Informatiebeveiligings- en privacy beleid

Naam	Stichting Ultiem
Van	Bestuurder (Verwerkingsverantwoordelijke) en Functionaris Gegevensbescherming
Aan	Alle betrokkenen
Datum	09-07-2020
Betreft	Informatiebeveiligings- en privacy beleid
Document	ULTIEM 29104 - Rev.2.0 09-07-2020
Bron	Kennisnet

Het informatiebeveiligings- en privacy beleid is aangepast aan de eisen en termen vanuit de AVG. Elke organisatie moet niet alleen de privacywetgeving naleven, maar moet ook aantoonbaar voldoen aan de AVG.

Dit document geeft een toelichting op het IBP beleid 2.0 (formeel). Het heeft dezelfde inhoud, maar is voorzien van een extra kolom met verdere uitleg per stap en verwijzingen naar onderliggende documenten, afspraken en procedures. Hiermee wordt de 'kapstokfunctie' van het beleid inzichtelijker.

Inhoudsopgave

Toelichting

Dit document bevat het IBP-beleid met in de rechter kolom een toelichting op het IBP-beleid. In de rechter kolom staan toelichtingen op het beleid en verwijzingen naar onderliggende documenten, afspraken en procedures. Dit geeft organisaties de nodige handvatten voor de te maken afspraken en maakt inzichtelijk wat de link is tussen een protocol en het ‘kapstokhaakje’ in het IBP-beleid.

0. Document geschiedenis

0.1. Revisies

Onderstaande tabel beschrijft de geschiedenis van dit document

Versie	Datum	Toelichting
2.0	27-08-2020	

0.2. Goedkeuring

Dit beleid is goedgekeurd door de onderstaande personen:

Naam	Functie	Versie	Datum
M.H.W. Bakker	Bestuurder	2.0	02-09-2020

IBP beleid

Het belang van informatiebeveiliging en privacy

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. 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.

Toelichting informatiebeveiliging en privacy

2.1 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 juist en volledig zijn.
- Vertrouwelijkheid: de mate waarin de toegang tot gegevens en/of functionaliteiten beperkt is tot degenen die daartoe bevoegd zijn.

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

Toelichting op het IBP beleid

Toelichting en verwijzingen
Het opstellen van een IBP-beleid valt onder de verantwoordelijkheid van de bestuurder (de rechtspersoon waar scholen onder vallen).
IBP gaat in eerste instantie niet om technische maatregelen of fysieke toegang, niet om ICT, maar om gedrag, cultuur en bewustwording. Iedereen moet het IBP-beleid kunnen lezen en begrijpen. Daarom is het goed om na te denken over een korte, bondige inleiding, die direct aangeeft waarom IBP belangrijk is en die geschreven is in een 'taal' die bij jouw organisatie past.
Een vastgesteld en bij iedereen bekendgemaakt IBP-beleid met duidelijke doelen, uitgangspunten en vastgelegde verantwoordelijkheden vormen dan ook de basis, de kapstok, om processen, richtlijnen en procedures rondom IBP goed te regelen.

Deze uitleg is cruciaal om in het begin te geven. Daarmee leg je niet alleen uit waarom het relevant is, maar maak je ook duidelijk waar de term IBP-beleid vandaan komt.
Deze aspecten van betrouwbaarheid zijn niet vrij te interpreteren maar zijn strikt gedefinieerd en dus niet op verschillende manieren uit te leggen.
Onder informatievoorziening wordt verstaan: apparatuur, programmatuur, gegevens, procedures en mensen.
Het is van belang om de risico's in beeld te krijgen en tot een minimum te beperken.

Verwijzing naar: classificeren en risicoanalyse

We werken met persoonsgegevens (van onszelf, leerlingen en anderen), hierop is privacywetgeving van toepassing. (tot 25 mei 2018 de Wbp, na 25 mei 2018 de AVG.)

2.2 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 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.

