Beleid verwerking persoonsgegevens en informatieveiligheid

U2023/3560
Vastgesteld door het College van bestuur op 26 september 2023

Open Universiteit

INHOUDSOPGAVE

Open Universiteit

Beleid verwerking persoonsgegevens Open Universiteit

Open Universiteit

Colofon

Beleid verwerking persoonsgegevens, als onderdeel van het Informatie en beveiligingsbeleid Open Universiteit

Auteurs: Mark Adriolo (JZ), Judith Niesters (JZ)
Afgestemd met Martin Romijn (ITF), CISO en Saskia van der Westen, (HJI), FG

Open Universiteit
Valkenburgerweg 177, 6419 AT Heerlen
Postbus 2960, 6401 DL Heerlen
T +31 45 576 28 88
info@ou.nl
www.ou.nl

Het beleid verwerking persoonsgegevens van de Open Universiteit is gebaseerd op het Model beleid verwerking persoonsgegevens, opgesteld door de SURF *Versie 2.0 maart 2018*

SURF is de ICT-samenwerkingsorganisatie van het Nederlandse hoger onderwijs en onderzoek.
Deze publicatie is digitaal beschikbaar via de website van SURF: www.surf.nl/publicaties

Inhoudsopgave

1. Inleiding

Opslag en Verwerking van Persoonsgegevens is noodzakelijk voor de bedrijfsprocessen van instellingen van onderwijs en onderzoek. Dit dient met de grootste zorgvuldigheid te gebeuren omdat misbruik van Persoonsgegevens grote schade kan berokkenen aan studenten, medewerkers en andere Betrokkenen bij Open Universiteit (OU), maar ook bij OU zelf. De OU hecht dan ook veel waarde aan het beschermen van de Persoonsgegevens die aan haar worden verstrekt en aan de wijze waarop Persoonsgegevens worden verwerkt. Het op een juiste manier verwerken van Persoonsgegevens is de verantwoordelijkheid van het College van bestuur van de OU.

Met het beschrijven van de maatregelen in dit beleidsdocument beoogt en neemt de OU haar verantwoordelijkheid om de kwaliteit van de verwerking en de beveiliging van Persoonsgegevens te optimaliseren en daarmee te voldoen aan de relevante privacywet- en regelgeving.

Naast dit beleid heeft het College van bestuur een Privacyverklaring vastgesteld die te vinden is op www.ou.nl/privacy. Deze verklaring bevat nadere informatie over van wie welke persoonsgegevens door de OU worden verwerkt.

1.1. Definities

AVG: Algemene Verordening Gegevensbescherming[1].

Beleid: dit beleid met betrekking tot het verwerken van Persoonsgegevens door de OU.

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

Verwerkingsverantwoordelijke: College van bestuur van de OU die het doel en de middelen van de Verwerking van Persoonsgegevens vaststelt.

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

Verwerker: een door de OU ingeschakelde (derde) partij die ten behoeve van de OU en op basis van diens schriftelijke instructies, Persoonsgegevens verwerkt.

Verwerking: elke handeling of geheel van handelingen met betrekking tot Persoonsgegevens, waaronder het verzamelen, vastleggen, ordenen, opslaan, raadplegen, bijwerken, afschermen, wissen of vernietigen van gegevens.

Derde: ieder ander, niet zijnde de Betrokkene, de Verwerkingsverantwoordelijke of de Verwerker, of enig persoon die onder rechtstreeks gezag valt van de Verwerkingsverantwoordelijke of de Verwerker en gemachtigd is om Persoonsgegevens te verwerken.

Datalek: een inbreuk op de beveiliging van Persoonsgegevens, die leidt tot enige ongeoorloofde Verwerking daarvan. Hier vallen zowel opzettelijke als onopzettelijke datalekken onder.

DTIA: Data Transfer Impact Assessment

[1] De Algemene Verordening Gegevensbescherming is op 25 mei 2016 in werking getreden en per 25 mei 2018 van kracht.

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

Privacy by Design: Het beheer van de gehele levenscyclus van Persoonsgegevens, vanaf het verzamelen tot het verwerken en verwijderen, waarbij mechanismen zo zijn ontworpen dat zij zo veel mogelijk rekening houden met de privacy van Betrokkenen. Hierbij wordt stelselmatig aandacht besteed aan allesomvattende waarborgen m.b.t. nauwkeurigheid, vertrouwelijkheid, integriteit, fysieke veiligheid en verwijdering van de Persoonsgegevens.

Privacy Impact Assessment (gegevensbeschermingseffectbeoordeling): Een beoordeling die helpt bij het identificeren van privacy risico's en de handvatten levert om deze risico's te verkleinen tot een acceptabel niveau.

Profilering: elke vorm van geautomatiseerde Verwerking van Persoonsgegevens waarbij aan de hand van Persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, onder andere met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.

Minderjarige: iedere persoon die de leeftijd van 16 jaar nog niet heeft bereikt.

1.2. Reikwijdte en doelstelling van het Beleid

Het Beleid heeft betrekking op het verwerken van Persoonsgegevens van alle Betrokkenen binnen de OU waaronder in ieder geval alle medewerkers, studenten, gasten, bezoekers en externe relaties (in-huur/outsourcing), alsmede op andere Betrokkenen waarvan de OU Persoonsgegevens verwerkt.

In het Beleid ligt de nadruk op de geheel of gedeeltelijk geautomatiseerde / systematische verwerking van Persoonsgegevens die plaatsvindt onder de verantwoordelijkheid van de OU alsmede op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen. Eveneens is het Beleid van toepassing op niet-geautomatiseerde verwerking van Persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

Bij de OU wordt het beschermen van Persoonsgegevens breed geïnterpreteerd. Er is een belangrijke relatie en gedeeltelijke overlap met het aanpalende beleidsterrein informatiebeveiliging, waarbij het gaat om de beschikbaarheid, integriteit en de vertrouwelijkheid van data, waaronder Persoonsgegevens. Op strategisch niveau wordt aandacht geschonken aan deze raakvlakken en wordt zowel planmatig als inhoudelijk afstemming gezocht. Het Beleid bij de OU heeft als doel om de kwaliteit van de Verwerking en de beveiliging van Persoonsgegevens te optimaliseren waarbij een goede balans moet worden gevonden tussen privacy, functionaliteit en veiligheid.

Beoogd wordt de persoonlijke levenssfeer van de Betrokkene zoveel mogelijk te respecteren. De gegevens die betrekking hebben op een Betrokkene dienen beschermd te worden tegen onwettelijk en ongeautoriseerd gebruik dan wel misbruik op basis van het fundamenteel recht op bescherming van zijn / haar Persoonsgegevens. Dit brengt met zich mee dat het verwerken van Persoonsgegevens dient te voldoen aan relevante wet- en regelgeving en dat Persoonsgegevens veilig zijn bij de OU.

Doelstelling van het Beleid voor de OU is concreet het volgende:

- Het bieden van een kader: het Beleid biedt een kader om (toekomstige) Verwerkingen van Persoonsgegevens te toetsen aan een vastgestelde 'best practice' of norm en om de taken, bevoegdheden en verantwoordelijkheden in de organisatie te beleggen.

- Het stellen van normen van risico's als gevolg van het niet compliant zijn met de relevante wet- en regelgeving. De basis voor de beveiliging van Persoonsgegevens is ISO 27001[2]. Maatregelen worden op basis van 'best practices' in het hoger onderwijs en o.b.v. ISO 27002 genomen[3].
- Het SURF Juridisch Normenkader (Cloud)services[4] wordt gehanteerd als best practice voor cloud services en andere outsource contracten.
- Het nemen van verantwoordelijkheid door het college van bestuur door middel van de uitgangspunten en de organisatie van het verwerken van Persoonsgegevens vast te leggen voor de hele organisatie/ de OU.
- Daadkrachtige implementatie van het beleid door duidelijke keuzes in maatregelen te maken en actieve controle toe te passen op de uitvoering van de beleidsmaatregelen.
- Compliant zijn met de Nederlandse en Europese wetgeving.

Naast bovenstaande concrete doelstellingen is een meer algemeen doel het creëren van bewustwording van het belang en de noodzaak van het beschermen van Persoonsgegevens.

[2] Voluit: NEN-ISO/IEC 27001: Eisen aan Managementsystemen voor informatiebeveiliging
[3] Voluit: NEN-ISO/IEC 27002: Code voor Informatiebeveiliging
[4] SURF juridisch Normenkader (Cloud)services, vastgesteld door bestuur Platform ICT & Bedrijfsvoering 3 april 2014 en geüpdatet in 2016, te vinden via https://www.surf.nl/kennisbank/2013/surf-juridisch-normenkader-cloudservices.html.

2. Beleidsprincipes Verwerking Persoonsgegevens

2.1. Beleidsuitgangspunt en –principes

Algemeen beleidsuitgangspunt is dat Persoonsgegevens in overeenstemming met de relevante wet- en regelgeving op behoorlijke en zorgvuldige wijze worden verwerkt. Hierbij dient een goede balans te worden aangebracht tussen het belang van de OU om Persoonsgegevens te verwerken en het belang van Betrokkene ter eerbiediging van zijn persoonlijke levenssfeer om in een vrije omgeving eigen keuzes te maken met betrekking tot zijn Persoonsgegevens.

