Informatiebeveiligings- en Privacybeleid 2024

ROC van Amsterdam-Flevoland

Uitgave	: Informatiebeveiligings- en Privacybeleid 2024
Auteur	: Information Security Officer (ISO), Dienst OI&I
Kenmerk	: Informatiebeveiligings- en privacybeleid 2024 (240603)
Vastgesteld door RvB op	: 3 juni 2024
Traject OR ROCvA-F	: ter informatie (4 juni 2024)
Traject CSR ROCvA-F	: n.v.t.
Traject GMR VOvA	: n.v.t.

Voorwoord

Alle onderdelen van onze organisatie zijn voor hun prestaties en continuïteit afhankelijk van het voortdurend betrouwbaar functioneren van een groot aantal voorzieningen voor het verwerken van informatie. Een ongestoorde voortgang van de werkzaamheden is van essentieel belang bij het vervullen van de wettelijke taken en het behalen van de organisatiedoelstellingen. Daarvoor moet informatie tijdig, correct en volledig op de juiste plek beschikbaar zijn. Met de zekerheid dat alleen degenen die daartoe zijn geautoriseerd toegang hebben tot vertrouwelijke informatie, waaronder privacy gevoelige gegevens. Robuuste, betrouwbare informatieverwerking is ook belangrijk voor het imago.

Informatiebeveiliging is een combinatie van weloverwogen organisatorische en technische beveiligingsmaatregelen en het bewust handelen van medewerkers. Informatiebeveiliging en het beleid daaromtrent zijn zonder uitzondering van toepassing op alle onderdelen van de organisatie. Het is een onderdeel van de kwaliteitszorg voor gegevensverwerkende processen (ook niet geautomatiseerde) en de daarbij gebruikte informatiesystemen. Bovendien geldt informatiebeveiliging voor het *gehele* proces van informatievoorziening en de *gehele* levenscyclus van informatiesystemen, ongeacht het karakter van de informatie en de toegepaste technologie. Tenslotte heeft informatiebeveiliging ook betrekking op het uitwisselen van informatie met de organisaties waar we mee samenwerken.

Deze beleidsnota bevat het strategische deel van het informatiebeveiligings- en privacybeleid. Het beschrijft toegesneden op onze organisatie onder meer de kaders, uitgangspunten, de wijze waarop we onze informatiebeveiliging beheersen en de organisatorische borging. Deze versie van het beleid is met ingang van 1 juli 2024 van kracht.

Een goede uitvoering van beveiligingsmaatregelen is niet van de ene op de andere dag gerealiseerd en vraagt blijvend aandacht van iedereen die binnen de organisatie met informatie werkt van medewerker tot en met de Raad van Bestuur (RvB). We kunnen het vereiste betrouwbaarheidsniveau alleen bereiken als iedereen haar/zijn steentje bijdraagt en de eigen verantwoordelijkheid op dit gebied serieus neemt.

En dus is het belangrijk dat iedere vaste en tijdelijke medewerker, ingehuurde medewerker, vrijwilliger, stagiair en externe gebruiker op de hoogte is van beleid, afspraken en regels die specifiek op hem/haar van toepassing zijn. En deze ook naleeft. Alleen dan is de betrouwbaarheid van de informatie en informatievoorziening, die nodig is voor de continuïteit van onze werkprocessen en activiteiten, gewaarborgd. Hierbij gaat het om het niveau dat wij onszelf opleggen en dat anderen van ons mogen verwachten.

Edo de Jaeger
Voorzitter RvB

Inhoudsopgave

1. Inleiding

Deze beleidsnota bevat het strategische deel van het informatiebeveiligingsbeleid. Het beschrijft toegesneden op ROC van Amsterdam-Flevoland (verder: “de organisatie”) onder meer de kaders, uitgangspunten, de wijze van realisatie en governance en maatregelen (op hoofdlijnen). Tactische en operationele maatregelen, richtlijnen, (gedrags)regels, procedures, protocollen, etc. zijn elders – voor zover zinvol –in detail vastgelegd.

1.1. Het belang van een Informatiebeveiliging & 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 steeds groter wordende afhankelijkheid van ICT en persoonsgegevens brengt nieuwe kwetsbaarheden en risico’s met zich mee. Het goed regelen van informatiebeveiliging en privacy (verder: IBP) in een Informatiebeveiligings- en Privacybeleid (verder: IBP-beleid) is noodzakelijk om de gevolgen van deze risico’s inzichtelijk te maken en tot een aanvaardbaar niveau te reduceren en te monitoren om vervolgens de voortgang van het onderwijs en de bedrijfsvoering optimaal te kunnen waarborgen. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades, boetes en imagoverlies. Ook de sociale veiligheid kan in het geding komen.

1.2. Toelichting Informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket aan maatregelen om de kwaliteitsaspecten beschikbaarheid, integriteit en vertrouwelijkheid (BIV) van informatie en de informatievoorziening te waarborgen:

- 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 beperkt is tot degenen die daartoe bevoegd zijn.

Informatiebeveiliging is een beleidsverantwoordelijkheid van het bestuur van de organisatie.

Privacy

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.

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 [1]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.*

Vervlechting Informatiebeveiliging & Privacy

Uit voorgaande blijkt dat informatiebeveiliging een belangrijke voorwaarde is voor privacy. Informatiebeveiliging en privacy staan naast elkaar en zijn van elkaar afhankelijk, en worden daarom samengevoegd tot één domein: ‘IBP’.

1.3. Onderwerpspecifieke beleidsregels

Het IBP-beleid is kaderstellend voor (formele) beleidsregels en normen met een sturende werking, die specifiek gericht zijn op deelgebieden ('onderwerpen') die een relatie hebben met informatiebeveiliging van gegevens van medewerkers, studenten, leerlingen en bedrijven, zoals (in willekeurige volgorde):

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

- Architectuurprincipes en Cloud.
- Logische toegang tot systemen en (bedrijfs)applicaties (IAM, accounts, authenticatie (MFA/SSO), toegangsrechten, etc.).
- Fysieke toegang tot locaties en ruimtes.
- Systeemontwikkeling en inrichting/configuratie ICT-nieuwbouw.
- Technisch en functioneel beheer.
- Monitoring en logging (SIEM).
- Informatiebeveiligingsincidenten (waaronder datalekken) - Incident Response.
- Technische weerbaarheid.
- ICT continuïteit.
- Inkoop en leveranciersrelaties.
- Informatieveilig werken.
- In-, Door- en Uitstroom van personeel (IDU-proces).
- Classificatie van systemen, applicaties en informatie.
- Cryptografie.
- Toetsing (auditing/pentesting).

Een '(beleids)regel' of 'norm' is een aanvaard beginsel of een aanvaarde instructie waarin de verwachtingen van de organisatie over welke handelingen vereist zijn, wat is toegestaan of niet is toegestaan is beschreven. 'Formeel' wil zeggen dat (beleids)regels zijn vastgesteld en kenbaar gemaakt door het daartoe passende (gemandateerde) managementniveau.

1.4. Herijkt IBP-beleid versie 2024 t.o.v. 2018

Deze beleidsnota vervangt het vastgestelde IBP-beleid uit 2018. Voor het opstellen van dit beleid is gebruikgemaakt van kennis en ervaring(en) van overige instellingen en de Regiegroep IBP mbo.

Ten opzichte van de 2018 versie zijn onderstaande onderwerpen nieuw of geactualiseerd:

- IBP Visie (nieuw).
- IBP Governance (nieuw).
- Realisatie IBP-beleid (geactualiseerd).
- BIV-classificatie en DPIA (nieuw).
- NBA volwassenheidsmodel (nieuw).
- Functionele inpassing IBP (geactualiseerd).
- Verplicht karakter awareness (nieuw).

2. Kaders en uitgangspunten

2.1. Visie

ROCvA-F wil aan haar studenten, leerlingen en medewerkers een veilige en professionele leer- en werkomgeving aanbieden. Daarbij is het noodzakelijk dat de door de organisatie verzamelde, verwerkte en gepubliceerde informatie te allen tijde beschikbaar, correct en beschermd is. Dit vraagt om een strategisch samenhangende aanpak van InformatieVeiligheid, die aantoonbaar aan de eisen voldoet, om blijvend een veilige en toekomstbestendige leer- en werkomgeving beschikbaar te stellen.

Werken aan de veiligheid van informatie is een continu proces dat zich moet aanpassen aan het voortdurend veranderende cyberdreigingslandschap. Onze visie is gebaseerd op de overtuiging dat een effectieve informatiebeveiligingsstrategie preventieve, detectieve en reactieve maatregelen moet omvatten.

Preventie is de eerste stap. Dit betekent het implementeren van sterke technische maatregelen, zoals firewalls en encryptie, maar ook het onderwijzen en trainen van medewerkers om bedreigingen zoals phishing te herkennen en te voorkomen of een ongenode gast te begeleiden naar de juiste persoon binnen de organisatie wanneer niet helder is waarom deze persoon aanwezig is.