Door het goed toepassen van informatiebeveiliging kan aan de wet- en regelgeving worden voldaan. Vooral het aspect vertrouwelijkheid is hiervoor van belang.
Kijk ook bij Welkom- Basisbegrippen IBP

Een beleid heeft altijd een doel. Wat wil je met het informatiebeveiligings- en privacy beleid bereiken?
Beschrijf de doelen in bewoordingen die bij de organisatie passen.

Als aanvulling op betrokkenen valt ook te denken aan sollicitanten, vrijwilligers en stagiaires.

2.3 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 proces: IBP. Dit beleid, verder te benoemen als IBP-beleid, vormt de basis om informatiebeveiliging en privacy binnen Stichting Ultiem te regelen en vormt de kapstok voor de onderliggende afspraken en procedures.

3 Doel en reikwijdte

3.1 Doel

Informatiebeveiliging en privacy heeft de volgende doelen:

- Het waarborgen van de continuïteit van het onderwijs en de bedrijfsvoering.
- Het garanderen van de privacy van alle betrokkenen waarvan Stichting Ultiem persoonsgegevens verwerkt, waaronder leerlingen, hun ouders/verzorgers en medewerkers
- 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, leerlingen en hun ouders/verzorgers) wordt gerespecteerd en Stichting Ultiem voldoet aan relevante wet- en regelgeving.

3.2 Reikwijdte

Het IBP-beleid binnen Stichting Ultiem geldt voor alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/ outsourcing). Onder dit beleid vallen ook alle devices van waar geautoriseerde toegang tot het schoolnetwerk verkregen kan worden.
Het IBP-beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen Stichting Ultiem waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op overige betrokkenen waarvan Stichting Ultiem persoonsgegevens verwerkt.
Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van Stichting Ultiem Hieronder valt tevens de gecontroleerde informatie, die door de school zelf is gegenereerd en wordt beheerd en de niet-gecontroleerde informatie waarop de school kan worden aangesproken. (b.v. uitspraken van medewerkers en leerlingen in discussies, op (persoonlijke pagina's van) websites en of social media.)
Het IBP-beleid geldt voor de geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens, die plaatsvindt onder de verantwoordelijkheid van Stichting Ultiem 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 Stichting Ultiem raakvlakken met:
Algemeen veiligheids- en toegangsbeveiligingsbeleid; met als aandachtspunten bedrijfshulpverlening, fysieke toegang en beveiliging, crisismanagement, huisvesting en ongevallen
Personeels- en organisatiebeleid; met als aandachtspunten in- en uitstroom van medewerkers, functiewisselingen, functiescheiding en vertrouwensfuncties
IT-beleid; met als aandachtspunten aanschaf, beheer en gebruik van ICT en (digitale) leermiddelen
Medezeggenschap van leerlingen, hun ouders/verzorgers en medewerkers

Waar is het beleid op van toepassing? Want doelen bereik je altijd in een bepaalde omgeving, met een bepaalde groep mensen en middelen.

Daarom is het van belang om de reikwijdte ('scope') duidelijk te beschrijven:

- voor **wie** geldt het beleid,
- **van wie** worden persoonsgegevens verwerkt,
- welke **toepassingen** vallen eronder,
- **welke verwerkingen** zijn erbij betrokken,
- **hoe worden ze verwerkt** en **hoe** zijn de gegevens **verkregen,**
- en waar liggen de **grenzen en raakvlakken** met andere afspraken?

Pas de reikwijdte eventueel aan, zodat inhoud en taalgebruik past bij de organisatie.

Uitleg:
Een **bestand** is onder de AVG **een gestructureerde verzameling persoonsgegevens die via een bepaalde logica toegankelijk is**.