Om aan bovenstaand beleidsuitgangspunt te voldoen gelden de volgende principes:

- Een Verwerking van Persoonsgegevens is gebaseerd op een van de wettelijke grondslagen zoals genoemd in artikel 6 van de AVG (“rechtmatigheid”).
- Persoonsgegevens worden alleen verwerkt op een manier die ten aanzien van de Betrokkene behoorlijk en transparant is. Dit houdt in dat het voor betrokkenen inzichtelijk moet zijn in hoeverre en op welke manier Persoonsgegevens worden verwerkt. Informatie en communicatie hierover moet eenvoudig toegankelijk en begrijpelijk zijn (“behoorlijkheid en transparantie”).
- Persoonsgegevens worden alleen verwerkt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Het gaat hier om specifieke en gerechtvaardigde doeleinden, die zijn vastgelegd en omschreven voordat men begint met de Verwerking. Persoonsgegevens worden niet verder Verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen (“doelbinding”).
- 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 (“minimale gegevensverwerking”).
- Verwerking van Persoonsgegevens gebeurt op de minst ingrijpende wijze en dient in redelijke verhouding te staan tot het beoogde doeleinde (“minimale gegevensverwerking”).
- Maatregelen worden getroffen om zoveel mogelijk te waarborgen dat de te verwerken Persoonsgegevens juist en actueel zijn (“juistheid”).

Persoonsgegevens worden adequaat beveiligd volgens de geldende beveiligingsnormen en de huidige stand van de techniek (“integriteit en vertrouwelijkheid”). Persoonsgegevens worden niet langer verwerkt dan noodzakelijk is voor de doeleinden van de Verwerking. Hierbij worden de van toepassing zijnde bewaar- en vernietigtermijnen uit de Basisselectielijsten Universiteiten en Universitaire Medische Centra 2020 (inclusief voorgangers en opvolgers) in acht genomen (“opslagbeperking”).

3. Wet- en regelgeving

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

3.1. Wet op het Hoger onderwijs en Wetenschappelijk onderzoek

De OU heeft een kwaliteitszorgsysteem, waarin (onder meer) het zorgvuldig omgaan met (persoons)gegevens en met de studieresultaten in de studentenadministratie is gewaarborgd. Daarnaast worden gedrags- en integriteitscodes voor (niet-)wetenschappelijk personeel nageleefd en toegepast.

3.2. Algemene Verordening Gegevensbescherming

De OU heeft de wettelijke vereisten (waaronder het rechtmatig en zorgvuldig verwerken van Persoonsgegevens en het nemen van passende technische- en organisatorische maatregelen tegen verlies en onrechtmatige Verwerking van data c.q. Persoonsgegevens) geïmplementeerd door middel van het Beleid.

3.3. Archiefwet

De OU houdt zich aan de voorschriften uit de Archiefwet en het Archiefbesluit over de wijze waarop omgegaan moet worden met informatie vastgelegd in (gedigitaliseerde) documenten, informatiesystemen, websites, e.d..

4. Rollen en verantwoordelijkheden met betrekking tot Verwerking Persoonsgegevens

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

4.1. College van bestuur

Het College van bestuur is de Verwerkingsverantwoordelijke en daarmee de eindverantwoordelijke voor de rechtmatige en zorgvuldige Verwerking van Persoonsgegevens binnen de OU en stelt het beleid, de maatregelen en de procedures op het gebied van Verwerking(en) vast.

4.2. Gemandateerde beveiliging Persoonsgegevens

Bij de Open Universiteit is het College van bestuur eindverantwoordelijk voor de beveiliging van Persoonsgegevens binnen de OU. Het College van bestuur heeft een gemandateerde verwerkingsverantwoordelijke benoemd die verantwoordelijk is voor de Informatiebeveiliging en het privacybeleid van de OU. Aanvullend is de gemandateerde het eerste aanspreekpunt voor de Functionaris Gegevensbescherming ingeval van een datalek.

4.3. Functionaris Gegevensbescherming

De OU heeft een interne toezichthouder op de Verwerking van Persoonsgegevens benoemd. Deze toezichthouder wordt Functionaris Gegevensbescherming genoemd (hierna: “FG”). De FG zal door de OU tijdig worden betrokken bij alle aangelegenheden waar Persoonsgegevens bij komen kijken. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie bij de OU. De OU zal de FG aanmelden bij de toezichthoudende autoriteit. De contactgegevens van de FG worden gepubliceerd op www.ou.nl/privacy.

De taken van de FG houden in:

- het informeren en adviseren van alle betrokken partijen over hun verplichtingen onder de AVG;
- het toezien op de naleving van de AVG en andere relevante privacywetgeving;
- het toezien op de naleving van dit privacybeleid door de OU;
- het toezien op een Privacy Impact Assessment;
- het toezien op een DTIA;
- het samenwerken met de toezichthoudende autoriteit;
- fungeren als eerste aanspreekpunt voor de toezichthoudende autoriteit.

4.4. Privacyofficer

De OU heeft een Privacyofficer in dienst, werkzaam bij de afdeling Juridische zaken, die de hele organisatie aan de voorkant adviseert over uiteenlopende (juridische) privacyvraagstukken en die bijdraagt aan het mede opstellen van beleid op het gebied van persoonsgegevens. Naast de adviserende rol heeft de Privacyofficer bepaalde taken indien een Betrokkene zich meldt met een specifiek verzoek ten aanzien van zijn / haar rechten.

4.5. Eigenaar bedrijfsproces

Een bedrijfsproces is een zich herhalende keten van activiteiten gericht op de klant en afgestemd op de organisatie. De eigenaar van een bedrijfsproces is de persoon die de bevoegdheid heeft om te bepalen hoe een bedrijfsproces verloopt, en de verantwoordelijkheid heeft ervoor te zorgen dat het bedrijfsproces aan de klantverwachtingen en bedrijfsbeleid en -doelstellingen blijft voldoen, vandaag en in de toekomst.
Voorbeeld: het financiële bedrijfsproces: de eigenaar van het financiële bedrijfsproces is de eigenaar van het financiële informatiesysteem, de financiële data (ook van financiële data die in een ander informatiesysteem dan het financiële informatiesysteem gebruikt worden).
Per bedrijfsproces is er één eigenaar.

4.6. Eigenaar data (datadomein)

Een eigenaar van data zorgt ervoor dat de gegevens volgens de geldende in- en externe regels worden verwerkt in het daarvoor bestemde informatiesysteem.
Voorbeeld: financiële domein: ook financiële data in een ander informatiesysteem dan het financiële systeem (bijv. binnen digitale campus) vallen onder eigenaarschap van de eigenaar van het financiële domein.
Bij gebruik van data in een systeem van een ander domein moeten de data eigenaren afspraken vastleggen welke data met wel doel in welk informatiesysteem verwerkt worden (leverancier – afnemer relatie)
Per domein is er één eigenaar.

4.7. Eigenaar informatie

Het verschil tussen data en informatie: data bestaat uit gegevens en informatie bestaat uit data die in een bepaalde c.q. relevante context geplaatst worden en daardoor betekenis en waarde hebben gekregen. Vanuit data wordt er iets waargenomen zonder dat er een betekenis aan de gegevens zit. Met andere woorden: Data zelf zijn de ruwe, onverwerkte gegevens in bijvoorbeeld datasets. Informatie is gestructureerde data in een nuttige c.q. relevante context.
Een eigenaar van informatie is de eigenaar van een bepaalde rapportage die informatie maakt van (ruwe) data. De eigenaar van informatie [als afnemer] moet afspraken maken met de data-eigenaar c.q. data-eigenaren [de data-leverancier(s)]. Deze afspraken moeten gebaseerd zijn op : wat-wie-welke-voor welk doel?
Er is één eigenaar per rapportage.

4.8. Eigenaar informatiesysteem

Een eigenaar van een informatiesysteem is verantwoordelijk voor het creëren en uitdragen van de productvisie en –strategie, eventueel via een gemandateerde product owner. Een eigenaar informatiesysteem:

- Moet ervoor zorgdragen dat het informatiesysteem geschikt blijft voor haar functie, conformeren aan belei van de OU en eventuele wettelijke verplichtingen.
- Kan een deel van zijn taken en bevoegdheden mandateren aan productowner(s) c.q. medewerkers.
- Is beslissingsbevoegd voor dat informatiesysteem en voor de toegang tot het informatiesysteem. Wijzigingen in het informatiesysteem of in de toegangsrechten tot het informatiesysteem vereisen de instemming van de eigenaar. De eigenaar controleert of het informatiesysteem en de toegangsrechten tot het informatiesysteem aan zijn eisen voldoen.
- Moet ervoor zorgdragen dat gegevens [in het informatiesysteem - data] volgens de geldende regels worden verwerkt.
- Verzorgt het budget voor de instandhouding van het informatiesysteem en voor de realisatie en controle van eventuele wijzigingen.

Er is één eigenaar per informatiesysteem.

4.9. Leidinggevende

Het creëren van bewustwording en de naleving van het Beleid is onderdeel van de integrale bedrijfsvoering. Iedere leidinggevende heeft de taak om:

- te zorgen dat zijn medewerkers op de hoogte zijn van het Beleid;
- toe te zien op de naleving van het Beleid door zijn medewerkers;
- periodiek het onderwerp privacy onder de aandacht te brengen in werkoverleggen.

Met leidinggevende wordt hier bedoeld: College van bestuur, decaan faculteit, directeur dienst, hoofd afdeling (en vergelijkbare functies), hoofd Bureau onderwijs en onderzoek (en vergelijkbare functies) conform de vigerende Autorisatieregeling Open Universiteit.