Detectie vormt een essentiële schakel in de keten van informatiebeveiliging. Het vermogen om cyberdreigingen en inbreuken tijdig te identificeren, verhoogt de kans om schade te beperken. Vanwege de omvang en de sterkte van de dreigingen zijn we genoodzaakt gebruik te maken van de nieuwste technologieën en methodieken om ongebruikelijk en mogelijk schadelijk gedrag te signaleren. Trainingen zijn nodig om gebruikers[2] van onze digitale wereld bewust te maken van het herkennen van mogelijke cyberdreigingen. Om te kunnen detecteren is het essentieel om te weten wat er in de digitale wereld omgaat.

Reactie is net zo belangrijk als detectie en preventie. In het geval van een incident moeten we snel en effectief reageren om de schade te minimaliseren en te herstellen. Hiervoor is het nodig ons vermogen om te reageren regelmatig op uiteenlopende typen (ernstige) incidenten te testen en trainen.

Kwetsbaarheid en weerbaarheid twee kanten van dezelfde medaille. Kwetsbaarheid verwijst naar de zwakheden die een organisatie blootstellen aan risico's. Deze kwetsbaarheden moeten we identificeren en beoordelen door middel van grondige audits en tests. Daarnaast moeten we ons richten op het vergroten van de weerbaarheid van de organisatie. Weerbaarheid gaat niet alleen om technische maatregelen, maar ook om de houding en het gedrag van de gebruikers. Een opgeleid en bewust team is de meest waardevolle verdediging is tegen cyberdreigingen.

Tot slot is continue verbetering essentieel. We moeten leren van elke ervaring en voortdurend onze strategieën en methoden bijwerken om gelijke tred te houden met nieuwe dreigingen. InformatieVeiligheid is geen einddoel, maar een continu proces van aanpassing en groei. We moeten een cultuur van informatieveiligheid zien te creëren, waarbij elke medewerker begrijpt wat zijn/haar/hen rol is in het beschermen van de organisatie tegen (cyber)dreigingen.

2.2. Ambitie

De organisatie heeft de ambitie om met het onderhavige beleidsdocument IBP 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 wordt opgenomen in een kwaliteits-cyclus (PDCA-cyclus). Deze versie van het IBP-beleid vervangt de eerdere vastgestelde versie uit 2018.

2.3. Doel

De organisatie wil met IBP het volgende bereiken:

- Het waarborgen van de continuïteit van het onderwijs en de bedrijfsvoering.
- Het waarborgen van de privacy van alle betrokkenen van wie de organisatie persoonsgegevens verwerkt[3].

[2] Deze nota verstaat onder 'gebruiker' elk persoon die op enige wijze is verbonden aan de organisatie, voor zijn werk middelen van de organisatie benut (zoals informatie, informatiesystemen en ruimten) en tot dit gebruik is geautoriseerd, zoals vaste en tijdelijke medewerkers, ingehuurd personeel, stagiairs, medewerkers van samenwerkingspartijen, leveranciers, dienstverleners, et cetera.
[3] Zoals studenten, leerlingen, cursisten, ouders/voogden/verzorgers/wettelijke vertegenwoordigers en medewerkers (ook van leveranciers en BPV-organisaties).

- Beveiligings- en privacy-incidenten voorkomen en de eventuele gevolgen hiervan beperken.

Het 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, veiligheid, functionaliteit en gebruikerservaring. Het uitgangspunt is dat de persoonlijke levenssfeer van betrokkenen wordt gerespecteerd en de organisatie voldoet aan relevante wet- en regelgeving.

2.4. Reikwijdte

Het IBP-beleid is van toepassing op de gehele organisatie. Ze is van toepassing op *alle* informatie, voorzieningen en applicaties die de organisatie benut, zowel de middelen die ze in eigen beheer heeft als welke die zijn uitbesteed. Het heeft betrekking op alle (tijdelijke, vaste en ingehuurde) medewerkers, studenten, leerlingen en externe gasten, waaronder uit het bedrijfsleven.

IBP is onderdeel van de kwaliteitszorg (en draagt daardoor ook bij aan de kwaliteitscultuur binnen de meerjarenstrategie) voor de primaire en ondersteunende processen en de daarbij gebruikte informatievoorzieningen, zowel geautomatiseerd als niet-geautomatiseerd, inclusief alle user endpoint devices van de organisatie zelf, maar ook Bring Your Own-devices (BYOD), waarmee geautoriseerde toegang tot de ICT-infrastructuur (inclusief applicaties en data) mogelijk is.

Het IBP-beleid is van kracht voor het *gehele proces van informatievoorziening* en de *gehele levenscyclus* van informatievoorzieningen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie. IBP heeft betrekking op *alle relaties* met derden waar de organisatie mee samenwerkt, waarbij sprake is van het verwerken c.q. uitwisselen van informatie. Tenslotte heeft het betrekking op *alle uitingsvormen* van informatie, alle mogelijke gegevensdragers, alle informatie verwerkende systemen en processen gericht op het beschermen van informatie, en op het *gedrag van mensen*.

2.5. Uitgangspunten

De uitgangspunten voor het IBP-beleid zijn:

1. 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 een integriteitscode is geformuleerd.
2. Het IBP-beleid moet voldoen aan de relevante wet- en regelgeving, in het bijzonder aan de Algemene Verordening Gegevensbescherming (AVG).
3. Een goede balans 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/hun persoonsgegevens.
4. 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. Hiervoor wordt aandacht gevraagd onder meer tijdens de onboarding van nieuwe medewerkers, gebruikersovereenkomst (voor bruikleenmiddelen), medewerker-leidinggevende (‘Goede’) gesprekken, een organisatie-brede integriteitscode en periodieke bewustwordingscampagnes.
5. De beheersing van IBP is een continu proces. Periodieke evaluatie, herijking en bijstelling van IBP-beleid vindt plaats. Technologische en organisatorische ontwikkelingen binnen en buiten de instelling maken het noodzakelijk om periodiek te beoordelen of de organisatie nog wel op de juiste wijze bezig is de veiligheid van informatie en privacy te waarborgen. Interne en externe audits maken het mogelijk de naleving en effectiviteit van het beleid en maatregelen te controleren en evalueren.
6. Bij de aanschaf van een nieuw of (door)ontwikkeling van een informatiesysteem besteedt het verantwoordelijke organisatieonderdeel in alle fasen van het inkoop- of ontwikkelingsproces nadrukkelijk aandacht aan IBP. Ze betrekt daarbij de ISO, Privacy Officer (PO) en/of Functionaris Gegevensbescherming (FG). Projecten, met inbegrip van wijzigingen aan processen en informatiesystemen, houden vanaf de start rekening met IBP. Het is onderdeel van het ontwerp- en opleverproces bij elk project (‘security & privacy by design’). Waar vereist of zinvol voert de organisatie een Data Protection Impact Assessment (DPIA) uit.
7. Voor analyse- en bewakingsdoeleinden en het voldoen aan wet- en regelgeving (zoals AVG) kent de organisatie een geautomatiseerd proces van registreren (‘loggen’) van informatie over menselijke

activiteiten en systeemactiviteiten. Denk hierbij aan het analyseren van storingen en het detecteren, opsporen en oplossen van beveiligingsincidenten, waaronder misbruik en fraude. Afdoende bescherming van de registratie is vereist ter waarborging van beschikbaarheid, integriteit en vertrouwelijkheid.

8. Het beveiligen van informatie en informatiesystemen is geen doel op zich. Maatregelen hebben als doel onacceptabele risico's terug te brengen tot een *acceptabel* niveau. Ze moeten proportioneel zijn voor de processen van de diverse onderdelen van de organisatie. Kosten moeten opwegen tegen (te verwachten) baten.
9. De organisatie bewaakt de doeltreffendheid en kosten van maatregelen en stuurt waar nodig bij;
10. Informatiebeveiliging is afdoende geborgd binnen de organisatie, waarbij de rollen en verantwoordelijkheden – waar noodzakelijk – op een adequate, eenduidige en toereikende wijze zijn beschreven en belegd.
11. Er is voldoende capaciteit en expertise beschikbaar om conform het IBP-beleid en daaruit voortvloeiende maatregelen invulling te kunnen geven aan IBP.
12. Slechts uitsluitend in het geval van onaanvaardbare veiligheidsrisico's (of een vergelijkbare zakelijk gegronde reden) en hij[4] dit schriftelijk documenteert, geeft de RvB daartoe bevoegde leidinggevenden of medewerkers ruimte om af te wijken van vastgesteld beleid ('pas toe of leg uit');
13. Belangrijke processen, bedrijfsmiddelen[5] en verwerkingen van persoonsgegevens hebben een Eigenaar[6].
14. Indien mogelijk en waar wenselijk / van toegevoegde waarde classificeert de organisatie haar informatiesystemen, informatie en gegevensverzamelingen naar de aspecten Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV).
15. Bij het aangaan van een samenwerkingsverband met een externe partij, waarbij sprake is van verwerking van informatie (incl. persoonsgegevens), besteedt de verantwoordelijke Eigenaar nadrukkelijk aandacht aan informatiebeveiliging. *Voorafgaand* aan de uitvoering van de samenwerking legt hij de afspraken hierover schriftelijk vast in een overeenkomst en - indien van toepassing - een verwerkersovereenkomst. Tijdens de samenwerking ziet hij toe op de naleving van de gemaakte afspraken;
16. Zodra de organisatie weet heeft van een kwetsbaarheid in een van haar informatiesystemen handelt ze met gepaste prioriteit, om te beletten dat het risico dat ermee gemoeid is zich te lang voordoet.