Denk hierbij bijvoorbeeld aan een archiefkast of een geordende verzameling naamkaartjes. Er is ook sprake van de verwerking van persoonsgegevens wanneer deze in een bestand worden opgenomen of bestemd zijn om daarin opgenomen te worden.
Wat losse papieren op een bureau met daarin de namen van personen vormen geen bestand (mits deze niet digitaal opgeslagen zijn)

Beleid is de basis voor het maken van afspraken, werkprocessen en communicatie rondom IBP.
Uitgangspunten vormen de achtergrond op basis waarvan je het beleid uitwerkt. Een simpel uitgangspunt is bijvoorbeeld: "We houden ons aan wet- en regelgeving". Dat lijkt eenvoudig opgeschreven, maar betekent onder andere ook dat er dan geen illegale

4 Beleid- Hoe doen we dat?

Stichting Ultiem hanteert de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging en privacy te bereiken:

1. Het schoolbestuur van Stichting Ultiem neemt de verantwoordelijkheid om ervoor te zorgen dat informatiebeveiliging en privacy geregeld wordt. Het bestuur is hierop aan te spreken en legt hier verantwoording over af. In termen van de wet is het bestuur de verwerkingsverantwoordelijke.
2. Stichting Ultiem voldoet aan alle relevante wet- en regelgeving.
3. Bij Stichting Ultiem is de verwerking van persoonsgegevens altijd gekoppeld aan een specifiek doel en gebaseerd op één van de wettelijke grondslagen. Een goede balans tussen het belang van Stichting Ultiem om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot het gebruik van zijn/haar persoonsgegevens is essentieel. Bij alle verwerkingen van persoonsgegevens op basis van toestemming kunnen betrokkenen ten alle tijden hun toestemming herzien.
4. Stichting Ultiem zal alle betrokkenen helder en actief informeren over de verwerkingen van de hun persoonsgegevens, die zowel direct als indirect zijn verkregen. Ook worden alle betrokkenen gewezen op hun rechten met betrekking tot informatie, inzage, verbetering, het wissen van gegevens, beperking van verwerking, verzet, dataportabiliteit en profilering.
5. Stichting Ultiem legt alle verwerkingen van persoonsgegevens vast in een dataregister en zal deze up-to-date houden. Stichting Ultiem voldoet hiermee aan de documentatieplicht.
6. Binnen Stichting Ultiem is het veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van iedereen. Hierbij hoort niet alleen het actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie, maar ook van papieren documenten.
7. Stichting Ultiem is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert de school informatie, waarvan het eigendom (auteursrecht) toebehoort aan derden. Medewerkers en leerlingen worden goed geïnformeerd over de regelgeving rondom het gebruik van informatie.

software op school aanwezig mag zijn. En dat leerlingen geen films en games mogen downloaden...

Vergeet niet dat de uitgangspunten de basis (kapstok) vormen voor het maken van afspraken, werkprocessen en communicatie rondom IBP. Ze geven antwoord op de vraag Hoe doen we dat?

1. Het beleid vormt de kapstok. Het geeft de haakjes waaraan onderliggende afspraken, protocollen en processen worden opgehangen.
2. De uitgangspunten hebben direct of indirect een link met de AVG en kunnen een rol spelen bij het 'aantoonbaar voldoen aan de AVG'.
3. Zie ook: Basisregels voor het verantwoord omgaan met persoonsgegevens waaronder; doel/doelbinding, grondslag et cetera (zie 5 vuistregels).

4. Dit kan geregeld worden door betrokkenen te informeren d.m.v. privacyreglement en/of een privacy toelichting, communicatie over de rechten betrokkenen en door de privacy bijsluiter(s) van de verwerkersovereenkomst(en) toegankelijk te maken (b.v. via de website).
5. Verwijzing naar het 'Dataregister': Kennisnet komt met 5 registers waaronder voor medewerkers, leerlingen, en externen.
6. Denk hierbij aan: Wachtwoordbeleid, toegangsbeleid (fysiek en digitaal), cleardesk policy, acceptable use policy enz.
7. Leg dit vast in bijv. acceptable use policy en maak medewerkers en leerlingen mediawijsheid en ICT-vaardig.