5. Implementatie Beleid

Het College van bestuur van de OU is verantwoordelijk voor Verwerkingen van Persoonsgegevens waarvan zij het doel en de middelen vaststelt. Zij wordt aangemerkt als de Verwerkingsverantwoordelijke in de zin van de AVG. De feitelijke Verwerking van Persoonsgegevens wordt echter op allerlei lagen van de OU uitgevoerd. Het goed, efficiënt en verantwoord leiden van een organisatie wordt vaak aangeduid met de term governance. Het omvat met name de relatie met de voornaamste belanghebbenden van de OU, zoals de eigenaren, werknemers, studenten, andere afnemers en de samenleving als geheel. Een goed corporate governance-beleid draagt zorg voor de rechten van alle Betrokkenen.

5.1. Verdeling van de verantwoordelijkheden

- Het zorgvuldig verwerken van Persoonsgegevens dient gezien te worden als een lijnverantwoordelijkheid: dat betekent dat de leidinggevenden (decanen, directeuren, (afdelings)hoofden, etc.) de primaire verantwoordelijk dragen voor een zorgvuldige Verwerking van Persoonsgegevens binnen hun faculteit c.q. op hun afdeling/ eenheid. Dit omvat ook de keuze van maatregelen, de uitvoering en handhaving ervan. Onder de lijnverantwoordelijkheid valt ook de taak om het beleid met betrekking tot de Verwerking van Persoonsgegevens te communiceren met de medewerkers die onder de verantwoordelijkheid van de leidinggevende vallen.

- Het zorgvuldig omgaan met Persoonsgegevens is ieders verantwoordelijkheid. Van medewerkers en studenten wordt verwacht dat ze zich integer gedragen. Niet acceptabel is dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/ of imagoverlies van de OU of van individuen. Het is om deze reden dat gedragscodes zijn geformuleerd en geïmplementeerd.

5.2. Inpassing in de instellingsgovernance / 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 onderdelen op elkaar af te stemmen, is het belangrijk om gestructureerd overleg te voeren over het onderwerp privacy op verschillende niveaus.

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 ingevuld in het MT-CvB-overleg.

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 in een periodiek overleg tussen de directeur ITF en de directeur HJI.

Op operationeel niveau worden de zaken besproken die de dagelijkse bedrijfsvoering (uitvoering) aangaan. Het operationeel niveau wordt ingevuld door de coördinatoren, hoofden en/of medewerkers van de diensten HJI en ITF.

5.3. Bewustwording en training

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van het verwerken van Persoonsgegevens uit te sluiten. Het is noodzakelijk om bij de OU het bewustzijn voortdurend aan te scherpen, zodat kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Onderdeel van het Beleid zijn de regelmatig terugkerende bewustwordingscampagnes voor medewerkers, studenten en gasten.

Deze campagnes kunnen aansluiten bij landelijke campagnes in het hoger onderwijs, zo mogelijk in afstemming met andere beveiligingscampagnes. Verhoging van het bewustzijn is de verantwoordelijkheid van de Functionaris Gegevensbescherming, de Privacyofficer en de Chief Information Security & Quality Officer.

5.4. Controle en naleving

Audits maken het mogelijk het Beleid en de genomen maatregelen te controleren op effectiviteit. De FG initieert gezamenlijk met de Chief Information Security & Quality Officer en de interne auditor de controle op het rechtmatig en zorgvuldig verwerken van Persoonsgegevens.

Eventuele externe controles worden uitgevoerd door onafhankelijke accountants en/of auditors. Dit is gekoppeld aan het jaarlijkse accountantsonderzoek en wordt zoveel mogelijk gecoördineerd met de normale Planning & Control cyclus.

Mocht de naleving op de bescherming van data- en privacygegevens ernstig tekortschieten, dan kan de OU de betrokken verantwoordelijke medewerkers een sanctie opleggen, binnen de wettelijke mogelijkheden.

Het verwerken van Persoonsgegevens is een continu proces. Technologische- en organisatorische ontwikkelingen binnen en buiten de OU maken het noodzakelijk om periodiek te bezien of men nog voldoende op koers zit met het Beleid.

6. Rechtmatige en zorgvuldige Verwerking van Persoonsgegevens

De OU verwerkt Persoonsgegevens in overeenstemming met de principes zoals uitgewerkt in paragraaf 2.1 van dit Beleid. Ter uitwerking van deze principes treft de OU de in dit hoofdstuk genoemde maatregelen.

6.1. Grondslag

De OU verwerkt slechts Persoonsgegevens als er sprake is van een van de wettelijke gronden zoals beschreven in artikel 6 van de AVG:

a. Toestemming van de Betrokkene.
b. Noodzakelijk voor de uitvoering van een overeenkomst met de Betrokkene.
c. Noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust.
d. Noodzakelijk om de vitale belangen van de Betrokkene of een ander natuurlijk persoon te beschermen.
e. Noodzakelijk voor de vervulling van een taak van algemeen belang of in het kader van uitoefening van openbaar gezag.
f. Noodzakelijk voor de behartiging van het gerechtvaardigd belang van de verwerkingsverantwoordelijke of een derde.

6.2. Privacyverklaring

De OU verwerkt Persoonsgegevens op een manier die ten aanzien van de Betrokkene behoorlijk en transparant is. Dit houdt in dat de OU aan de Betrokkene inzichtelijk maakt in hoeverre en op welke manier diens Persoonsgegevens verwerkt worden. Bij het verzamelen van de Persoonsgegevens zal de OU middels een privacyverklaring de Betrokkene inlichten. Inlichting zal plaatsvinden voorafgaand aan de Verwerking, tenzij dit redelijkerwijs niet mogelijk is. Zie nader paragraaf 8.1 van dit Beleid.

6.3. Bewaartermijnen

Persoonsgegevens worden niet langer bewaard dan noodzakelijk is voor de doeleinden waarvoor zij zijn verzameld of worden gebruikt, in overeenstemming met de Basisselectielijsten Universiteiten en Universitaire Medische Centra 2020 (inclusief voorgangers en opvolgers). Persoonsgegevens dienen na het verlopen van de bewaartermijn[5] buiten het bereik van de actieve administratie gebracht te worden. De OU zal de Persoonsgegevens na het verlopen van de bewaartermijn vernietigen of, indien de Persoonsgegevens bestemd zijn voor historische, statistische of wetenschappelijke doeleinden, in een archief bewaren.

6.4. Passende beveiligingsmaatregelen

De OU draagt zorg voor een adequaat beveiligingsniveau en legt passende technische- en organisatorische maatregelen ten uitvoer om Persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige Verwerking. Deze maatregelen zijn mede gericht op onnodige c.q. onrechtmatige verzameling en Verwerking van Persoonsgegevens te voorkomen. De OU heeft een intern beveiligingsbeleid geïmplementeerd waarin maatregelen zijn uitgewerkt die werknemers van de OU hanteren.

Een risicoanalyse op privacybescherming en informatiebeveiliging maakt deel uit van het intern risicobeheersings- en controlesysteem van de OU.

[5] Bewaartermijnen kunnen wettelijk zijn bepaald, zoals bij financiële gegevens of bij formele studieresultaten, maar ze kunnen ook zijn vastgelegd door de OU, b.v. in een overeenkomst tussen de OU en de Betrokkenen.

6.5. Documentatieplicht

De OU heeft meerdere maatregelen getroffen om aan te tonen en te voldoen aan de wettelijke eisen uit de AVG, waaronder implementatie van het onderhavige Beleid.

Daarnaast dient elke geheel of gedeeltelijk geautomatiseerde Verwerking van Persoonsgegevens gemeld te worden bij de FG van de OU. De FG beoordeelt de rechtsgeldigheid van de Verwerking en draagt zorg voor adequate documentatie van alle relevante gegevens.

Tevens voert de OU een Privacy Impact Assessment en/of DTIA uit, bij (onderzoeks)projecten, infrastructurele wijzigingen en/ of de aanschaf van nieuwe systemen die waarschijnlijk een hoog risico inhouden voor de rechten en vrijheden van natuurlijke personen. Als hieruit blijkt dat de Verwerking een hoog risico zou betekenen indien de OU geen maatregelen neemt om het risico te beperken, raadpleegt de OU voorafgaand aan de verwerking, de toezichthoudende autoriteit.

6.6. Privacy by Design en Privacy by Default

De OU hanteert bij de implementatie van iedere Verwerking de principes “Privacy by Design” en “Privacy by Default”.

Vanwege de aanzienlijke materiële risico’s is de risicoanalyse op privacybescherming en informatiebeveiliging opgenomen in de Governance Code van de OU en daarmee ondergebracht in het aandachtsgebied van de directeur Finance en control.

6.7. Geheimhouding

Bij de OU worden alle Persoonsgegevens als vertrouwelijk geclassificeerd. Eenieder behoort de vertrouwelijkheid van Persoonsgegevens te kennen en daarnaar te handelen.

Ook personen voor wie niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift een geheimhoudingsplicht geldt, zijn verplicht tot geheimhouding van de Persoonsgegevens waarvan zij kennisnemen, behoudens voor zover enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit.

6.8. Bijzondere Persoonsgegevens

Het verwerken van bijzondere Persoonsgegevens is in beginsel verboden, tenzij sprake is van een van de wettelijke uitzonderingen uit de AVG, waar onder meer ‘uitdrukkelijke toestemming van de Betrokkene’ en een ‘zwaarwegend algemeen belang’ onder vallen. Tevens gelden zwaardere eisen voor de beveiliging van deze bijzondere Persoonsgegevens. Daar waar de basisbescherming niet voldoende is moeten voor elk informatiesysteem individueel afgestemde extra maatregelen worden genomen.