2.6. Privacy principes

Voor het verwerken van persoonsgegevens door de organisatie zijn de volgende privacy principes van kracht:

1. De verwerking van persoonsgegevens is gebaseerd op een van de wettelijke grondslagen zoals genoemd de Algemene Verordening Gegevensbescherming.
2. Persoonsgegevens worden alleen verwerkt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking geformuleerd.
3. 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 voor het bereiken van het doel noodzakelijk (dataminimalisatie) is.
4. Verwerking van persoonsgegevens gebeurt op de minst ingrijpende wijze en dient in redelijke verhouding te staan tot het beoogde doeleinde.
5. Maatregelen worden getroffen om zoveel mogelijk te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn.
6. Persoonsgegevens worden adequaat beveiligd volgens de geldende beveiligingsnormen. Voor het veilig verwerken van data zijn instructies beschikbaar zoals voor het veilig versturen van e-mail en veilig gebruik van wachtwoorden.
7. Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.
8. Persoonsgegevens worden niet langer verwerkt dan noodzakelijk is voor de doeleinden van de Verwerking. Hierbij worden de van toepassing zijnde wettelijke en contractuele bewaar- en vernietigingstermijnen in

[4] Voor de leesbaarheid hanteert de beleidsnota de term 'hij' en kan ook 'zij', 'hen', etc. worden gelezen.
[5] Denk hierbij aan middelen die baat hebben bij eigenaarschap, zoals (bedrijfs)applicaties, ruimtes, gegevensverzamelingen, contracten/overeenkomsten en andere specifieke documenten.
[6] Een 'Eigenaar' is een identificeerbaar, aangewezen persoon binnen de organisatie die een *specifieke rol* vervult ten aanzien van het benoemde bedrijfsmiddel (proces, applicatie, systeem, gegevensverzameling, overeenkomst, etc.). Eigenaarschap is hierbij niet in juridische zin bedoeld en ligt veelal bij de (verantwoordelijke) leidinggevende van een afdeling of team.

acht genomen. Hierover worden met dienstverleners/leveranciers in de Verwerkersovereenkomst afspraken gemaakt.
9. Iedere betrokkene heeft het recht te verzoeken om inzage, verbetering, aanvulling, verwijdering en overdraagbaarheid van zijn persoonsgegevens alsmede het recht om bezwaar te maken tegen de verwerking.
10. Studenten en leerlingen onder 16 jaar worden door de ouders/voogden/verzorgers/wettelijke vertegenwoordigers vertegenwoordigd in het kader van privacy.
11. 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.
12. Een FG is aangesteld om regelmatige observatie en toetsing uit te voeren.

2.7. Geldigheid, borging en bijstelling

Het Informatiebeveiligings- en Privacybeleid 2024 is goedgekeurd en vastgesteld door de RvB. Het IBP-beleid is geclassificeerd als ‘Intern’ en in eerste instantie gericht op leidinggevenden en medewerkers met een specifieke rol in de beveiligingsorganisatie van de organisatie.

Het IBP-beleid wordt kenbaar gemaakt aan alle leidinggevenden en is via het Intranet voor alle medewerkers beschikbaar. Het beheer van het IBP-beleid is belegd bij de ISO.

Het IBP-beleid en de daaruit voortvloeiende maatregelen worden iedere twee jaar geëvalueerd en – indien nodig – bijgesteld, om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is. Daarnaast vindt tussentijdse bijstelling plaats als daartoe specifiek aanleiding is, zoals bij wijziging van wet- en regelgeving, gehanteerde normen, organisatorische veranderingen, ontwikkelingen in technologie, et cetera. De ISO legt nieuwe versies opnieuw ter vaststelling voor aan de RvB.

3. Realisatie IBP-beleid

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

Functionele inpassing

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

Raad van Bestuur (RvB)

De RvB is eindverantwoordelijk voor de opzet, bestaan en werking van informatiebeveiliging en privacy binnen de organisatie. De RvB stelt het beleid en de basismaatregelen op het gebied van IBP vast en draagt deze uit. De RvB faciliteert IBP door richting te geven, toont betrokkenheid en kent taken, verantwoordelijkheden en bevoegdheden toe op het gebied van IBP.

Portefeuillehouder IBP

De RvB portefeuillehouder van de centrale dienst OI&I is aanspreekpunt voor aangelegenheden op het gebied van IBP op bestuurs- cq. directieniveau.

Chief Information Security Officer (CISO)

De CISO definieert de informatiebeveiligingsstrategie, gebaseerd op een risicomanagementbenadering en rekening houdend met het informatiebeveiligingsdreigingenbeeld, trends en organisatiebehoefte. Richt de informatiebeveiligingsorganisatie in, bepaalt de daarvoor benodigde middelen en wijst deze toe. Initieert en coördineert de implementatie van informatiebeveiliging voor de gehele organisatie en houdt daar toezicht op. Zorgt voor een geschikt niveau van informatiebeveiliging en informatiebeveiligingsgedrag in de organisatie, gebaseerd op de behoeften en de risicobereidheid van de organisatie. De rol CISO is belegd bij de directeur centrale dienst OI&I.

Information Security Officer (ISO)

De Information Security Officer (ISO) is een identificeerbaar persoon en acteert op strategisch en tactisch niveau. De ISO adviseert samen met de Directeur OI&I aan de RvB. De ISO bewaakt de uniformiteit binnen de organisatie en formuleert het IBP-beleid. De ISO heeft de opdracht om voor de gehele organisatie zorg te dragen voor een volwassen IBP. De ISO-functie is belegd bij de centrale dienst OI&I.

Functionaris Gegevensbescherming (FG)

De Functionaris voor gegevensbescherming (FG) houdt binnen de organisatie toezicht op de toepassing en naleving van de Algemene Verordening Gegevensbescherming (AVG). De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie. De FG wordt aangesteld door de RvB en heeft een wettelijk omschreven onafhankelijke toezichthoudende taak. Deze functie is belegd bij afdeling Internal Audit, maar heeft een directe rapportagelijn naar de RvB portefeuillehouder van de afdeling Internal Audit.

Privacy Officer (PO)

De Privacy Officer (PO) is vraagbaak binnen de organisatie voor AVG en privacy-aangelegenheden. De PO beoordeelt wat volgens wet- en regelgeving nodig is als het gaat om privacy en geeft hiervoor handvatten aan de organisatie. De PO werkt hierbij nauw samen met de ISO en FG. De PO-rol is belegd bij een privacy jurist van de afdeling Juridische Zaken (onderdeel Bestuursdienst).

Medewerkers/gebruikers[7] (incl. leidinggevenden)

Medewerkers gaan op een verantwoorde, veilige wijze om met informatie en systemen en houden zich aan de integriteitscode van de organisatie. Op individueel niveau is elke medewerker gehouden mee te werken aan en verantwoordelijk voor een effectieve veiligheid van alle aan hen toevertrouwde middelen van de organisatie. Ook verwacht de organisatie van alle medewerkers dat zij beveiligingsincidenten (incl. informatiebeveiligingsincidenten en datalekken) direct melden conform de meldingsprocedure.

[7] Deze beleidsnota verstaat onder ‘gebruiker’ elk persoon die op enige wijze is verbonden aan de organisatie, voor zijn/haar werk middelen van de organisatie benut (zoals informatie, informatiesystemen en ruimten) en tot dit gebruik is geautoriseerd, zoals vaste en tijdelijke medewerkers, ingehuurd personeel, stagiairs, medewerkers van samenwerkingspartijen, leveranciers, dienstverleners, et cetera.

Leidinggevenden (directeuren, managers, coördinatoren, teamleiders, etc.)

Naleving van het IBP-beleid is onderdeel van de integrale bedrijfsvoering en integraal leidinggeven. Leidinggevenden dragen het vastgestelde beleid uit en zijn verantwoordelijk voor de omgang van hun medewerkers met informatie en informatiesystemen. Iedere leidinggevende heeft de taak om:

- Toe te zien op de naleving van het IBP-beleid door zijn medewerkers.
- Periodiek de onderwerpen informatiebeveiliging en privacy onder de aandacht te brengen in werkoverleggen.
- Als aanspreekpunt beschikbaar te zijn voor alle personeel gerelateerde IBP-zaken. De ISO, PO en FG kunnen hierin leidinggevenden ondersteunen.
- Medewerkers te scholen op het gebied van IBP.
- Onrechtmatigheden te signaleren.

Proceseigenaar

Een proceseigenaar is een identificeerbaar persoon binnen de organisatie die verantwoordelijk is voor één van de onderwijsondersteunende processen en bedrijfsvoeringsprocessen, zoals Inkoop en HRM.

Dataeigenaar

Een dataeigenaar is een identificeerbaar persoon binnen de organisatie die in het kader van IBP verantwoordelijk is voor één of meer verwerkingen van persoonsgegevens, met name wat betreft het voldoen aan de AVG, zie ook Paragraaf 4.4.