8. Stichting Ultiem classificeert informatie en informatiesystemen. 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.
9. Stichting Ultiem sluit met alle leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) verwerkersovereenkomsten af als zij, in opdracht van de school, persoonsgegevens verwerken. Dit geldt ook voor andere organisaties indien er gegevens van leerlingen of medewerkers worden verstrekt.
10. Stichting Ultiem verwacht van alle medewerkers, leerlingen, (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. Stichting Ultiem heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.
11. Informatiebeveiliging en privacy is bij Stichting Ultiem een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.
12. Stichting Ultiem kijkt bij wijzigingen 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.
13. Stichting Ultiem neemt passende 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.
14. Stichting Ultiem zal alle beveiligingsincidenten vastleggen en datalekken volgens een vast protocol afhandelen en melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen.

8. Informatie heeft een waarde: financieel, economisch maar zeker ook emotioneel. Maak risico's daarom inzichtelijk d.m.v.: Classificatie en risicoanalyse.
   Hieruit volgen de bijbehorende (technische en organisatorische) maatregelen zoals autorisatiematrix, back-up enz.
9. Maak hiervoor gebruik van de meest recente versie van het convenant 'Digitale leermiddelen privacy' (www.privacyconvenant.nl) en de bijbehorende model verwerkersovereenkomst.
   Zie ook Checklist gebruik digitale onderwijsmiddelen en checklist afspraken leveranciers in de Aanpak
10. Leg dit vast in bv. Gedragscode ICT en internetgebruik/ acceptable use policy afspraken sociale media, wachtwoordbeleid, Responsible disclosure
11. Door evalueren en verbeteren (PDCA-cyclus), hierbij kan ingespeeld worden op actuele ontwikkelingen en eventuele daaruit voortkomende aanpassingen.
12. (D)PIA (data protection impact assessment) en privacy by design spelen hier een rol.
13. Technische maatregelen(informatiebeveiliging) Persoonsgegevens moeten beveiligd worden volgens de geldende beveiligingsnormen (ISO 27001/27002). Dit houdt in dat organisaties moeten gebruiken om persoonsgegevens te beschermen.
    LET OP: hou hier ook rekening mee als het ICT beheer
14. Maak een protocol datalekken in kader van meldplicht datalekken en zorg ervoor dat alle incidenten geregistreerd kunnen worden

5 Uitwerking van het beleid – Wat doen we?

Dit hoofdstuk geeft een praktische invulling van bovenstaande beleidspunten en is daarmee de minimale invulling van het beleid.

5.1 Relevante wet- en regelgeving

De uitwerking van het beleid voldoet aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder:

- Wet op het primair onderwijs en/of Wet voortgezet onderwijs en/of Wet op de expertisecentra
- Wet goed onderwijs en goed bestuur PO/VO
- Wet onderwijstoezicht
- Wet bescherming persoonsgegevens (Wbp; tot 25 mei 2018)
- Algemene Verordening Gegevensbescherming (AVG; vanaf 25 mei 2018) *
- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht

De internationale norm voor informatiebeveiliging NEN-ISO/IEC 27001 en 27002 (2015) is leidend voor de te nemen beveiligingsmaatregelen. Daarnaast wordt ook gebruik gemaakt van in het onderwijs toegepaste standaarden. (bijvoorbeeld de ROSA katern IBP).
De bepalingen van de meest recente versie van het convenant 'Digitale onderwijsmiddelen en privacy' zijn leidend bij het maken van afspraken met leveranciers, die in opdracht van de verwerkingsverantwoordelijke persoonsgegevens verwerken.

5.1: Een school leeft niet alleen privacywetgeving na, maar ook andere wetgeving. Eigen protocollen en richtlijnen spelen ook een rol in het kader van de uitwerking van IBP.

Benoem deze wet- en regelgeving ook in het IBP-beleid.

Benoem ook de internationale norm voor informatiebeveiliging. (NEN-ISO/IEC 27001 en 27002 (2015))

Op termijn wordt de Aanpak aangevuld met praktische beveiligingsmaatregelen.
* organisaties moeten niet alleen de AVG naleven, maar hier ook aantoonbaar voldoen.