Onder bijzondere Persoonsgegevens vallen de volgende gegevens:

- gegevens waaruit ras of etnische afkomst blijkt;
- politieke opvattingen;
- religieuze of levensbeschouwelijke overtuigingen;
- gegevens waaruit lidmaatschap van een vakbond blijkt;
- genetische gegevens met het oog op de unieke identificatie van een persoon;
- biometrische gegevens met het oog op de unieke identificatie van een persoon;
- gegevens over gezondheid;
- gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.

Voor twee soorten Persoonsgegevens geldt dat zij niet onder de categorie bijzondere Persoonsgegevens vallen, maar dat de Verwerking en beveiliging ervan wel aan strenge eisen zijn gebonden:

a. Verwerking van Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten mag slechts onder toezicht van de overheid of binnen Europese of nationale wetgeving.

b. Onder de Nederlandse wetgeving mag een nationaal identificatienummer (het BSN of het onderwijsnummer) alleen worden verwerkt als dat wettelijk is bepaald.

6.9. Doorgifte Persoonsgegevens

6.9.1. Uitbesteden van Verwerking aan een Verwerker

Indien de OU Persoonsgegevens laat verwerken door een Verwerker, wordt de uitvoering van Verwerkingen geregeld in een verwerkersovereenkomst, tussen de OU als de Verwerkingsverantwoordelijke en deze Verwerker.

6.9.2. Doorgifte Persoonsgegevens binnen de Europese Economische Ruimte (hierna 'EER')

De OU verstrekt Persoonsgegevens alleen aan een Verwerker gevestigd binnen de EER, als de verwerking is gebaseerd op een van de grondslagen voor gegevensverwerking uit artikel 6 of artikel 9 AVG en als de Verwerker voldoet aan de wettelijke vereisten uit de AVG.

6.9.3. Doorgifte Persoonsgegevens buiten de EER

De OU verstrekt Persoonsgegevens alleen aan Verwerkers die zich bevinden in een land buiten de EER, indien aan een van de volgende voorwaarden is voldaan:

1. Het derde land, gebied, welbepaalde sector in een derde land, of de internationale organisatie in kwestie biedt volgens de Europese Commissie een passend beschermingsniveau.

Als passend beschermingsniveau hanteert de OU:

- De algemene lijst van landen met passend beschermingsniveau gepubliceerd door de Europese Commissie[6].

2. Doorgifte vindt plaats op basis van passende waarborgen uit de artikelen 46 en 47 AVG.

3. Doorgifte vindt plaats op basis van een van de wettelijke uitzonderingen uit artikel 49 AVG.

6.10. Vragen- en klachtenprocedure

6.10.1. Melding en registratie

Vragen of klachten in verband met (de verwerking van) Persoonsgegevens kunnen gemeld worden. Studenten en Derden kunnen zich melden via info@ou.nl. Medewerkers kunnen zich melden bij de Privacyofficer (privacyofficer@ou.nl). Van vragen of klachten met een (potentiele) significante impact, zal een register bijgehouden worden.

Vragen en klachten kunnen worden gemeld door eenieder, waaronder Betrokkenen, Verwerkers of Derden.

[6] Deze kunt u vinden via de volgende link http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

6.10.2. Zwakke plekken in de beveiliging

Werknemers zullen waargenomen zwakke plekken in systemen of diensten registreren en direct rapporteren bij servicedesk@ou.nl. Van alle meldingen betreffende zwakke plekken in de beveiliging zal een register bijgehouden worden.

6.10.3. Afhandeling

Vragen, klachten en zwakke plekken in de beveiliging worden doorgezet naar de verantwoordelijke afdeling of persoon en vervolgens conform de daarvoor vastgestelde procedures zo snel mogelijk afgehandeld.
Als de Persoonsgegevens van Betrokkene(n) of de bedrijfsprocessen, de financiën of goede naam van de OU ernstig in gevaar zijn, wordt in ieder geval het College van bestuur en ook de FG en de woordvoerder op de hoogte gesteld. Desgewenst kan ook het Crisis Management Team (CMT) worden geraadpleegd.

6.10.4. Evaluatie

Het is van belang om te leren van de feedback die middels de vragen- en klachtenprocedure wordt geleverd. Registratie van significante vragen, klachten en zwakke plekken en een periodieke rapportage daarover horen thuis bij een professionele manier van verwerken van Persoonsgegevens. De rapportage hierover maken daarom een vast onderdeel uit van de jaarrapportage van het College van bestuur en die van de FG.

7. Datalek

Dit hoofdstuk beschrijft het beleid met betrekking tot de melding, registratie en afhandeling van een Datalek of het vermoeden van een Datalek in de reguliere bedrijfsvoering en in bijzondere omstandigheden.

7.1. Datalek

Van een Datalek is sprake als een inbreuk op de beveiliging van Persoonsgegevens plaatsvindt, die leidt tot enige ongeoorloofde Verwerking daarvan. Het kan hierbij bijvoorbeeld gaan om een hack/ransomware aanval, een diefstal van een laptop, een in de trein vergeten usb-stick of een e-mail die naar de verkeerde persoon is verstuurd. Datalekken moeten worden gemeld bij de toezichthouder binnen 72 uur na ontdekking daarvan en in sommige gevallen ook bij de Betrokkene.

7.2. Melding en registratie

Een Datalek kan bij de OU zowel binnen de eigen organisatie ontstaan, maar ook bij een door de OU ingeschakelde Verwerker. De volgende situaties moeten hierbij worden onderscheiden:

a. Medewerker: medewerkers moeten, indien zij een (mogelijk) Datalek waarnemen of vermoeden zelf onderdeel te zijn van een Datalek, contact opnemen met servicedesk@ou.nl en fg@ou.nl.
b. Verwerker*:* het is ook mogelijk dat een Datalek plaatsvindt bij een door de OU ingeschakelde Verwerker. De Verwerker zal overeenkomstig de afgesloten verwerkersovereenkomst het Datalek melden aan de OU via servicedeskk@ou.nl.
c. Andere personen: indien een ander dan een medewerker of een Verwerker een (mogelijk) Datalek waarneemt of zelf onderdeel is van een Datalek of een Datalek heeft veroorzaakt, dient contact opgenomen te worden met servicedesk@ou.nl en fg@ou.nl.

Een melding van een (mogelijk) Datalek dient zo spoedig mogelijk te worden gemaakt. De volgende gegevens dienen doorgegeven te worden bij melding van een Datalek:

- Wie heeft gemeld?
- Wat is gemeld?
- Waar kwam de melding vandaan?
- Om welke data (gegevens) gaat het?
- Hoe heeft het incident plaatsgevonden?
- Welke systemen zijn betrokken bij/geraakt door het incident?
- Wanneer heeft het incident plaatsgevonden?
- Indien de melding is gedaan door een medewerker van de OU: wat is gedaan om het incident op te lossen/ in de toekomst te voorkomen?

Elk Datalek en de afhandeling daarvan zal worden bijgehouden in een register.

7.3. Afhandeling

Indien sprake is van een Datalek wordt deze conform de in de relevante wet- en regelgeving opgenomen specifieke bepalingen over Datalekken afgehandeld, zoals beschreven in de beleidsregels meldplicht datalekken van de Autoriteit Persoonsgegevens[7]. De melding van het Datalek dient tijdig de juiste personen, en uiteindelijk de toezichthouder en Betrokkenen te bereiken.

Als de Persoonsgegevens van Betrokkene(n) of de bedrijfsprocessen, de financiën of goede naam van de OU ernstig in gevaar zijn, wordt in ieder geval het College van bestuur en indien aanwezig ook de FG en de woordvoerder op de hoogte gesteld.

7.4. Besluitvorming

Nadat een melding heeft plaatsgevonden van een (mogelijk) Datalek overeenkomstig de voorgaande paragrafen, zal de FG een advies uitbrengen omtrent de verplichting om te melden aan de toezichthoudende autoriteit en de Betrokkene. Dit advies zal door het College van bestuur en de Gemandateerde in overweging worden genomen. Het College van bestuur zal verantwoordelijk zijn voor het besluit om al dan niet de melding te doen.

7.5. Evaluatie

Het is van belang om te leren van Datalekken om de waarschijnlijkheid van toekomstige Datalekken te verkleinen. Registratie van Datalekken en een periodieke rapportage daarover horen thuis bij een professionele manier van verwerken van Persoonsgegevens. De rapportage over Datalekken met betrekking tot Persoonsgegevens maken daarom een vast onderdeel uit van de jaarrapportage van het College van bestuur en van de FG.

[7] Beleidsregels meldplicht datalekken van de Autoriteit Persoonsgegevens:
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/richtsnoeren_meldplicht_datalekken_0.pdf

8. Rechten van Betrokkenen

De AVG geeft Betrokkenen bepaalde rechten waarmee zij controle kunnen uitoefenen op de Verwerking van hun Persoonsgegevens. Een verzoek kan schriftelijk worden ingediend bij info@ou.nl. Medewerkers kunnen zich hiervoor het beste melden bij hun leidinggevende.

Voor alle in dit hoofdstuk uitgewerkte rechten van Betrokkenen gelden de volgende punten:

- **Melding aan Betrokkene**

De OU draagt zorg dat de informatie en communicatie op een beknopte, toegankelijke en begrijpelijke manier en in duidelijke en eenvoudige taal wordt verstrekt aan Betrokkene. De taal zal worden afgestemd op de doelgroep.

