidingsmanagers en de managers van de diensten zijn verantwoordelijk voor de uitvoering en naleving van het Informatiebeveiliging en Privacy beleid binnen de eigen organisatorische eenheid.

Medewerkers:
Alle medewerkers van het Alfa-college zijn verantwoordelijk voor de uitvoering en naleving van het Informatiebeveiliging en Privacy beleid binnen hun eigen werkzaamheden.

Studenten:
Alle studenten van het Alfa-college zijn aanspreekbaar op de uitvoering en naleving van het Informatiebeveiliging en Privacy beleid in het kader van hun opleidingsactiviteiten.

Functionaris Gegevensbescherming
De Functionaris Gegevensbescherming (FG) legt direct verantwoording af aan het College van Bestuur. De FG informeert en adviseert de verwerkingsverantwoordelijke, de medewerkers en de studenten van het Alfa-college over hun verplichtingen ten aanzien van de Algemene Verordening Gegevensbescherming en andere gegevensbeschermingsbepalingen. De FG houdt binnen de organisatie toezicht op de toepassing en naleving van de privacywetgeving en het Informatiebeveiliging en Privacy beleid. De FG zorgt voor de training en bewustwording van de medewerkers en studenten ten aanzien van de privacywetgeving, voert audits uit en beoordeeld de data protection impact assessments (DPIA's). De FG is het eerste aanspreekpunt voor de Autoriteit Persoonsgegevens.

Aanspreekpunt voor Privacy:
De FG is het eerste aanspreekpunt voor vragen over Privacy.
De adviseur Informatiebeveiliging en Privacy en de Portefeuillehouders privacy op de locaties van het Alfa-college zorgen samen met de FG ervoor dat vragen over Privacy, datalekken en rechtenverzoeken op de juiste wijze worden afgehandeld en betrokkenen van het Alfa-college goed worden geïnformeerd.

Verantwoording

Informatiebeveiliging en Privacy is onderdeel van de Governance en Compliance van het Alfa-college. De Functionaris Gegevensbescherming adviseert en ziet toe op het beleid ten aanzien van Informatiebeveiliging en Privacy. Het Alfa-college en de verwerkers van de applicaties zorgen voor een effectieve werking van de organisatorische en technische maatregelen en het inrichten van de IT en de processen.
Door middel van audits wordt de effectieve werking van de maatregelen aangetoond. De FG ziet toe op de privacy en security boekhouding.

Jaarlijks levert de Functionaris gegevensbescherming een rapport op met de status van Informatiebeveiliging en privacy. Dit rapport wordt aan het College van Bestuur, de Raad van Toezicht gepresenteerd. De uit het rapport volgende verbeter- en ontwikkelpunten worden in het jaarplan Informatiebeveiliging en Privacy verwerkt. Tevens schrijft de FG de “Declaration of Accountability”(DOA). De DOA bevat een mededeling (rapportage) over het voldoen aan de AVG.

Bijlage 1: Ondersteunende documenten

Informatiebeveiliging

- Classificatiemodel
- Documentair Structuur Plan (DSP)
- *Intellectuele eigendomsrechten (wordt deel van de Gedragscode)*
- Clear Desk, clear screen beleid
- Responsible disclosure verklaring
- *Richtlijn cryptografische maatregelen (wordt in 2020 opgesteld)*
- Gedragscode inzake het gebruik van en toezicht op informatie- en communicatiesystemen
- Back-up en Recovery beleid
- Printbeleid
- Telefoniebeleid
- Werkplekbeleid
- Procedure meldplicht datalekken
- Procedure Informatiebeveiligingsincident leveranciers
- Calamiteitenplan ICT / business continuïty plan
- Wachtwoordbeleid
- Toegangsbeveiliging (procedure autorisatiebeheer*)*
- *Monitoring en Logging (wordt in 2020 opgesteld)*

Privacy

- Procedure toestemming gebruik beeldmateriaal (toestemmingsverklaring)
- *Procedure voor verwijderen van gegevens (wordt in 2020 opgesteld)*
- Communicatie rechten betrokkenen (privacystatement)
- Procedure rechtenverzoeken
- Privacyreglementen (medewerkers / studenten)
- Richtlijnen Social Media (AlfaConnect Veilige school)
- Procedure Meldplicht Datalekken
- Dataregisters
- Verwerkersovereenkomsten
- Procedure Gegevensbeschermingseffectbeoordeling (DPIA) incl BIV!
- Cameraprotocol

De cursief opgenomen documenten zijn nog niet ontwikkeld. Vaak is de inhoud elders beschreven.

Bijlage 2: Verklarende woordenlijst

AVG: Algemene Verordening Gegevensbescherming.

Beleid: Beleid met betrekking tot het verwerken en beschermen van persoonsgegevens door het Alfa-college.

Beschikbaarheid: De mate waarin de informatie op het juiste moment beschikbaar is voor gebruikers.

Betrokkene: Een individueel en natuurlijk persoon op wie een persoonsgegeven betrekking heeft.

Beveiligingsincident: Een gebeurtenis die de betrouwbaarheid van de informatie of de informatieverwerking kan verstoren.

Broneigenaar: Aangewezen directeur die verantwoordelijk is voor persoonsgegevens van één of meerdere categorieën van Betrokkenen. De Broneigenaar voert de persoonsgegevens in en zorgt voor de vernietiging. In de tussentijd leent hij ze uit aan de organisatorische eenheden binnen [mbo-instelling]. De organisatorische eenheden mogen dan de persoonsgegevens verrijken.