Applicatie-eigenaar

Een applicatie-eigenaar is een Identificeerbaar persoon binnen de organisatie die ervoor verantwoordelijk is dat een applicatie blijvend 1) een goede ondersteuning biedt aan het proces c.q. de processen en de gebruikers waarvoor deze bedoeld is en 2) voldoet aan wet- en regelgeving en toepasselijke beveiligingseisen en -normen.

Security manager

De security manager adviseert over en coördineert specifieke informatiebeveiligingsmaatregelen in projecten en in de lijn en bewaakt de consistentie van de maatregelen. Hij doet verbetervoorstellen voor de beveiliging van ICT, ontwerpt ICT-beveiligingsrichtlijnen en ziet toe op technische naleving. Is vraagbaak voor technische ICT-beveiligingsoplossingen en –maatregelen. Deze rol is belegd binnen de centrale dienst OI&I. Deze rol stemt af met de verschillende aanspreekpunten van de betrokken afdelingen van de centrale diensten.

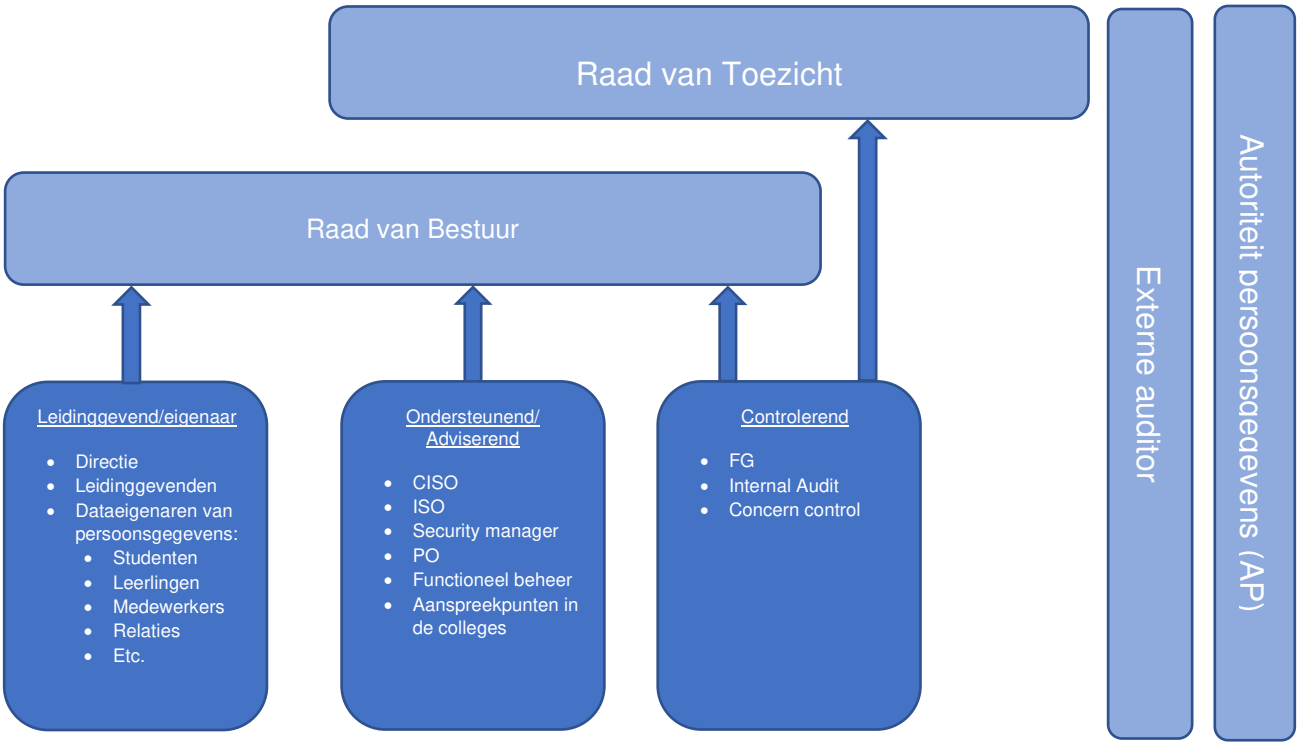
Internal Audit (IA)

De afdeling Internal Audit (IA) voert in afstemming met de FG en ISO, als onderdeel van hun toezichthoudende taak, audits uit gericht op (deelgebieden van) IBP. Ze controleert daarbij op opzet, bestaan en/of werking van een selectie van processen c.q. (beheers)maatregelen en rapporteert de bevindingen aan de RvB Portefeuillehouder van de afdeling Internal Audit, FG en CISO.

4. IBP Governance

De organisatie van IBP gaat over beleid, processen, gewoontes, wetten en regels die van betekenis zijn voor de manier waarop mensen een organisatie sturen, besturen, beheren en controleren. Hierbij spelen de relaties tussen de verschillende betrokkenen en de doelen van de organisatie een rol. Wil IBP optimaal functioneren, dan moet dit goed ingeregeld zijn: de governance moet op orde zijn.

De organisatie hanteert bij de IBP-governance een model waarbij een drietal 'functies' worden onderscheiden: leidinggevend/eigenaar (eerste lijn), ondersteunend/adviserend (tweede lijn) en controlerend (derde lijn). Schematisch ziet dit er als volgt uit:



De eerste lijn (leidinggevend) binnen dit model is cruciaal, immers iedere leidinggevende dient erop toe te zien dat het organisatieonderdeel, waar hij verantwoording voor draagt, het IBP-beleid naleeft.

4.1. Raad van Bestuur

De RvB is eindverantwoordelijk voor de verwerkingen van persoonsgegevens van de organisatie. De RvB wordt aangemerkt als de verwerkingsverantwoordelijke in de zin van de AVG. De verantwoordelijkheid houdt kort samengevat in:

- Dat de persoonsgegevens verwerkt worden in overeenstemming met de voor de verwerking vastgestelde doelen, dat die doelen gerechtvaardigd zijn en dat de verwerking zorgvuldig gebeurt.
- Dat hierover verantwoording kan worden afgelegd aan de Autoriteit Persoonsgegevens (AP).

De feitelijke verwerking van persoonsgegevens wordt op allerlei lagen van de organisatie uitgevoerd. Het is niet één dienst of college die effectief verantwoordelijk kan zijn voor alle persoonsgegevens die de organisatie verwerkt. Onderscheid bestaat tussen centrale en decentrale verwerkingen, waarvoor resp. de centrale en decentrale organisatieonderdelen zelf verantwoordelijk zijn.

4.2. Leidinggevend/eigenaar (Directeuren)

De leidinggevenden/eigenaren bewaken naleving van het IBP-beleid binnen het eigen organisatieonderdeel (zoals MBO College, School en centrale/decentrale dienst). Zij voeren de daarbij horende operationele taken uit, zoals:

- Zorgen dat geen andere verwerkingen plaatsvinden dan vastgelegd in de dataregisters voor studenten, leerlingen, medewerkers en relaties.
- Zorgen dat geen persoonsgegevens door externe verwerkers worden verwerkt of aan externe partijen worden aangereikt zonder een wettelijke grondslag dan wel een bekrachtigde verwerkersovereenkomst.
- Melden van incidenten rond persoonsgegevens als het vermoeden bestaat dat het gaat om een datalek.
- Zorgen dat medewerkers voldoende geschoold zijn in het kader van de AVG.
- Vastleggen van eventuele bijzondere, extra taken en rollen van medewerkers en de daarbij behorende rechten binnen de bijbehorende systemen/processen.
- Tegengaan c.q. beletten van het gebruik van 'schaduw IT', d.w.z. het inkopen en/of gebruiken van systemen en/of applicaties buiten het zicht van de afdeling Inkoop en/of de centrale dienst OI&I.

4.3. Ondersteunend/adviserend

Adviseurs op het gebied van IBP adviseren, gevraagd en ongevraagd, m.b.t. IBP en ondersteunen de leidinggevenden/eigenaren, bijvoorbeeld bij het afsluiten van overeenkomsten met derde partijen. De adviseurs ontwikkelen beleid op het gebied van IBP. De RvB stelt IBP-beleid vast.

Daarnaast is een interne toezichthouder op de verwerking van persoonsgegevens aangesteld: de FG. De FG dient door de organisatie tijdig te worden betrokken bij alle aangelegenheden waarbij sprake is van de verwerking van persoonsgegevens. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie binnen de organisatie. De FG is aangemeld bij de Autoriteit Persoonsgegevens (AP).

De functie FG kent verschillende taken. Naast een toezichthoudende rol kan de FG ook een *adviserende* rol vervullen.