Uiteindelijk is er dan maar één regel, die elke medewerker moet onthouden: 'je moet het IBP-beleid en de regels die daaruit voortvloeien nakomen'

5.2 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. 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.
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,

5.2: Artikel 5 van de Algemene Verordening Gegevensbescherming geeft basisuitgangspunten rondom **verwerking van persoonsgegevens** aan.
Ook hier geldt dat deze eisen het haakje vormen waar afspraken, protocollen en procedures aan gekoppeld moeten (kunnen) worden.
LET OP: *De AVG eist dat organisaties aantoonbaar moeten voldoen aan de AVG. Zij moeten kunnen laten zien welke maatregelen zij genomen hebben*. Bijvoorbeeld door:
Ad 1: documentatieplicht, dataregister

Ad 2: waar nodig toestemming regelen: toestemmingsformulier; beeldmateriaal en gebruik social media in de les onder de 16 jaar.
Ad 3: privacy by design, verzamel niet meer dan nodig, verwijder gegevens tijdig (bewaartermijnen!)

alternatieve of andere gegevens worden bereikt (subsidiair). Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk.

4. Transparantie: de school legt aan betrokkenen (leerlingen, hun ouders en medewerkers) op transparante wijze verantwoording af over het gebruik van hun persoonsgegevens, alsmede over het gevoerde IBP-beleid. Deze informatievoorziening vindt ongevraagd plaats. Daarnaast hebben betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming 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 juist en actueel zijn.

Ad 4: communicatie naar alle betrokkenen (informatieplicht) over: procedure rechten betrokkenen, dataregister, privacyreglement, privacy bijsluiter verwerkersovereenkomst, cameratoezicht

Ad 5: controle en logging, toegangsmatrix, informatiebeveiliging

5.3 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 de diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen. Daarnaast worden alle verwerkingen van persoonsgegevens vastgelegd en up-to-date gehouden in een dataregister.

5.3: Als aanvulling bij uitwerking beleid is een niet limitatieve opsomming in bijlage 1 opgenomen. Eventuele wijzigingen zijn dan eenvoudig in de bijlage bij te werken. Pas de situatie van de onderwijsorganisatie.

5.4 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 verantwoordelijke IBP, de FG en de Privacy Officer met het bestuur als eindverantwoordelijke.

5.4: Bewustzijn creëren en voorlichten is één van de eisen en aandachtpunten vanuit de AVG. Dit geldt voor zowel de huidige als de nieuwe medewerkers en leerlingen (en ouders).
Denk hierbij aan:

- de mogelijkheid om IBP-onderdeel van de gesprekscyclus te laten zijn.
- Het benoemen van mensen die hiervoor verantwoordelijk zijn.
- Communicatiemedewerkers, bewustwording; Acceptabel use policy, gedragscode ICT en internetgebruik

5.5 Classificatie en risicoanalyse

Alle informatie heeft waarde, daarom worden alle gegevens en informatiesystemen waarop dit beleid van toepassing is, 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 betrouwbaarheidsaspecten die van belang zijn.

5.5: Alle informatie heeft een waarde, maar hoe groot is die waarde? En welke gegevens gebruiken we eigenlijk in welke systemen? Tot welke hoogte moet de informatie beveiligd worden? Daarom is het nodig om informatie en – systemen te classificeren.

- Verplichte risicoanalyse en PIA vanuit de AVG
- Classificatie komt ook terug in het dataregister.

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. Vanaf de start van nieuwe (ICT)projecten wordt rekening gehouden met informatiebeveiliging en privacy.

5.6 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 fg@ultiemonderwijs.nl.
Periodiek zullen de beveiligingsincidenten besproken worden en waar nodig aanvullende passende beleidsmaatregelen genomen worden.

5.6: Procedure melden datalekken; **Let op** dat de beschreven taken en rollen bij '**organisatie'** ook hier gebruikt worden. Zorg ervoor dat het voor iedereen duidelijk is waar (beveiligings)incidenten gemeld kunnen worden.
Registreer alle beveiligingsincidenten. Niet alle incidenten hoeven gemeld te worden bij de AP, maar moeten wel allemaal worden vastgelegd (aantoonbaarheid). **Denk hierbij aan:** FG benoemen, procedure melden datalekken, register beveiligingsincidenten.