- **Termijn**

Op een verzoek van een Betrokkene wordt zo spoedig mogelijk, doch uiterlijk binnen vier weken na indiening schriftelijk gereageerd. Hierbij zal de Betrokkene in ieder geval in kennis worden gesteld over het gevolg dat aan het verzoek is gegeven. Indien de termijn van vier weken redelijkerwijs niet haalbaar is, zal Betrokkene daarvan binnen deze termijn op de hoogte worden gesteld. De OU zal in dat geval binnen twee maanden na het verstrijken van de eerste termijn gevolg geven aan het verzoek van de Betrokkene.

- **Identiteit Betrokkene**

De OU draagt bij het verstrekken van de betreffende informatie zorg voor een deugdelijke vaststelling van de identiteit van de verzoeker. Hiertoe kan de OU extra informatie verzoeken.

- **Minderjarigen**

Een verzoek tot uitoefening van een van de rechten zoals uitgewerkt in dit hoofdstuk door een Betrokkene, zijnde Minderjarig, onder curatele gesteld of ten behoeve van wie een bewind of mentorschap is ingesteld, geschied door diens wettelijk vertegenwoordiger. Een reactie door de OU zal ook naar deze wettelijke vertegenwoordiger worden verstuurd.

8.1. Recht op informatie

De Betrokkene heeft het recht om door de OU te worden geïnformeerd over bepaalde aspecten van de Verwerking van zijn Persoonsgegevens. De OU informeert de Betrokkene kosteloos over de Verwerking van diens Persoonsgegevens, zowel in de situatie waarin de Persoonsgegevens direct bij de Betrokkene zijn verzameld, als wanneer ze langs een andere route zijn verkregen.

A. Verkrijging direct van Betrokkene

De OU verstrekt de Betrokkene voorafgaand aan de verzameling van de gegevens, tenminste de volgende informatie indien de gegevens direct bij de Betrokkene worden verzameld:

- De identiteit en contactgegevens van de Verwerkingsverantwoordelijke en, in voorkomend geval, de FG.
- De specifieke doeleinden van Verwerking waarvoor de Persoonsgegevens zijn bestemd alsook de rechtsgrond voor de verwerking.
- De gerechtvaardigde belangen van de Verwerkingsverantwoordelijke of Derde als de Verwerking is gebaseerd op de rechtsgrond ‘gerechtvaardigd belang’.
- In voorkomend geval, het voornemen van de Verwerkingsverantwoordelijke om de Persoonsgegevens door te geven aan een derde land, welk land dit is en op welke grond de Persoonsgegevens daarnaartoe worden verstuurd.
- De periode gedurende welke de Persoonsgegevens worden opgeslagen, of indien niet mogelijk, de criteria die dienen om deze termijnen te bepalen.

- Het bestaan van het recht om de Verwerkingsverantwoordelijke te verzoeken om inzage, rectificatie of wissen van de Persoonsgegevens, beperking van de hem betreffende verwerking, alsmede het recht tegen de Verwerking bezwaar te maken en het recht op dataportabiliteit.
- Het recht om een klacht in te dienen bij de toezichthoudende autoriteit.
- De ontvangers of categorieën van ontvangers van de Persoonsgegevens.
- Indien de Verwerking is gebaseerd op de grondslag 'toestemming', het recht van de Betrokkene om die toestemming te allen tijde in te trekken.
- Of de Persoonsgegevens nodig zijn voor de uitvoering van een overeenkomst of om te voldoen aan een wettelijke verplichting.
- Of de Persoonsgegevens mede worden gebruikt voor geautomatiseerde besluitvorming. Tevens moet de onderliggende logica, alsmede het belang en de te verwachte gevolgen van de Verwerking voor de Betrokkene worden gemeld.

B. Verkrijging niet direct van Betrokkene

Als de Persoonsgegevens niet direct bij de Betrokkene zelf zijn verzameld maar langs een andere route, zal aan de Betrokkene, in aanvulling op de hiervoor genoemde punten, de volgende informatie worden verstrekt:

- De categorieën van Persoonsgegevens.
- De bron waar de Persoonsgegevens vandaan komen.

Deze informatie zal zo snel mogelijk, maar niet later dan vier weken, na verkrijging van de gegevens, dan wel bij het eerste contact met de Betrokkene, worden verstrekt.

8.2. Recht op inzage

- *Verzoek*

Iedere Betrokkene heeft het recht om te informeren of zijn Persoonsgegevens worden verwerkt en, als dat het geval blijkt, het recht op inzage in hem betreffende verwerkte Persoonsgegevens.

- *Mededeling*

Indien gegevens worden verwerkt, bevat de mededeling van de OU een volledig overzicht van de volgende gegevens:

- Een omschrijving van de doeleinden van de Verwerking.
- De categorieën van gegevens waarop de Verwerking betrekking heeft.
- Categorieën van ontvangers.
- Beschikbare informatie over herkomst van de gegevens.
- De termijn van bewaring van gegevens of indien dat niet mogelijk is, de criteria om die termijn te bepalen.
- Het recht van Betrokkene om de Verwerkingsverantwoordelijke te verzoeken om rectificatie of wissen van gegevens, beperking of bezwaar van Verwerking alsmede het recht op dataportabiliteit.
- Het recht van de Betrokkene om een klacht in te dienen bij een toezichthoudende autoriteit.
- Alle beschikbare informatie over de bron van de gegevens, als de gegevens niet bij de Betrokkene zijn verzameld.
- Of de Persoonsgegevens mede worden gebruikt voor geautomatiseerde besluitvorming. Tevens moet de onderliggende logica, alsmede het belang en de verwachte gevolgen van de Verwerking voor de Betrokkene worden gemeld.
- De passende waarborgen die zijn getroffen, indien de gegevens worden doorgegeven aan een derde land.

- *Kopie*

De Betrokkene kan om een kopie van alle Persoonsgegevens verzoeken. Deze kopie dient in een gangbare elektronische vorm te worden verstrekt, tenzij het verzoek op papier is gedaan of de Betrokkene expliciet om een papieren kopie verzoekt.

- *Kosten*

Ieder kopie kan kosteloos worden aangevraagd.

- *Rechten en vrijheden van anderen*

De OU zal bij verstrekking van de gegevens rekening houden met de rechten en vrijheden van anderen.

8.3. Recht op dataportabiliteit

- *Gronden voor verzoek*

Iedere Betrokkene kan een verzoek indienen bij de OU om (kosteloos) zijn gegevens te verkrijgen in een gestructureerde, gangbare en machine leesbare vorm dan wel deze rechtstreeks aan een andere Verwerkingsverantwoordelijke over te laten dragen, zonder daarbij te worden gehinderd door de OU indien is voldaan aan de volgende voorwaarden:

1. De Verwerking door de OU berust op de grondslag ‘toestemming’ dan wel ‘uitvoering van een overeenkomst met de Betrokkene’.
2. De Verwerking in kwestie is geheel geautomatiseerd.

- *Rechten en vrijheden van anderen*

De OU zal bij verstrekking van de gegevens rekening houden met de rechten en vrijheden van anderen.

- *Verwijderen van gegevens*

Indien een Betrokkene zijn recht van dataportabiliteit heeft uitgeoefend in het kader van een Verwerking ter uitvoering van een overeenkomst, mag de OU niet besluiten de gegevens te wissen. Na het verstrijken van de bewaartermijn, dient de OU de gegevens echter alsnog te wissen.

Indien het recht is uitgeoefend in het kader van een Verwerking op grond van toestemming van de Betrokkene, mag de OU wel besluiten om de gegevens te wissen na uitoefenen van het recht.

8.4. Recht op rectificatie, aanvulling, verwijdering of beperking van de Verwerking

- *Verzoek tot rectificatie, aanvulling, verwijdering of beperking*

Iedere Betrokkene kan met betrekking tot over hem opgenomen Persoonsgegevens bij de OU van deze gegevens verzoeken die te corrigeren, aan te vullen, te verwijderen of de Verwerking te beperken. Bij het recht op beperking worden de Persoonsgegevens tijdelijk afgeschermd en niet meer verwerkt door de OU. De beperking wordt duidelijk in het bestand aangegeven.

- *Kennisgeving*

Indien blijkt dat de opgenomen Persoonsgegevens van de Betrokkene feitelijk onjuist zijn, voor het doel of doeleinden van de Verwerking onvolledig of niet ter zake dienend zijn dan wel anderszins in strijd met een wettelijk voorschrift zijn verwerkt, zal de OU als Verwerkingsverantwoordelijke deze gegevens verbeteren, permanent verwijderen, aanvullen dan wel beperken. Indien sprake is van een Verwerker zal de OU hem deze opdracht verstrekken.

Derden aan wie de gegevens zijn verstrekt, worden voorafgaand aan de rectificatie, aanvulling, verwijdering dan wel beperking hiervan in kennis gesteld, tenzij dit redelijkerwijs niet mogelijk of gezien de omstandigheden niet relevant is. De verzoeker mag opgave verzoeken van degene aan wie de OU deze mededeling heeft gedaan.

- *Termijn voor uitvoering*

De OU als Verwerkingsverantwoordelijke zorgt ervoor dat een beslissing tot verbetering, aanvulling, verwijdering of afscherming zo spoedig mogelijk wordt uitgevoerd. De uitvoering hiervan geschiedt kosteloos voor de Betrokkene.