4.4. Verdeling van de verantwoordelijkheid verwerkingen

De organisatie onderscheidt vijf typen verwerkingen van persoonsgegevens met daarbij benoemde dataeigenaren:

1. De directeur van de centrale dienst OI&I is dataeigenaar van en daarmee verantwoordelijk voor de verwerkingen van persoonsgegevens van alle MBO-studenten die onderwijs volgen c.q. hebben gevolgd, waaronder ook de studenten van Educatie & Inburgering, met inbegrip van eventuele persoonsgegevens van hun ouders/voogden/verzorgers/wettelijke vertegenwoordigers. De directeur van de centrale dienst OI&I is ook dataeigenaar van de persoonsgegevens van de contactpersonen van stage verlenende organisaties die in de centraal beheerde systemen worden geregistreerd.
2. De voorzitter van de directie van het VOvA resp. de rector van het VAVO zijn dataeigenaar van en daarmee verantwoordelijk voor de verwerkingen van persoonsgegevens van alle leerlingen die bij hun organisatieonderdeel onderwijs volgen c.q. hebben gevolgd, met inbegrip van eventuele persoonsgegevens van hun ouders/voogden/verzorgers/wettelijke vertegenwoordigers.
3. De directeur van de centrale dienst HRM is dataeigenaar van en daarmee verantwoordelijk voor de verwerkingen van persoonsgegevens van alle personen die voor de organisatie werkzaam zijn c.q. zijn geweest, en zowel met arbeidsovereenkomst als ingehuurd.
4. De directeur van de centrale dienst PRC&M is dataeigenaar van en daarmee verantwoordelijk voor de verwerkingen van persoonsgegevens van belangstellenden en alumni.
5. De directeuren bedrijfsvoering van de colleges, het VOvA en het VAVO zijn dataeigenaar van de persoonsgegevens geregistreerd in de decentrale systemen van hun college.

De benoemde dataeigenaren zijn tevens verantwoordelijk voor de invulling en het actueel houden van de met de verwerkingen corresponderende dataregisters. Buiten de verantwoordelijkheid van de bovengenoemde dataeigenaren vinden geen verwerkingen van persoonsgegevens plaats, tenzij dit met toestemming van de FG plaatsvindt. De FG bepaalt op welke manier deze verwerkingen worden gedocumenteerd.

4.5. Inpassing in instellingsgovernance en afstemming met aanpalende beleidsterreinen

Om de samenhang in de organisatie met betrekking tot gegevensbescherming goed tot uitdrukking te laten komen en de initiatieven en activiteiten op het gebied van verwerking van persoonsgegevens binnen de

verschillende organisatieonderdelen op elkaar af te stemmen, is het belangrijk om op verschillende niveaus gestructureerd overleg te voeren over het onderwerp privacy.

Op strategisch niveau wordt richtinggevend gesproken over governance en compliance, alsmede over doelen, scope en ambitie op het gebied van privacyaspecten. Het strategisch niveau wordt voorbereid door de tweede en derde lijn. Op tactisch niveau wordt de strategie vertaald naar plannen, te hanteren normen, en evaluatiemethoden. Deze plannen en instrumenten zijn sturend voor de uitvoering. Het tactisch niveau wordt ingevuld door de tweede lijn. Op operationeel niveau vindt de dagelijkse uitvoering plaats.

5. Maatregelen

De organisatie volgt voor IBP dezelfde managementcyclus die ook voor andere bedrijfsaspecten geldt: beleid, analyse, plan implementatie, uitvoering, controles en evaluatie. De maatregelen die getroffen moeten worden om het beleid uit te voeren worden in concrete, gedocumenteerde acties vertaald.

5.1. IBP-beleid

Het IBP-beleid 2024 ligt ten grondslag aan de aanpak van IBP 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 gedragen wordt en de organisatie er naar handelt wordt het IBP-beleid uitgedragen door (of namens) de RvB. De ISO formuleert het IBP-beleid, afgestemd met het MT van de centrale dienst OI&I en andere centrale diensten die kernapplicaties beheren. Het IBP-beleid wordt goedgekeurd door de CISO (directeur van de dienst OI&I) en tot slot vastgesteld door de RvB.

5.2. Planning en controle

Het IBP-beleid wordt tweejaarlijks geëvalueerd en eventueel opnieuw vastgesteld door de RvB. 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 de organisatie een jaarlijks verbeterplan voor IBP. 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. Een en ander leidt tot een (nieuw) jaarplan IBP.

5.3. Rapportage

Elk jaar levert de CISO een jaarverslag en een jaarplan voor het volgende jaar op aan de RvB portefeuillehouder OI&I. In het jaarverslag wordt o.a. ingegaan op incidenten, resultaten van risicoanalyses (incl. genomen maatregelen) en andere initiatieven op het gebied van IBP die het afgelopen jaar hebben plaatsgevonden. Dergelijke verslagen lenen zich voor opname in de bestuurlijke Planning & Control-cyclus. Het jaarplan is mede gebaseerd op de resultaten van periodieke controles/audits/NBA-meting.

Tevens rapporteert de ISO via de dienst OI&I Q rapportage. Dit omvat de voortgang volgens het IBP jaarplan en de security incidenten cq. datalekken.

De FG levert elk jaar een jaarverslag op aan de RvB portefeuillehouder Internal Audit over de naleving van de privacywetgeving en het interne beleid.

5.4. NBA volwassenheidsmodel informatiebeveiliging

De Koninklijke Nederlandse Beroepsorganisatie van Accountants (NBA) heeft in 2016 het Volwassenheidsmodel Informatiebeveiliging gepubliceerd en het in 2019 geactualiseerd. Het model is bedoeld om interne en externe accountants handvatten te geven bij het beoordelen van de volwassenheid van de informatiebeveiliging van een organisatie. Het is geen normenkader (zoals ISO 27001/27002) maar een hulpmiddel om de IBP-volwassenheid -gelet op de risico's- in kaart te brengen, om vervolgens te bepalen waar de organisatie staat en wat er moet gebeuren om het gewenste niveau van informatiebeveiliging te bereiken. Het mbo heeft in navolging van het wo en hbo het NBA-model eveneens geadopteerd.

De organisatie zal jaarlijks d.m.v. NBA de volwassenheid van informatiebeveiliging meten en op basis hiervan haar informatiebeveiliging verbeteren. De meting wordt jaarlijks sector breed vanuit mbo digitaal geïnitieerd. Sector breed is in 2021 de afspraak gemaakt om elke instelling op een volwassenheid van gemiddeld '3' per eind 2026 te krijgen. De organisatie committeert zich hier aan.

5.5. BIV-classificatie en DPIA

Alle informatie heeft waarde, daarom worden alle gegevens waarop dit beleid van toepassing is, geclassificeerd op basis van het ROSA-model. Het ROSA-model is het Referentie Onderwijs Sector Architectuur model en richt zich als onderwijs brede ketenreferentiearchitectuur op het gehele onderwijsdomein en dan met name op zaken die gemeenschappelijk zijn in dat onderwijsdomein (of meerdere delen daarvan) als het gaat om samen te werken in ketenprocessen als ook op (onderwijs)sector overstijgende aspecten van informatievoorziening.

Het niveau van de te nemen beveiligingsmaatregelen is afhankelijk van de toegekende classificatie. De classificatie van informatie is afhankelijk van de gegevens in het informatiesysteem en wordt bepaald op basis van risicoanalyse. Daarbij zijn Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV) de kwaliteitscriteria die van belang zijn.

Binnen de organisatie wordt een op maat gemaakt BIV-classificatieschema gebruikt voor het classificeren van informatie. In dit schema wordt expliciet aangegeven welke maatregelen ter bescherming van de informatie minimaal genomen moet worden. Een BIV-classificatie is van toepassing voor alle door onze organisatie aangeschafte applicaties waarin persoonsgegevens worden verwerkt.

Vanaf de start van elk nieuw project wordt rekening gehouden met IBP, maar ook als er tussentijds iets wijzigt. Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen, wordt vóóraf gekeken naar de impact van beoogde ontwikkelingen en verwerkingen op de bestaande informatiebeveiliging en privacy via een verplichte pre DPIA-toets. Uit deze toets volgt of een volledige DPIA conform de AVG verplicht is. Na uitvoering van de DPIA is inzichtelijk welke passende maatregelen genomen moeten worden.

5.6. Verplicht karakter bewustwording en training

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van het verwerken van persoonsgegevens beheersbaar te houden. Het is noodzakelijk om het bewustzijn van medewerkers voortdurend aan te scherpen, zodat bij de organisatie kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Onderdeel van het beleid zijn de regelmatig terugkerende verplichte bewustwordingscampagnes voor medewerkers en vrijblijvende bewustwordingscampagnes voor studenten/leerlingen en relaties. Verhoging van het bewustzijn is de verantwoordelijkheid van elke leidinggevende en wordt gefaciliteerd door de tweede lijn (zie Hoofdstuk 4).

5.7. Controles

Assessments maken het mogelijk het beleid en de genomen maatregelen te controleren op effectiviteit. De afdeling Internal Audit initieert gezamenlijk met de tweede en derde lijn (zie Hoofdstuk 4) de controle op het rechtmatig en zorgvuldig verwerken van persoonsgegevens.
Eventuele externe controles worden uitgevoerd door onafhankelijke partijen. Deze externe controles worden gepland en geformuleerd in een nauwe samenspraak met de derde lijn van de organisatie.
Het verwerken van persoonsgegevens is een continu proces. Technologische en organisatorische ontwikkelingen binnen en buiten de organisatie maken het noodzakelijk om periodiek te bezien of de organisatie nog voldoende op koers is met het IBP-beleid.