5.7 Planning en controle

Dit IBP-beleid 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 actuele geïnventariseerde risico's;
- de effectiviteit van de genomen maatregelen en aantoonbare werking daarvan.

Daarnaast kent Stichting Ultiem een jaarlijkse planning en control cyclus voor informatiebeveiliging en privacy. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het informatiebeveiligings- en privacy beleid wordt getoetst. Tevens worden hier eventuele actuele ontwikkelingen op het gebied van techniek, wet- en regelgeving et cetera meegenomen.

5.7: Als je wilt kunnen zeggen dat je IBP onder controle hebt, dan moet je dat kunnen aantonen. Zorg dat je duidelijke processtappen hebt en dat er een continu verbetertraject aanwezig is. Neem aanpassingen en verbeteringen mee in een PDCA-**cyclus**. Dit kan aansluiten bij een bestaande PDCA-cyclus. Doe dit jaarlijks.
Ook kunnen ontwikkelingen zoals nieuwe processen of nieuwe systemen vragen om aanpassingen van het beleid.

5.8 Naleving en sancties

Voor toezicht op de naleving van de AVG vervult de Functionaris voor Gegevensbescherming (FG) een belangrijke rol. De FG wordt aangesteld door, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FG werkt via een door het vast te stellen reglement.

5.8: verwijzing naar: Beleidsterreinen, bewustwording; Acceptabel use policy, gedragscode ICT en internetgebruik
Procedure melden datalekken, register beveiligingsincidenten

Mocht de naleving van dit beleid ernstig tekortschieten, dan kan Stichting Ultiem de betrokken verantwoordelijke medewerkers een sanctie op leggen binnen de kaders van de CAO en de wettelijke mogelijkheden

5.9 Logging en monitoring

Logging en monitoring door de IT-afdeling zorgt ervoor dat gebeurtenissen met betrekking tot geautomatiseerde systemen en toegang tot gegevens wordt vastgelegd. Hieronder vallen onder andere het in- uitloggen van gebruikers en (poging) tot ongeautoriseerde toegang tot het netwerk.

5.9: Hiermee kunnen beveiligingsincidenten worden gedetecteerd, afgehandeld en gerapporteerd

6. Organisatie- wie doet wat?

6.1 Rollen en verantwoordelijkheden

De organisatie van IBP gaat over processen, gewoontes, beleid, wetten en regels die van betekenis zijn voor de manier waarop mensen een organisatie sturen, besturen, beheren en controleren. Hierbij spelen de relaties tussen de verschillende betrokkenen en de te bereiken doelen een rol.
In tabelvorm is weergegeven wie, welke verantwoordelijkheden en taken heeft bij Stichting Ultiem.

Ondanks dat iedere school anders georganiseerd is, kom je veelal dezelfde functies, rollen en taken tegen. Dat geldt ook rondom het organiseren van IBP.
Omschrijf rollen en taken zo specifiek mogelijk.
Bedenk:

- Wie gaat er verantwoordelijk zijn voor een bepaalde taak
- Waar gaat het precies over (afspraken, processen, dagelijks werk)
- Welke documenten ondersteunen het. Hoe maak je het aantoonbaar

Bijlage 1: Ondersteunende richtlijnen en procedures

Geef hier de afspraken en documenten aan, die in de organisatie aanwezig zijn.

Deze bijlage bevat een aantal aanvullende beleidsstukken, richtlijnen, procedures en protocollen. Een aantal zijn vanuit de Algemene Verordening Gegevensbescherming verplicht.

Documenten:	**Aandachtspunten**:
Procedure toestemming gebruik beeldmateriaal	(Toestemmingsbrief)
Procedure voor verwijderen van gegevens	(bewaartermijnen)
Communicatierechten betrokkenen	(communicatie richting betrokkenen)
Procesbeschrijving rechten gen	proces rondom aanvra- gen van betrokkenen)
Privacyreglement	
Autorisatiematrix	(wie mogen gegevens in zien, bewerken enz.)
Afspraken gebruik sociale media	(bewustzijn creëren)
Procedure rondom training mede-werkers	
Cameratoezicht	
Wachtwoordbeleid	
Responsible disclosure	
Gedragscode ICT en internetgebruik	
Acceptable use policy	(verantwoord gebruik bedrijfsmiddelen)
Procedure rondom uitwisselen gegevens	(passend onderwijs, leerling dossiers, leerplicht enz.)