8.5. Recht van bezwaar

- *Gronden voor bezwaar*

Voor Betrokkenen bestaan twee gronden om bezwaar te maken tegen een Verwerking:

1. In verband met zijn of haar persoonlijke omstandigheden, mag iedere Betrokkene bezwaar maken tegen Verwerking bij de OU, als deze Verwerking plaatsvindt op grond van a) de vervulling van een taak van algemeen belang of in het kader van de uitoefening van het openbaar gezag van de Verwerkingsverantwoordelijke, of b) de behartiging van het gerechtvaardigd belang van de OU of van een Derde aan wie de gegevens worden verstrekt. Zie voor een beschrijving van de grondslagen, paragraaf 6.1.

   De OU zal bij bezwaar de verdere Verwerking in beginsel staken. Indien de OU kan aantonen dat zijn dwingende gerechtvaardigde belangen zwaarder wegen dan de belangen of grondrechten en de fundamentele vrijheden van de Betrokkene, zal de Verwerking worden voortgezet. Indien het bezwaar gerechtvaardigd is, treft de OU (kosteloos) maatregelen die nodig zijn om de Persoonsgegevens voor de betreffende doeleinden niet meer te verwerken.

2. Bij een Verwerking met het doel ‘direct marketing’, heeft een Betrokkene te allen tijde het recht om bezwaar te maken. De OU zal bij bezwaar de Verwerking voor direct marketing doeleinden direct (kosteloos) staken en gestaakt houden.

8.6. Geautomatiseerde besluitvorming

Gronden
Betrokkenen hebben het recht om niet onderworpen te worden aan een uitsluitend op geautomatiseerde Verwerking gebaseerd besluit, waaraan voor hem rechtsgevolgen zijn verbonden. Onder een ‘besluit gebaseerd op een geautomatiseerde Verwerking’ wordt verstaan een besluit dat is gemaakt zonder menselijke tussenkomst. Hieronder valt onder andere Profilering.

Slechts in de volgende drie situaties mag de OU besluiten nemen op grond van geautomatiseerde Verwerking:

1. Indien het besluit noodzakelijk is bij de sluiting of uitvoering van een overeenkomst met de Betrokkene.
2. Indien het besluit is toegestaan bij een Europese of nationale wet, mits deze wet voorziet in passende maatregelen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de Betrokkene.
3. Indien het besluit berust op uitdrukkelijke toestemming van de Betrokkene. Deze toestemming kan te allen tijde worden ingetrokken.

In alle hierboven beschreven situaties, zal de OU passende maatregelen nemen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de Betrokkene. Hieronder zullen tenminste vallen het recht op menselijke tussenkomst door de OU, het recht van de Betrokkene om zijn standpunt kenbaar te maken, alsmede het recht om het besluit aan te vechten. Minderjarigen zullen nimmer worden onderworpen aan geautomatiseerde besluitvorming.

8.7. Rechtsbescherming

- *Algemene klachten*

Indien de Betrokkene van mening is dat de wettelijke bepalingen inzake de privacybescherming dan wel de bepalingen van dit reglement jegens hem niet correct worden gehandhaafd, kan hij een schriftelijke klacht indienen bij de OU via fg@ou.nl.

- *Overige bezwaarmogelijkheden*

Naast de algemene interne klachtenprocedure zoals hierboven beschreven, heeft de Betrokkene de volgende mogelijkheden als hij het idee heeft dat de OU een hem rakende overtreding van de AVG heeft begaan:

A. <u>Verzoekschriftprocedure bij de kantonrechter</u>

Indien de OU afwijzend heeft beslist op een verzoek zoals beschreven in paragraaf 8.1 t/m 8.6 van dit Beleid, of de OU heeft het verzoek van de Betrokkene afgewezen, heeft de Betrokkene de mogelijkheid een verzoekschriftprocedure te starten bij de kantonrechter.

Het verzoekschrift dient binnen zes weken na ontvangst van het antwoord van de OU ingediend te worden bij de kantonrechter. Indien de OU niet binnen de gestelde termijn heeft geantwoord op het verzoek van Betrokkene, moet het verzoekschrift binnen zes weken na afloop van die termijn worden ingediend. Indiening van het verzoekschrift hoeft niet door een advocaat te geschieden.

B. <u>Bezwaar en beroep</u>

Indien de OU afwijzend heeft beslist op een verzoek zoals beschreven in paragraaf 8.1 t/m 8.6 van dit Beleid, of de OU heeft het verzoek van de Betrokkene afgewezen, en het besluit van de OU is aan te merken als een besluit van een bestuursorgaan in de zin van artikel 6 lid 4 van de Awb, heeft de Betrokkene de mogelijkheid een bezwaarschriftprocedure te starten. Een bezwaarschriftprocedure moet altijd gestart worden binnen 6 weken na bekendmaking van een besluit van de OU. Tegen de beslissing op bezwaar, staat beroep open bij de rechtbank.

C. <u>Verzoek tot handhaving bij toezichthoudende autoriteit</u>

Indien de OU afwijzend heeft beslist op een verzoek zoals beschreven in paragraaf 8.1 t/m 8.6 van dit Beleid, of de OU heeft het verzoek van de Betrokkene afgewezen, heeft de Betrokkene de mogelijkheid om een klacht in te dienen bij een toezichthoudende autoriteit, dan wel om een belangenorganisatie namens hem op te laten treden.

9. Tot slot

Dit beleid is vastgesteld door het College van bestuur van de Open Universiteit op 26 september 2023 met instemming van de Ondernemingsraad d.d. 20 september 2023 en na verkregen advies van de Studentenraad d.d. 18 september 2023.

Dit beleid wordt samen met het Informatiebeveiligingsbeleid periodiek geëvalueerd. Indien nodig wordt het beleid aangepast en opnieuw door het College van bestuur vastgesteld, na raadpleging van de Ondernemingsraad.

Voor vragen of opmerkingen met betrekking tot dit beleid kunt u terecht bij de Privacyofficer (privacyofficer@ou.nl).

Beleid informatieveiligheid

Definitief

Open Universiteit

document

identificatie	U2023 3560 Beleid verwerking p-gegevens_informatieveiligheid v1.0.0 (vastgesteld).docx
status	Definitief
auteur(s)	Martin Romijn
eigenaar	Directeur ITF
datum afdruk	5 oktober 2023
opgeslagen	https://openuniversiteit.sharepoint.com/sites/P_Beleid_Informatieveiligheid/Gedeelde documenten/Beleid/Definitief/U2023 3560 Beleid verwerking p-gegevens_informatieveiligheid v1.0.0 (vastgesteld).docx

wijzigingshistorie

versie	auteur	datum	wijziging	review
	MR1	09-06-2021	De SCIPR-model-IB-beleid-3.0-final tekst overgezet naar OU format	
01	MR1	16-06-2021	Het SCIPR modelbeleid passend gemaakt op de OU situatie	
02	MR1	20-10-2021	Feedback Judith verwerkt	
03	MR1	12-01-2022	Nieuwste keuzes HJI/ITF overleg aangebracht	
081	MR1	6-7-2022	Feedback MT ITF (met name Hilde) verwerkt	
090	MR1	25-8-2022	Feedback gemarkeerd	
095	MR1	18-10-2022	Feedback Hilde, wijzigingen Judith en vragen Jan verwerkt	
096	MR1	27-10-2022	De beveiliging van webapplicaties specifiek benoemd	
099	MR1	02-05-2023	Finale eindredactie voor aanbieding Cvb	
1.0	MR1	05-10-2023	Versienummer, vaststellingsgegevens via JNI	

Colofon

Beleid informatieveiligheid OU Versie 1.0.0 (2023)

Vervangt Informatiebeveiligings- en privacybeleid v24

Auteur: Martin Romijn, CISO, ITF

Dit beleid is vastgesteld door het College van bestuur van de Open Universiteit op 26 september 2023 met instemming van de Ondernemingsraad d.d. 20 september 2023 en na verkregen advies van de Studentenraad d.d. 18 september 2023.

Open Universiteit

Inhoudsopgave Beleid Informatieveiligheid

Samenvatting

Het succes van een organisatie hangt in hoge mate af van informatie, nieuwe technologieën en computersystemen. Die informatie moet goed worden beveiligd, zeker als er persoonsgegevens worden opgeslagen. In dit document is verwoord op welke manier de Open Universiteit (OU) voorziet in adequate informatiebeveiliging en daarmee voldoet aan de relevante wet- en regelgeving.
Met het informatiebeveiligingsbeleid wil de OU ook bijdragen aan een betere kwaliteit van de informatievoorziening en zorgen voor een juiste balans tussen functionaliteit, veiligheid en privacy.

Beschreven wordt op wie, op welke onderdelen van de instelling en op welke apparaten en applicaties het beleid van toepassing is. Informatiebeveiliging werkt door in alle lagen van de organisatie. Naast de reikwijdte van het beleid worden de verantwoordelijkheden van de betrokken functionarissen beschreven. Het lijnmanagement is verantwoordelijk voor haar eigen processen, de directie zorgt ervoor dat beveiligingsmaatregelen daadwerkelijk worden geïmplementeerd. Eindverantwoordelijkheid ligt bij het College van bestuur.

Vijf beleidsprincipes zijn leidend, namelijk:

1. *Risico-gebaseerd*
   We baseren de maatregelen op de mogelijke veiligheidsrisico's van onze informatie, processen en IT-faciliteiten.
2. *Iedereen*
   Iedereen is en voelt zich verantwoordelijk voor een juist en veilig gebruik van middelen en bevoegdheden.
3. *Altijd*
   Informatiebeveiliging zit in het DNA van al onze werkzaamheden.
4. *Security by Design*
   Informatiebeveiliging is vanaf de start een integraal onderdeel van ieder project of iedere verandering m.b.t. informatie, processen en IT-faciliteiten.
5. *Security by Default*
   Gebruikers hebben alleen toegang tot informatie en IT-faciliteiten die zij nodig hebben voor hun werkzaamheden. Het openstellen van informatie is een bewuste keuze.