5.8. Logging en monitoring

'Logging en monitoring' door de beheerafdelingen van de diensten OI&I, PRC&M, FC&I en HRM zorgt er voor dat relevante gebeurtenissen met betrekking tot geautomatiseerde systemen en toegang tot gegevens worden vastgelegd. Hieronder vallen onder andere het in- en uitloggen van gebruikers en (pogingen tot) ongeautoriseerde toegang tot het netwerk. De organisatie zal deze logging regelmatig laten beoordelen door de ISO en/of security specialisten. Voor de monitoring van ongebruikelijke activiteiten en het acteren hierop maakt de organisatie gebruik van een Security en Network Operations Center (SOC/NOC).

5.9. Naleving en sancties

De naleving bestaat uit algemeen toezicht op de naleving van beleid en richtlijnen in de dagelijkse praktijk. Naleving van het IBP-beleid is een primaire verantwoordelijkheid van alle medewerkers binnen de organisatie. Leidinggevenden nemen hun verantwoordelijkheid om hun medewerkers aan te spreken in geval van tekortkomingen. Er wordt actief aandacht besteed aan IBP bij de aanstelling van nieuwe medewerkers, tijdens functioneringsgesprekken, d.m.v. een organisatie-brede integriteitscode, d.m.v. periodieke bewustwordingscampagnes, et cetera.
Voor toezicht op de naleving van de AVG vervult de FG een belangrijke rol.
Mocht de naleving van dit beleid en de gedragsregels die er uit voortkomen ernstig tekortschieten, dan heeft de organisatie de mogelijkheid om de betreffende medewerker(s) sancties op te leggen binnen de kaders van de CAO en de wettelijke mogelijkheden.

5.10. Meldpunt incidenten en datalekken

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 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 AP verzorgt.

5.11. Verwerkersovereenkomsten applicaties en educatieve software

Voor iedere verwerking van persoonsgegevens (data) waarbij sprake is van uitbesteding dient met de leverancier (verwerker) een verwerkingsovereenkomst te worden afgesloten, zoals bij onderwijs- en bedrijfsapplicaties en educatieve software. De organisatie heeft hiervoor een procedure Tekenen Verwerkersovereenkomsten vastgelegd waarbij gebruik gemaakt dient te worden van de standaard mbo verwerkersovereenkomst dan wel het privacy convenant Kennisnet (indien een leverancier hierbij is aangesloten). Juridische zaken (JZ) is verantwoordelijk voor het doorlopen van de procedure en de registratie van (bekrachtigde) verwerkersovereenkomsten. De PO en de ISO beoordelen en adviseren over verwerkersovereenkomsten, waarbij de PO zich richt op privacyaspecten en de ISO controleert op een toereikend informatiebeveiligingsniveau.

5.12. Integriteitscode

Op het gebied van informatiebeveiliging stelt de organisatie codes op voor de integriteit en het gedrag van medewerkers, studenten, leerlingen, derden en - indien van toepassing - specifieke doelgroepen. Tweejaarlijks vindt een review plaats van deze codes door de ISO in samenwerking met de PO en afdeling Juridische Zaken.

6. Bijlage Concretisering Governance

In het kader van IBP zijn verschillende onderwerpen van belang. In onderstaand schema (uit het framework IBP mbo) is per onderwerp weergegeven welke taken op welk moment door welke functionaris/lijn (leidinggevend/eigenaar, ondersteunend/adviserend of controlerend) worden uitgevoerd (❶, ❷, ❸ en ❹ zijn *volgordelijke* stappen):

Onderwerp	Leidinggevend (eerste lijn)	Ondersteunend/adviserend (tweede lijn)	Controlerend (derde lijn)
Autorisaties/ toegangsrechten	Applicatie-eigenaar legt gewenste autorisaties/rechten vast en Functioneel Beheer voert uit. ❶	Functioneel Beheer adviseert over en ondersteunt bij het instellen van (toegangs)rechten. ❷	Internal Audit (IA) toetst of 1) het autorisatieproces wordt nageleefd en 2) rechten zijn ingericht conform de principes *need-to-know c.q. least privilege*. ❸
IBP-beleidsstukken	Directie zorgen ervoor dat goedgekeurde kaders en richtlijnen uit vastgestelde beleidsstukken worden opgevolgd. ❷	De adviseurs initiëren en onderhouden n.a.v. evaluatie IBP beleidsstukken en bespreken deze met alle stakeholders. Nieuwe c.q. herziene beleidsstukken leggen ze bij de RvB ter vaststelling voor. ❶	IA toetst de werking van onderdelen uit de door de RvB goedgekeurde IBP-beleidsstukken. ❸
Bewaartermijn	Directie is verantwoordelijk voor het handhaven van de bewaartermijnen conform het Documentair StructuurPlan (DSP). ❶	De adviseurs adviseren aan de hand van het DSP de leidinggevenden over de geldende bewaartermijnen. ❷	IA toetst de werking van onderdelen uit het DSP. ❸
Bewustwording	Directie voert bewustwordingsplannen van de adviseurs uit of voert een afgeleide plannen uit. ❷	De adviseurs stellen jaarlijks een plan op voor bewustwording en scholing op het gebied van IBP en faciliteren centrale training. ❶	IA toetst de werking van plannen voor bewustwording en scholing, en komt eventueel met aanbevelingen. ❸
Data Protection Impact Assessment (DPIA, beoordeling van privacy risico's)	Directie vraagt om een nieuwe verwerking. ❶ Directie wordt betrokken bij de uitvoering en vaststelling van de DPIA ❸	De ISO, FG en PO stellen via een pre-DPIA vast of een DPIA vereist is en, zo ja, organiseren de uitvoering van de DPIA. ❷	IA toetst de werking van de beheersmaatregelen rondom DPIA. ❹
Datalekken	Medewerkers melden zelf intern een datalek via TOPdesk of via de Servicedesk. Directie draagt zorg voor bekendheid van de meldprocedure en scholing hierin van haar medewerkers. ❶	De FG en PO besluiten, in overleg met de dataeigenaar, om het datalek al dan niet te melden bij de AP en/of betrokkene(n). ❷ De FG en PO registreren datalekken in een datalekregister en rapporteren periodiek m.b.t. datalekken aan de RvB.	IA toetst de werking van de beheersmaatregelen rondom het proces van datalekken. ❸
Dataregisters centraal	De dataeigenaren bewaken periodiek de actualiteit van het dataregister. ❶	De adviseurs controleren op volledigheid, juistheid en actualiteit van de Dataregisters. ❷	IA toetst of dataregisters voldoen aan wet- en regelgeving. ❸
Door het management aangewezen uitvoerders	Directie wijst deelprocesuitvoerders aan (bijv. examinering, roostering, stage, etc.). ❶	Functioneel beheer toetst het toegewezen eigenaarschap aan de autorisatie. ❷	IA toetst de werking van de beheersmaatregelen rondom het aanwijzen c.q. autoriseren van deelprocesuitvoerders. ❸

Onderwerp	Leidinggevend (eerste lijn)	Ondersteunend/adviserend (tweede lijn)	Controlerend (derde lijn)
Rechten van de betrokkenen	Dataeigenaar ontvangt verzoeken van betrokkenen en nemen deze in behandeling. ❶	De PO en/of FG adviseren m.b.t. de afhandeling van verzoeken van betrokkenen. ❷	IA toetst de werking van de beheersmaatregelen rondom de afhandeling van verzoeken van betrokkenen. ❸
Verwerkersovereenkomsten	In geval van uitbestede verwerking draagt de dataeigenaar zorg voor een toereikende, rechtsgeldige verwerkersovereenkomst. Dienst OI&I en JZ adviseren hierbij. ❶	FG, PO en ISO adviseren (verplicht) bij de totstandkoming van verwerkersovereenkomsten. ❷	IA toetst de werking van de beheersmaatregelen rondom verwerkersovereenkomsten. ❸
Vragen van medewerkers betreffende IBP-gerelateerde onderwerpen	Directie is het eerste aanspreekpunt voor vragen inzake privacy en security. ❶	De PO en/of FG adviseren de leidinggevende en/of medewerker. ❷	IA toetst het proces van informeren van betrokkenen. ❸

N.b. Toetsing door Internal Audit vindt jaarlijks en risicogericht plaats.

7. Bijlage Afkortingen en Begrippen

Afkortingen

De volgende afkortingen zijn relevant in het kader van het IBP-beleid en de onderwerp specifieke beleidsregels van ROC van Amsterdam-Flevoland:

AP	Autoriteit Persoonsgegevens
AVG	Algemene Verordening Gegevensbescherming
BIA	Business Impact Analyse
DPIA	Data Protection Impact Assessment
FG	Functionaris Gegevensbescherming
IBP	InformatieBeveiliging en Privacy
ICT	Informatie- en CommunicatieTechnologie
ISO	Information Security Officer
MFA	Multi-Factor Authentication
NPA	Niet Persoonsgebonden Account
PGA	PersoonsGebonden Account
P&C	Planning en Control
PO	Privacy Officer

Begrippen

Voor de informatiebeveiliging en privacy van ROC van Amsterdam - Flevoland gelden de volgende definities:

Account: Een deel van een ICT-systeem/applicatie waartoe een gebruiker of andere systeem toegang heeft. Er bestaan verschillende soorten accounts, zoals gebruikersaccounts, beheeraccounts, administratoraccounts, serviceaccounts, et cetera. Bij een account hoort informatie over de gebruiker (kan ook een computerservice/-proces zijn), zoals inloggegevens en de delen van c.q. informatie in het systeem waar de gebruiker bij mag.