Verplicht vanuit de AVG:

Procesbeschrijving melden datalekken
Registratie beveiligingsincidenten
Dataregister om te voldoen aan de registratieplicht
Verwerkersovereenkomsten
(privacy bijlage beschikbaar stellen)
Procedure gegevensbeschermingseffectbeoordeling (DPIA)
Risicoanalyse
Functionaris voor Gegevensbescherming
(communicatie hierover richting medewerkers)

Bijlage 2: Rollen en verantwoordelijkheden

Deze bijlage beschrijft hoe IBP op drie niveaus wordt georganiseerd

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

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

Richtinggevend

Bestuurder
De bestuurder is eindverantwoordelijk voor IBP en stelt het beleid en de basismaatregelen op het gebied van informatiebeveiliging en privacy vast.
De toepassing en werking van het IBP-beleid wordt op basis van regelmatige rapportages geëvalueerd. De inhoudelijke verantwoordelijkheid voor IBP is gemandateerd aan de manager IBP.

Beleidsmatig

Werkgroep IBP
Werkgroep IBP heeft een rol op sturend niveau. Hij/zij geeft terugkoppeling en advies aan de eindverantwoordelijke (het bestuur) en stuurt de mensen aan op uitvoerend niveau. De Interne PO moet:

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

Functionaris voor Gegevensbescherming (extern belegd)
De functionaris voor gegevensbescherming (FG) houdt binnen Stichting Ultiem toezicht op de toepassing en naleving van de AVG. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie. De FG zorgt voor het verbeteren en stimuleren van bewust-

Ondanks dat iedere school anders georganiseerd is, kom je veelal dezelfde functies, rollen en taken tegen. Dat geldt ook voor het organiseren van IBP. Omschrijf rollen en taken zo specifiek mogelijk.
Bedenk:

- Wie gaat er verantwoordelijk zijn voor bepaalde taak
- Waar gaat het precies over (afspraken, processen, dagelijks werk)
- Welke documenten ondersteunen het. Hoe maak je het aantoonbaar

Het gaat hier niet om dat er extra rollen en/of functies gemaakt moeten worden, maar kijk wie op jouw school die taken kan vervullen. Ook kan één persoon prima meerdere rollen vervullen.
Let daarbij op dat de rollen niet conflicteren met andere verantwoordelijkheden.

Het schoolbestuur is eindverantwoordelijk, Kies voor de rest van dit hoofdstuk de juiste benaming op de plaats van 'eindverantwoordelijke', zodat deze van toepassing is op de eigen organisatie en voer deze consequent in het beleid door.

Werkgroep IBP adviseert o.a. het de bestuurder. De werkgroep bewaakt de uniformiteit binnen het schoolbestuur. Wie plaats neemt in de werkgroep krijgt hangt ook af van de grootte van de organisatie.

wording rondom IBP, het afhandelen van informatiebeveiligingsincidenten, adviseert over het regelen van privacy, onderhoudt zo nodig de contacten met de Autoriteit Persoonsgegevens (AP) en rapporteert aan de eindverantwoordelijke (het bestuur). De FG heeft regelmatig overleg met manager IBP. De FG is meestal ook de contactpersoon voor klachten en vragen van betrokkenen.

Beleidsterrein
Binnen de school zijn er verschillende domeinen/processen, zoals ICT, P&O, F&H, O&K en de verantwoordelijke op de scholen (directeuren). Op elk van deze domeinen/processen is iemand verantwoordelijk om te bepalen op welke wijze IBP daarbinnen wordt vormgegeven in richtlijnen, procedures en instructies.