Beleid en maatregelen alleen zijn niet voldoende om risico's op het terrein van informatiebeveiliging te mitigeren. Bij de OU werken we daarom voortdurend aan het vergroten van het beveiligingsbewustzijn van medewerkers en studenten om kennis van risico's te verhogen en veilig en verantwoord gedrag aan te moedigen.

Informatiebeveiliging is een continu proces, waarbij we steeds kijken naar mogelijke verbeteringen. Dit gebeurt onder andere door jaarplannen, controles en bijsturing. Naast informatiebeveiligingsfunctionarissen kunnen de Functionaris Gegevensbescherming en de interne auditor hier bijvoorbeeld adviezen voor geven.

In de bijlagen is aandacht voor de managementcyclus voor periodieke bijstelling inclusief de documenten die hiervoor van belang zijn op het gebied van informatiebeveiliging. De vijf beleidsprincipes voor informatiebeveiliging zijn in de bijlage volledig uitgewerkt. Daarnaast is een overzicht gegeven van de belangrijkste wet- en regelgeving rondom informatiebeveiliging en worden de rollen van betrokken functionarissen verhelderd.

1. Inleiding

Het succes van de OU hangt in hoge mate af van informatie, nieuwe technologieën en computersystemen. We kunnen niet meer zonder het digitaal verzamelen, vastleggen en delen van informatie met zowel interne als externe partners, collega's en studenten.

De digitale werkelijkheid is constant in beweging en dat brengt steeds nieuwe en andere risico's met zich mee voor de Informatieveiligheid[8]. De risico's vormen een bedreiging voor de kwaliteit en continuïteit van processen en voor het behalen van de strategische doelen. De bedreigingen kunnen de beschikbaarheid, integriteit en vertrouwelijkheid van informatie beïnvloeden. Voorbeelden van bedreigingen zijn kwetsbaarheden in systemen of ongeautoriseerde toegang tot informatie. Dit kan de waarde van een OU-diploma/certificaat, behaalde cijfers of de legitimiteit van onderzoekconclusies ondermijnen.
Ook de privacy[9] van studenten, medewerkers en gasten (waaronder belangstellenden) en de reputatie van de OU kunnen worden geschaad. Informatiebeveiliging is daarom van cruciaal belang.

Informatiebeveiliging vraagt steeds om bijstelling zodat er een passend beveiligingsniveau blijft. Dat komt onder andere door de technologische ontwikkelingen, de aangescherpte eisen om te voldoen aan de wet- en regelgeving rondom gegevensbescherming en privacy (AVG), en de afspraken met onderzoek- en onderwijspartners.

Het verkleinen en beheersen van de risico's vraagt om inspanningen op organisatorisch, procesmatig en technologisch vlak. Daarnaast moeten medewerkers, leidinggevenden, studenten en gasten (waaronder belangstellenden) van de OU zich ook bewust worden van de risico's en hun handelen daarop afstemmen.

Informatieveiligheid is niet te bereiken door alleen een aantal technische en organisatorische maatregelen vast te stellen. Door de veranderende wereld is het een dynamisch proces. In dit document zijn om die reden vijf hoofdprincipes leidend voor informatiebeveiliging binnen de OU. De vast te stellen maatregelen, procedures en richtlijnen kunnen getoetst worden aan de vijf hoofdprincipes die in hoofdstuk 3 zijn beschreven.

Er is een belangrijke relatie tussen informatiebeveiligingsrisico's en risico's op andere gebieden, zoals met name de domeinen privacy, safety[10] (arbowetgeving), veiligheid in onderwijs en onderzoek, fysieke beveiliging en bedrijfscontinuïteit. Soms overlappen ze elkaar gedeeltelijk. Afstemming vindt dan plaats met de domeinverantwoordelijke.

1.1 Definities

De definities zijn opgenomen in het separate document "Definities begrippen", opgenomen in de Teams map met de beleidsdocumenten informatieveiligheid.

1.2 Informatieveiligheid en Informatiebeveiliging

De begrippen informatieveiligheid en informatiebeveiliging worden vaak door elkaar gebruikt, maar ze hebben niet dezelfde betekenis. Informatieveiligheid richt zich op het beschikbaar, integer en vertrouwelijk

[8] Zie toelichting paragraaf 3.1 over verschillen in de definities 'informatieveiligheid' en 'informatiebeveiliging'
[9] Voor het specifieke Privacy beleid zie ook https://www.ou.nl/privacy
[10] *Safety* wordt als verzamelterm gebruikt voor de verschillende aspecten van personele veiligheid: Arbo en milieu, sociale veiligheid, bedrijfshulpverlening e.d.

houden van informatie. Hiervoor moeten informatie en informatiesystemen beschermd worden tegen mogelijke bedreigingen. Dit wordt gedaan door het nemen, onderhouden en controleren van beveiligingsmaatregelen, ook wel informatiebeveiliging genoemd.

De eindverantwoordelijkheid voor informatieveiligheid ligt bij het College van bestuur van de OU.

2. Wet- en regelgeving

De OU streeft ernaar om in al haar processen en procedures te (blijven) voldoen aan de relevante wet- en regelgeving. Dit doet zij op basis van het principe “Pas toe of leg uit”, waardoor de OU altijd kan verantwoorden waarom zij wel of niet voldoet. In bijlage D is een overzicht opgenomen van de relevante wet- en regelgeving.

3. Doelstelling, doelgroep en reikwijdte

3.1 Doelstelling, randvoorwaarden en uitgangspunten

Informatiebeveiliging heeft de volgende doelen:

- Het waarborgen van de beschikbaarheid van informatie van het onderwijs, onderzoek en de bedrijfsvoering.
- Het waarborgen dat informatie juist, volledig en actueel is (integriteit) en alleen toegankelijk is voor personen die vanuit hun rol/functie daar toegang tot mogen hebben (vertrouwelijkheid).
- Het voorkomen van beveiligings- en privacy-incidenten en de eventuele gevolgen hiervan verminderen.

Met het informatiebeveiligingsbeleid (IB-beleid) wil de OU bijdragen aan een betere kwaliteit van de informatievoorziening en zorgen voor een juiste balans tussen functionaliteit, veiligheid en privacy en uiteraard de daarmee samenhangende kosten. Het IB-beleid sluit daarmee aan bij de missie van de instelling.

De OU heeft de ambitie om met behulp van dit beleidsdocument de informatieveiligheid structureel boven volwassenheidsniveau 3 (https://www.surf.nl/normenkader-surfaudit-audit-je-informatiebeveiliging) te opereren en daar te houden. Dit doet zij onder meer door het beschrijven van verantwoordelijkheden, taken en bevoegdheden en concrete doorvertaling van wet- en regelgeving.

Het IB-beleid, en de opvolging daarvan, moet de OU in staat stellen ‘in control’ en compliant te zijn. Op basis daarvan kunnen de betrokken decanen en directeuren samen met het College van bestuur verantwoording afleggen aan de Raad van toezicht. De uitvoering van het beleid is de basis is om te voldoen aan wettelijke voorschriften.

Randvoorwaarden
Om deze doelstellingen te kunnen bereiken zijn de volgende randvoorwaarden voor de OU van belang:

- *Beveiligingsorganisatie*
  De verantwoordelijkheden, taken en bevoegdheden van de informatiebeveiligingsfunctie zijn expliciet vastgelegd en worden gedragen door het bestuur, en afgeleid daarvan, door de hele instelling.
- *Procesbenadering*
  Informatiebeveiliging is een continu proces. Periodiek worden er risicoanalyses en audits uitgevoerd. De resultaten hiervan worden opgenomen in vastgestelde jaarplannen met duidelijke keuzes in beveiligingsmaatregelen. De uitvoering van deze beveiligingsmaatregelen wordt periodiek gecontroleerd vanuit de eerste, tweede en derde lijn.

Uitgangspunten
Uit de doelstelling en de randvoorwaarden komen de volgende uitgangspunten voort:

- *Kader*
  Het beleid biedt een kader om (toekomstige) maatregelen in de informatiebeveiliging te toetsen aan de vastgestelde beveiligingsprincipes (hoofdstuk 4), best practices en normen. Daarnaast biedt het een kader om de taken, bevoegdheden en verantwoordelijkheden in de instelling te beleggen.
- *Normen*
  Specifiek voor de SURF gemeenschap is het 'SURF Normenkader Informatie Beveiliging Hoger Onderwijs' (IBHO) [11] vastgesteld. Het IBHO is gebaseerd op de normen die zijn vastgelegd in de ISO-27000-serie. Het IBHO vormt samen met dit beleidsdocument de basis voor een informatiebeveiligingsmanagementsysteem (ISMS[12], zie bijlage A) van de OU. Het ISMS is ingericht op basis van de internationale standaard ISO 27001. Formele certificering, bijvoorbeeld volgens de norm ISO 27001, wordt niet als noodzakelijk gezien voor de OU.
- *Volwassenheid*
  IBHO omschrijft een norm voor de volwassenheid van de Informatiebeveiliging volgens het Capability Maturity Model[13]. De OU streeft naar een volwassenheidsniveau volgens de SURF-richtlijnen.
- *Maatregelen*
  De OU neemt maatregelen op basis van de internationaal vastgestelde ISO-27002-standaard. Hierbij worden de 'SURF Baseline Informatie Beveiliging Hoger Onderwijs' en overige best practices in de SURF-gemeenschap als uitgangspunt genomen. De specifieke basismaatregelen voor de OU zijn beschreven in het document Baseline informatiebeveiliging op https://mijn.ou.nl/group/mdw/-/informatiebeveiliging-en-privacy.