Actor(en): Identificeerbare personen en gremia met een bepaalde, gedefinieerde rol, die als speler/deelnemer betrokken zijn in het informatiebeveiligingsproces.

Applicatie: Computerprogramma bedoeld voor één of meer eindgebruikers (resp. single user en multi user), wordt vaak afgekort tot ‘app’. Alternatieve term: ‘toepassing’. In de context van IBP hebben we het veelal over (web)applicaties met meerdere eindgebruikers ter ondersteuning van een (bedrijfs)proces.

Applicatie-eigenaar: Identificeerbaar persoon binnen de organisatie die ervoor (eind)verantwoordelijk is dat een applicatie blijvend 1) een goede ondersteuning biedt aan het proces c.q. de processen en de gebruikers waarvoor deze bedoeld is en 2) voldoet aan wet- en regelgeving.

Audits: Onafhankelijke controles op naleving van het gedocumenteerde beleid, beheersmaatregelen, richtlijnen, (gedrags)regels, procedures, enzovoorts.

Authenticatie/authentiseren: Het met een zekere betrouwbaarheid verifiëren van de identiteit van een persoon, andere computer of applicatie, aan de hand van met de identiteit verbonden kenmerken, bijvoorbeeld aan de hand van iets wat slechts alleen de betreffende persoon kan weten (zoals een niet uitgelekt wachtwoord) of in zijn bezit heeft (bijvoorbeeld een vingerafdruk).

Autorisatie: Specifiek formeel toegekende rechten of bevoegdheden, zie **Autoriseren**.

Autoriseren: Het toekennen van specifieke rechten of bevoegdheid aan een persoon of groep van personen, zoals het mogen betreden van of werken in bepaalde ruimten, het gebruiken van middelen, kennisnemen van informatie, doen van betalingen, et cetera. De persoon die autoriseert kan dit alleen doen als hij/zij hiertoe bevoegd is.

Beschikbaarheid: De mate waarin (geautoriseerde) gebruikers toegang hebben tot informatie en aanverwante bedrijfsmiddelen (informatiesystemen) op het vereiste moment en de vereiste locatie.

Betrokkene: Individueel, natuurlijk persoon op wie een persoonsgegeven betrekking heeft.

Betrouwbaarheid: De mate waarin de organisatie zich kan verlaten op een informatiesysteem voor zijn informatievoorziening, ter ondersteuning van een of meer afhankelijke bedrijfsprocessen.

Bijzondere persoonsgegevens: Gegevens over iemands:
- ras of etnische afkomst;
- politieke opvattingen;
- religieuze of levensbeschouwelijke overtuiging;
- lidmaatschap van een vakvereniging;
- genetische of biometrische gegevens met oog op unieke identificatie;
- gezondheid;
- seksueel gedrag of seksuele gerichtheid;
- strafrechtelijk verleden.

Calamiteit: Gebeurtenis die een of meer bedrijfsprocessen in ernstige mate kan ontwrichten en daarmee het bereiken van de bedrijfsdoelstellingen of zelfs het voortbestaan van de organisatie in gevaar kan brengen. Een calamiteit kan uitmonden in een crisis(situatie).

Client: Intelligent device (apparaat) waarmee de gebruiker werkt, zoals laptop/PC/computer, tablet en smartphone.

Cybercrisis: Iedere (moedwillige) verstoring, uitval of misbruik van een gedigitaliseerd proces, (informatie)systeem of informatiedienst die de maatschappelijke continuïteit, openbare orde en veiligheid bedreigt of verstoort.

Cybergevolgbestrijding: Het zoveel mogelijk beperken van de impact van een cybercalamiteit.

Data Protection Impact Asessment (DPIA): Een gestructureerde, systematische beoordeling die helpt bij het identificeren van privacy risico's en leveren van de handvatten om geïdentificeerde risico's te verkleinen tot een acceptabel niveau.

Dataeigenaar: Identificeerbaar persoon binnen de organisatie die in het kader van IBP verantwoordelijk is voor één of meer verwerkingen van persoonsgegevens, met name wat betreft het voldoen aan de AVG.

Datalek: Een inbreuk op de beveiliging die (per ongeluk of op onrechtmatige wijze) leidt tot de vernietiging, het verlies, de wijziging, de ongeoorloofde verstrekking of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens.
Nb. Als bij de inbreuk geen persoonsgegevens betrokken zijn, spreken we niet van een datalek.

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

Dataregister (ook wel 'Register van Verwerkingsactiviteiten' of 'Verwerkingsregister'): Overzicht van de persoonsgegevens die verwerkt worden, met informatie over het doel daarvan, de grondslag ervoor, de bewaartermijnen van de gegevens en bron of ontvanger van de gegevens.

Eigenaar: Identificeerbaar, aangewezen persoon binnen de organisatie die een specifieke rol vervult ten aanzien van het benoemde bedrijfsmiddel (proces, applicatie, systeem, gegevensverzameling, overeenkomst, etc.). Eigenaarschap is hierbij niet in juridische zin bedoeld en ligt veelal bij de (verantwoordelijke) leidinggevende van een afdeling of team.

Systeemeigenaar: Identificeerbaar, aangewezen persoon binnen de organisatie die een specifieke rol vervult ten aanzien van een specifiek informatiesysteem. Denk onder meer aan het (eind)verantwoordelijk zijn voor het formuleren en vaststellen van beveiligingseisen en implementeren en handhaven van de beveiliging van het systeem. Eigenaarschap is hierbij niet in juridische zin en ligt veelal bij de leidinggevende van de afdeling of het team dan wel de verantwoordelijke voor het proces dat het informatiesysteem in hoofdzaak benut ('proceseigenaar').

Functiescheiding: Het vanuit controle- en/of risico-overwegingen aanbrengen van een splitsing in taken en bevoegdheden, die samenhangen met handelingen die in potentie verstrekkende gevolgen (kunnen) hebben, over verschillende daartoe aangewezen functionarissen. Zie ook vier-ogenprincipe.

Functionaris voor de Gegevensbescherming (FG): Interne toezichthouder en privacy adviseur aangesteld door de Raad van Bestuur, op grond van artikel 37 van de Algemene Verordening Gegevensbescherming (AVG).

Gebruiker: Elk (natuurlijk) persoon die op enige wijze is verbonden aan de organisatie, voor zijn/haar werk middelen van de organisatie benut (zoals informatie, informatiesystemen en ruimten) en tot dit gebruik geautoriseerd is, zoals medewerkers met een arbeidsovereenkomst, ingehuurd personeel, vrijwilligers, stagiairs, medewerkers van samenwerkingspartijen, leveranciers, dienstverleners, enzovoort. Hierbij zijn:

- **Interne gebruikers** medewerkers van de organisatie met een tijdelijke of vaste aanstelling alsmede ingehuurd personeel, vrijwilligers en stagiairs;
- **Externe gebruikers** medewerkers van samenwerkingspartijen, leveranciers, dienstverleners, enzovoort.

Hardening: Het vergaand bestand maken van een systeem tegen pogingen, primair van buitenaf, maar ook eventuele aanvallen van binnenuit (als een indringer kans heeft gezien toegang te krijgen tot het systeem), het te overmeesteren, via een combinatie van acties/aanpassingen op het systeem.

Identificatie: Het kenbaar maken van de identiteit van iets: een ‘subject’ (bijv. een gebruiker of een proces), aan de hand van een uniek kenmerk. Op basis van identiteit en autorisatie krijgt het subject met vooraf bepaalde rechten toegang tot objecten. Een object is bijvoorbeeld een computerbestand, een gegevensverzameling of een onderdeel van een bedrijfsapplicatie, zoals een beheermodule of een financieel dashboard. Identificatie kan op uiteenlopende manieren plaatsvinden.

Informatiebeveiliging: Het proces van vaststellen, treffen, onderhouden en controleren van een samenhangend pakket van maatregelen ter waarborging van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie en informatiesystemen. Zodat informatie en informatievoorzieningen beschikbaar zijn op de momenten dat dat vereist is, vertrouwelijke informatie niet toegankelijk is voor personen voor welke deze niet is bedoeld en we kunnen vertrouwen op de juistheid en volledigheid van informatie.

Informatiebeveiligingsgebeurtenis (‘beveiligingsincident’): Geconstateerde dan wel vermoede aantasting van de vertrouwelijkheid, integriteit en/of de beschikbaarheid van informatie of informatievoorzieningen alsmede situaties die het ontstaan van een aantasting in de hand werken.