Datalek: Een inbreuk in verband met persoonsgegevens, die leidt tot enige ongeoorloofde verwerking daarvan. Hier vallen zowel opzettelijke als onopzettelijke inbreuken onder.

Dataportabiliteit: Het recht om persoonsgegevens en informatie over te dragen aan een nieuwe verwerker zonder technische problemen.

Dataregister: De AVG spreekt van het Register van Verwerkingsactiviteiten, dit is een overzicht van de persoonsgegevens die verwerkt worden, met informatie over het doel daarvan, de grondslag daarvoor, de bewaartermijnen van de gegevens en bron of ontvanger van de gegevens.

DPIA: Data Protection Impact Assessment (Gegevensbeschermingseffectbeoordeling): een beoordeling die helpt bij het identificeren van privacy risico's en de handvaten levert om deze risico's te verkleinen tot een acceptabel niveau. Soms ook wordt de term PIA gebruikt, Privacy Impact Assessment.

Functionaris voor Gegevensbescherming: Interne toezichthouder en privacy adviseur aangesteld door het College van Bestuur, op grond van artikel 37 van de AVG, ook wel aangeduid als FG.

Informatiebeveiliging: Het vakgebied dat zich richt op het beveiligen van informatie, het maken van plannen om te voorkomen dat er beveiligingsincidenten plaatsvinden, en het nemen van maatregelen om de gevolgen daarvan te verkleinen.

Integriteit: De mate waarin de gegevens een afspiegeling zijn van de werkelijkheid. Het omvat onder anderen de kenmerken correctheid, volledigheid, nauwkeurigheid en controleerbaarheid.

Minderjarige: Voor de AVG geldt iedere persoon die de leeftijd van 16 jaar nog niet heeft bereikt. Buiten de AVG geldt jonger dan 18 jaar.

Niet-geautomatiseerde verwerking: Voorbeelden: aangetekende stukken, pasjes die zichtbaar gedragen worden, klassenlijsten met foto's (smoelenboek), etc.

Persoonsgegeven: Elk gegeven betreffende een geïdentificeerd of identificeerbaar natuurlijk persoon.

Privacy by Default: Een gegevensverwerking waarbij de standaardinstellingen van producten en diensten zo zijn ingesteld dat de privacy van betrokkenen maximaal wordt gewaarborgd. Dit betekent onder meer dat er zo min mogelijk gegevens worden gevraagd en verwerkt.

Privacy by Design: Al tijdens de ontwikkeling van producten en diensten (zoals informatiesystemen) wordt ten eerste aandacht besteed aan privacy verhogende maatregelen. Ten tweede wordt rekening gehouden met dataminimalisatie: er worden zo min mogelijk persoonsgegevens verwerkt, alleen de gegevens die noodzakelijk zijn voor het doel van de verwerking.

Ontvanger: Degene aan wie de persoonsgegevens worden verstrekt.

Ondubbelzinnige toestemming:

	De betrokkene heeft voor de verwerking zijn ondubbelzinnige toestemming gegeven. Deze uitdrukkelijke toestemming wordt ook geïnformeerde toestemming of informed consent genoemd. Dat betekent dat de betrokkene exact weet waar hij of zij toestemming voor gegeven heeft.
Vertrouwelijkheid:	De mate waarin de toegang tot en het gebruik van gegevens beperkt is tot de juiste personen.
Verwerker:	Een door het Alfa-college ingeschakelde (derde) partij die ten behoeve van het Alfa-college, en op basis van haar schriftelijke instructies, persoonsgegevens verwerkt, e.e.a. vastgelegd in een verwerkersovereenkomst.
Verwerking:	Elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder het verzamelen, vastleggen, ordenen, opslaan, raadplegen, bijwerken, afschermen, wissen of vernietigen van gegevens.
Verwerkingsverantwoordelijke:	Het bestuursorgaan dat, alleen of tezamen met anderen het doel en de middelen van de verwerking van persoonsgegevens vaststelt.

Bijlage 3: Relevante wet- en regelgeving

Voor de Informatiebeveiliging en Privacy zijn de volgende wetgevingen van belang:

Wet- en regelgeving	**Relevantie**
Algemene verordening gegevensbescherming	De AVG heeft m.i.v. 25 mei 2018 de Richtlijn 95/46/EG vervangen.
Europees Verdrag Rechten van de Mens en fundamentele vrijheden (EVRM), artikel 8.	Artikel 8 EVRM vormt de basis van het privacy recht in de breedste zin van het woord. Het is een verdrag van de Raad van Europa.
Grondwet, artikel 10	De Nederlandse basis voor het privacy recht
Internationaal Verdrag inzake Burgerrechten en Politieke Rechten (IVBPR), artikel 17	Het internationale recht op privacy en gegevensbescherming
Handvest Grondrechten van de EU, artikel 7, 8 en 52(1)	De basis voor privacy recht vanuit de Europese Unie
Wet algemene bepalingen Burgerservicenummer	
Wet op de computercriminaliteit	
Telecommunicatiewet	
Archiefwet	
Sectorale Europese regelgeving	Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie), 2002/58/EG, 31 juli 2002 Richtlijn van het Europees Parlement en de Raad houdende maatregelen om een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de Unie te waarborgen, 7 februari 2013, NIB COM (2013) 48 final Verordening nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt, 4 juni 2012
Sectorale Nederlandse regelgeving	In de onderwijssector is specifieke regelgeving van toepassing. Denk aan de WEB, Wet op de loonbelasting, Ziektewet, WIA, de Jeugdwet, de leerplicht en wetgeving ten aanzien van VSV (voortijdig schoolverlaters).