Deze proceseigenaar is tevens verantwoordelijk voor de risico's die veroorzaakt worden doordat personen of applicaties ten onrechte toegang krijgen tot applicaties. Om deze risico's te verkleinen hebben proceseigenaren de volgende specifieke taken:

- Samen met de bestuurder stellen zij het beleid voor toegang (autorisaties) vast.
- Samen met BICT zien zij erop toe dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn voor hun werkzaamheden toegang toe moeten hebben.
- Samen met BICT beoordelen zij periodiek de toegangsrechten van en verleende toegang aan gebruikers.

Uitvoerend

Werkgroep IBP
De werkgroep IBP vormt een technisch aanspreekpunt inzake informatiebeveiliging voor het management en de medewerkers.

BICT
Ieder softwarepakket of (web-)applicatie heeft een beheerder. Bij vragen over die software of applicatie is bekend wie daarvoor aangesproken kan worden. De functioneel beheerder wordt vanuit het beleidsterrein voorzien van een ingevuld werkpakket, bestaande uit richtlijnen, procedures en instructies. Op basis hiervan voert hij zijn of haar taken uit.

Medewerkers

Werkgroep IBP is het technisch aanspreekpunt als gaat om het oplossen en uitzoeken van beveiligingsincidenten (in samenwerking met de FG).

LET OP: Als de school het ICT-beheer elders heeft ondergebracht (bv bij outsourcing), dan moeten er afspraken gemaakt worden over waar welke verantwoordelijkheden en taken liggen

BICT voert toegangsrechten, instellingen en procedures door zoals aangegeven zijn in de goedgekeurde richtlijnen.

Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging en privacy in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in o.a. het Kwaliteitshandboek en de handleiding acceptabel gebruikmaken van bedrijfsmiddelen. Daarnaast worden medewerkers in hun dagelijkse werkzaamheden, waar nodig, ondersteund met checklists en formulieren.

Informatiebeveiliging en privacy is de verantwoordelijkheid van ieder individu, elke **medewerker**.

Medewerkers worden 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 MR)

Leidinggevende
Naleving van het informatiebeveiligingsbeleid is onderdeel van de integrale bedrijfsvoering.

Leidinggevende heeft o.a. de volgende taken: Communiceren, informeren en toezien op naleving van de gemaakte afspraken en procedures.

Iedere leidinggevende heeft op uitvoerend niveau 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 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. Leidinggevenden hebben hierbij een voorbeeldrol ten opzichte van hun medewerkers

Werkgroep IBP
De werkgroep IBP wordt organisatie breed zowel preventief als curatief benoemd voor informatiebeveiliging en privacy incidenten. De leden van de werkgroep IBP zijn benoemd door de bestuurder en handelen in diens opdracht.

De werkgroep IBP van Stichting Ultiem heeft de volgende opdracht:

- Het signaleren en registreren van alle privacy verzoeken, beveiligingsincidenten en datalekken. Het coördineren van de maatregelen en het toezien op de oplossing van problemen die tot incidenten hebben geleid of waardoor de incidenten zijn veroorzaakt (of het bieden van ondersteuning daarbij);
- Het geven van voorlichting en het doen van algemene aanbevelingen aan netwerkbeheerders, systeembeheer-

ders, ontwikkelaars en eindgebruikers door het verspreiden van informatie;
- Het leveren van managementrapportages aan beleidsterreinen over de beveiligingsincidenten en verzoeken tot uitoefening privacy rechten van de betrokkenen.

Bij een calamiteit kan de werkgroep IBP terstond bij elkaar worden geroepen op initiatief van de FG, in opdracht van Stichting Ultiem. Het doel hiervan is om de continuïteit van de informatievoorziening en de privacy te waarborgen. Onder calamiteiten worden verstaan:
- Datalek;
- Grote verstoringen van het netwerk (bijvoorbeeld DDoS aanval);
- Natuurrampen (brand, overstroming, storm, etc.).

De werkgroep IBP bij Stichting Ultiem 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 werkzaamheden van de werkgroep IBP bij Stichting Ultiem is gedocumenteerd en door de eindverantwoordelijke bekrachtigd.
De rol van werkgroep coördinator wordt belegd bij de FG.