Informatiesysteem: Het interne netwerk alsmede alle (bedrijfs)applicaties met meerdere gebruikers waarvan de organisatie eigenaar dan wel opdrachtgever is. Losse toepassingen voor één gebruiker worden er niet onder verstaan. Naar gelang de context kunnen de termen ‘informatiesysteem’ en ‘(bedrijfs)applicatie’ afwisselend worden gebruikt.

Information Security Management System (ISMS): Kwaliteitssysteem voor het bewerkstelligen en handhaven van een passend niveau van informatiebeveiliging door het iteratief en periodiek doorlopen van een plan-do-check-act cyclus.

InformatieVeilig Werken: Onder informatieveilig werken vallen tal van activiteiten om de veiligheid van informatie te vergroten. Initiatieven op dit gebied hebben ten doel het veiligheidsbewustzijn en juist handelen van medewerkers te vergroten.

Integriteit: De mate van juistheid en volledigheid van informatie en de verwerking ervan.

Logging: Het proces van registreren (loggen) van informatie over menselijke- en systeemactiviteiten voor analyse- en bewakingsdoeleinden.

Logische toegang: Toegang tot digitale informatiesystemen, d.w.z. tot het interne netwerk en alle bedrijfsapplicaties waarin de organisatie zelf in voorziet alsmede die in Saas of andere vorm die ze afneemt van leveranciers.

Maatregel: Handeling of ingreep met een bepaald doel, bijv. gericht op het reduceren van dreiging, het verlagen van de kans op manifestatie, het voorbereid zijn op incidenten, het (zo snel mogelijk) detecteren van incidenten (incl. alarmering), het inperken en onder controle krijgen van incidenten en het herstellen van de oude situatie.

Minderjarige: Voor de AVG is een minderjarige ieder natuurlijk persoon die de leeftijd van 16 jaar nog niet heeft bereikt. Buiten de AVG geldt jonger dan 18 jaar.

MultiFactor Authenticatie (MFA): Een betrouwbare wijze van authentiseren, aan de hand van meer dan één factor, bijvoorbeeld aan de hand van iets wat de gebruiker weet (zoals toegangscode/wachtwoord) in combinatie met een uniek middel dat de gebruiker bezit (zoals een chipkaart). Bij twee-factor authenticatie (2FA), ook wel aangeduid als tweetrapsverificatie, wordt de identiteit van de gebruiker geverifieerd aan de hand van twee factoren. Bij tweestapsverificatie wordt de identiteit van de gebruiker geverifieerd *in twee slagen* aan de hand van twee factoren.

Niet-persoonsgebonden account (NPA): Account dat niet bij een bepaalde (natuurlijk) persoon hoort. Er zijn twee soorten NPA's:

- **Non-interactive NPA.** Dit soort accounts worden uitsluitend gebruikt voor/door systemen, niet door gebruikers of beheerders.
- **Interactive NPA.** Dit soort accounts worden gedeeld door twee of meer (natuurlijke) personen voor bepaalde taken, bijvoorbeeld voor beheertaken. Ze zijn veelal uit den boze omdat de handelingen die verricht zijn via het account niet tot een natuurlijk persoon als 'dader' te herleiden zijn.

Persoonsgebonden account (PGA): Account dat bij een bepaald (natuurlijk) persoon als gebruiker hoort. Het is deze persoon, als gebruiker/eigenaar van het account, door de organisatie verboden het account door andere personen te laten gebruiken. Handelingen, die verricht zijn via het account, zijn het herleiden tot de gebruiker/eigenaar van het account (als 'actor).

Persoonsgegevens: Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"). Als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

Privacy by Default: Beleidsregel c.q. richtlijn om standaardinstellingen van producten en diensten zodanig te laten zijn 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: Beleidsregel c.q. richtlijn om tijdens de (door) ontwikkeling van een nieuw of bestaand informatiesysteem aandacht te besteden aan 1) privacy verhogende maatregelen en 2) dataminimalisatie: het zo min mogelijk verwerken van persoonsgegevens, uitsluitend gegevens die noodzakelijk zijn voor het doel van de verwerking.

Proceseigenaar: Identificeerbaar persoon binnen de organisatie die verantwoordelijk is voor één van de primaire of ondersteunende processen, zoals Onderwijs, Inkoop en HRM.

Provisioning: Het proces van het verstrekken van faciliteiten en permissies aan een persoon op basis van vastgestelde regels. Term voor het deelproces binnen het Identity and Access Management (IAM)-proces waarmee aan een individu (toegangs-)rechten voor informatiesystemen worden verstrekt (= User Provisioning), op basis van de functie of rol van de persoon (Role Based Access Control). Andere mogelijkheid: het toekennen van dezelfde rechten als een gelijksoortige gebruiker (via het kopiëren van de rechten van die andere gebruiker).

Restrisico: Het risico dat overblijft (resteert) nadat maatregelen zijn getroffen.

Risico: De kans (waarschijnlijkheid) dat een onzekere gebeurtenis met negatieve effecten zich in een gegeven periode en situatie zal voordoen.

Risicobeheer/risicomanagement: Het inzichtelijk en systematisch inventariseren, beoordelen en - door het treffen van maatregelen - beheersbaar maken van risico's en kansen, die het bereiken van de doelstellingen van een organisatie bedreigen dan wel bevorderen, op een zodanige wijze dat verantwoording kan worden afgelegd over de gemaakte keuzes.

Self assessments: Controles waarbij de organisatie zelf, aan de hand van een lijst met controlepunten, toetst in hoeverre ze maatregelen correct en volledig uitvoert.

Serviceaccount: Een niet-persoonsgebonden account specifiek bedoeld voor een computerservice/-proces, voor het uitvoeren van taken en diensten zonder gebruikersinteractie (non-interactive).

Single Sign On (SSO): Een ICT-implementatie waarbij de gebruiker slechts eenmalig behoeft te authentiseren (inloggen, zich aanmelden) om toegang te krijgen tot een ICT-omgeving inclusief beschikbare applicaties.

Social engineering: Het (door kwaadwillenden) misbruiken c.q. manipuleren van mensen op basis van menselijke zwakheden en valkuilen, zoals hebzucht, begeerte, nieuwsgierigheid, goedgelovigheid, gevoeligheid voor misleiding, blindheid, dienstbaarheid, et cetera.

Step-up: Een extra ingebouwde, verplichte authenticatieslag om een of meer handelingen te kunnen verrichten waarvoor bijzondere rechten nodig zijn, bijvoorbeeld voor het invoeren van gezondheidsgegevens of het plegen van technisch of functioneel beheer.

Systeem voor wachtwoordbeheer: De functionaliteit cq. het onderdeel van een informatiesysteem voor onder meer het interactieve beheer van wachtwoorden en technisch afdwingen van het beleid rondom wachtwoorden, zoals het gebruik van sterke wachtwoorden.
Nb. Systeem voor wachtwoordbeheer is een veelal tot verwarring leidende ISO27002/NEN7510/BIO term. NIET bedoeld worden digitale wachtwoordbeheertools als Dashlane, Keepass of LastPass.

Uitingsvorm: De vorm waarin een boodschap, informatie, gegevens, data, etc. is ‘verpakt’, op welke wijze dan ook, zoals schrift, stilstaand beeld (tekening, diagram, foto, emoji, etc.), bewegend beeld (video, animatie, etc.), spraak, geluid, digitaal, analoog, etc.

User endpoint devices: Laptops, desktops, smartphones, tablets etc.

Toepassing: (Bedrijfs-)Applicatie.

Vertrouwelijkheid: De mate waarin informatie uitsluitend toegankelijk moet zijn voor geautoriseerde gebruikers. Het gaat hier onder meer om het beveiligen van ruimtes, informatiesystemen en de ICT-infrastructuur tegen onbevoegde toegang (hackers en andere indringers) en malware (virussen, ransomware, Trojan horses e.d.). Maar ook om maatregelen om te voorkomen dat gebruikers toegang krijgen tot informatie die niet voor hen is bedoeld.

Verwerken/verwerking: Elke bewerking/handeling of een geheel van bewerkingen/handelingen met betrekking tot een registratie, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking, stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens. In de context van de Algemene Verordening Gegevensbescherming (AVG) gaat het hierbij specifiek om persoonsgegevens of een geheel van persoonsgegevens.

Verwerker: Een ingeschakelde (derde) partij die in expliciete opdracht ten behoeve van de organisatie (als verwerkingsverantwoordelijke) persoonsgegevens verwerkt, e.e.a. op de wijze als schriftelijk vastgelegd in een (hoofd)overeenkomst en verwerkersovereenkomst, aangevuld met eventuele andere document, zoals een dienstverleningsovereenkomst, instructies, etc.).

Verwerkingsverantwoordelijke: Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

Vier-ogenprincipe: Werkwijze met meervoudige onafhankelijke controle door twee of meer personen/partijen (bijvoorbeeld bij het goedkeuren van een betaling of het invoeren van examenresultaten). Het vier-ogenprincipe is een procedureel uitgangspunt dat stelt dat voor bepaalde handelingen altijd tenminste twee personen nodig zijn, zodat zij elkaar kunnen controleren en de correctheid niet afhankelijk is van slechts één individu.