3.2 Doelgroep

Het IB-beleid is bestemd voor iedereen die – intern of extern – te maken heeft met de bedrijfsprocessen van de OU. Het beleid richt zich in eerste instantie op het bestuur, hoger management, de beveiligingsorganisatie en de leidinggevenden. Zij dragen uit dat het beleid van toepassing is op alle medewerkers, studenten, gasten (waaronder belangstellenden), bezoekers en externe relaties.

3.3 Reikwijdte van het beleid

Bij de OU wordt informatieveiligheid breed geïnterpreteerd. Het gaat over alle vormen van formeel vastgelegde informatie (dus niet alleen digitale informatie) die de instelling of haar relaties genereren en beheren. Daarnaast heeft het beleid betrekking op niet-formeel vastgelegde informatie, zoals uitspraken van studenten en medewerkers in discussies, op webpagina's en persoonlijke websites, waarop men de OU kan aanspreken.

Het IB-beleid heeft betrekking op alle instellingsonderdelen en -dienstverlening. Het gaat over alle apparaten en (web)applicaties waarmee geautoriseerde toegang tot (diensten van) het OU-netwerk kan worden verkregen en/of waarmee data van de instelling wordt verwerkt.

Onder apparaten en applicaties vallen:

---

[11] De actuele documenten zijn te vinden op https://www.surf.nl/informatiebeveiliging en https://www.surf.nl/surfaudit-inzicht-in-je-informatiebeveiliging-en-privacy en voor SCIPR-leden op de ondersteunende wiki's https://wiki.surfnet.nl/display/SCIPR/SCIPR+Home en https://wiki.surfnet.nl/display/SA/SURFaudit+Home
[12] ISMS: Information Security Management System.
[13] https://nl.wikipedia.org/wiki/Capability_Maturity_Model

- Alle fysiek op het netwerk aangesloten apparaten zoals servers, werkstations (waaronder laptops), gebouwbeheerssystemen.
- Alle draadloos op het netwerk aangesloten mobiele apparaten, zoals laptops, tablets, smartphones, smartwatches.
- IoT[14]-devices, zoals bewakingscamera's en sensoren.
- Alle op deze apparaten beschikbare (web/cloud)services en applicaties ('apps'), waaronder webapplicaties

De OU staat het gebruik van niet door de OU beheerde apparatuur voor toegang tot OU data toe. Daarbij is de beveiligingsstatus van het apparaat mede bepalend bij de toegang die geboden wordt. In alle gevallen valt het gebruik van niet door de OU beheerde apparatuur voor toegang tot applicaties of informatie van de instelling onder dit IB-beleid.

Het beleid is locatie-onafhankelijk: het geldt ook als men op een andere locatie dan op het terrein van de OU met informatie of informatievoorzieningen van de OU werkt (zoals thuis, in de trein of bij een andere onderwijsinstelling).

[14] Internet of Things

4. Beleidsprincipes informatiebeveiliging

4.1 Inleiding

De OU is een instelling met een open karakter. Vanuit het onderwijs- en onderzoeksperspectief is de insteek "*Open waar mogelijk, gesloten waar nodig*". Dit past ook bij de FAIR[15] doelstellingen in het onderzoeksdomein. Adequate beveiliging van informatie is steeds een randvoorwaarde en het openstellen van informatie moet een bewuste keuze zijn.

De OU heeft vijf beleidsprincipes voor informatiebeveiliging vastgesteld. Deze helpen om te bepalen welke beveiligingsmaatregelen er nodig zijn. Een beleidsprincipe bestaat uit:

- Een titel (vaak verklarend).
- Een korte uitleg (de achtergrond).
- De implicaties die uit het beleidsprincipe volgen als basis voor de te nemen maatregelen.

Een korte introductie van de vijf beleidsprincipes volgt in paragraaf 4.2. Een gedetailleerde uitwerking van de principes is opgenomen in bijlage B.

De uiteindelijk door de instelling vastgestelde maatregelen zijn niet altijd 1-op-1 toepasbaar in alle situaties. Soms zijn er bijvoorbeeld processen die afwijken of bestaan er technische of organisatorische beperkingen. In die gevallen moeten er vervangende maatregelen worden genomen waarmee het achterliggende principe tot zijn recht komt en de risico's voldoende worden afgedekt, volgens het uitgangspunt "Pas toe of leg uit"[16].

Om tot een goede afweging te komen of vervangende maatregelen inderdaad tot een acceptabel restrisico leiden, moeten ze aan het IB-beleid van de OU worden getoetst. Met de beleidsprincipes en hun implicaties voor informatiebeveiliging uit dit hoofdstuk kan die toetsing plaatsvinden, ook al zijn vervangende maatregelen niet uitputtend in het beleid of in baselines vastgelegd.

4.2 Beleidsprincipes

De vijf hierna vermelde beleidsprincipes helpen bij de implementatie van het IB-beleid.
Op basis van deze vijf beleidsprincipes kunnen maatregelen worden geformuleerd die relevant zijn voor de bescherming van processen van de OU. De beleidsprincipes vormen de basis voor de communicatie rondom het IB-beleid van de OU.

Allerlei onderdelen die uit het IB-beleid volgen, kunnen ter toetsing langs de beleidsprincipes worden gehouden. Denk daarbij aan:

- Het Information Security Management System (ISMS zie bijlage A).
- Richtlijnen voor projectmatig werken, werkinstructies en awareness-programma's.
- Classificatie (bijlage C) waarmee een risicoanalyse kan worden uitgevoerd als basis voor technische en organisatorische maatregelen.

[15] Findable – Accessible – Interoperable – Reusable (zie https://nl.wikipedia.org/wiki/FAIR-principes)
[16] "pas toe" gaat over de specifieke maatregelen, voor "leg uit" dienen de principes als referentie.

Ook zijn de beleidsprincipes bedoeld om als basis te gebruiken voor de toetsing van uitzonderingen of keuzes bij onvoorziene omstandigheden.

De vijf door de OU vastgestelde beleidsprincipes zijn:

1. Risico-gebaseerd
2. Iedereen
3. Altijd
4. Security by Design
5. Security by Default

1	**Risico-gebaseerd** Informatiebeveiliging is risico-gebaseerd 
Kern	We baseren de maatregelen op de mogelijke veiligheidsrisico's van onze informatie, processen en IT-faciliteiten.
Achtergrond	Het delen van kennis (openheid) is een belangrijke kernwaarde van het onderwijs- en onderzoekproces. Voor een goede risicoafweging bij het beschermen van informatie en het treffen van de juiste maatregelen, is het van belang om de waarde van informatie vast te stellen. Als de waarde van informatie bekend is, kan ook de juiste mate van beveiliging worden bepaald, één die past bij de risico's. Proportionaliteit daarin is gewenst, ook om de beschikbare financiële middelen efficiënt te gebruiken ('Fit for purpose').
Implicaties	Denk aan het inrichten van een risicomanagementproces (classificatie), het vastleggen van verantwoordelijkheden, het borgen van risico's in contracten. Zie bijlage B voor een overzicht van alle implicaties.

2	**Iedereen** Informatiebeveiliging is een verantwoordelijkheid van iedereen 
Kern	Iedereen is en voelt zich verantwoordelijk voor een juist en veilig gebruik van middelen en bevoegdheden.
Achtergrond	Iedereen is zich bewust van de waarde van informatie en handelt daarnaar. Deze waarde wordt bepaald door de mogelijke schade als gevolg van verlies van beschikbaarheid, integriteit of vertrouwelijkheid. Van zowel medewerkers, studenten als derden (waaronder leveranciers)

	wordt verwacht dat ze bewust omgaan met informatie in welke vorm dan ook en dat ze actief bijdragen aan de veiligheid van de geautomatiseerde systemen en de daarin opgeslagen informatie. Het succes van beveiliging staat of valt met goede communicatie. Goede communicatie wordt daarom actief bevorderd, op en tussen alle niveaus in de instelling.
Implicaties	Denk hierbij aan het vastleggen van afspraken in arbeidsvoorwaarden, omgangsvormen, gedragscodes, huisregels en contracten met Service Level Agreements, etc. Zie bijlage B voor een overzicht van alle implicaties.

3	**Altijd** Informatiebeveiliging is een continu proces 
Kern	Informatiebeveiliging zit in het DNA van al onze werkzaamheden.
Achtergrond	De omgeving verandert continu; cyberdreigingen nemen toe en af; processen veranderen, medewerkers en studenten veranderen, leveranciers veranderen etc. Eenmalig de maatregelen bepalen en implementeren is onvoldoende om een veilig klimaat te behouden. Informatiebeveiliging heeft alleen zin als dit een continu proces is van het nemen van maatregelen, bewustzijn en controles.
Implicaties	Denk hierbij aan het houden van awareness campagnes, het inrichten van een audit-proces. Zie bijlage B voor een overzicht van alle implicaties.

4	**Security by Design** Integrale aanpak informatiebeveiliging 
Kern	Informatiebeveiliging is vanaf de start een integraal onderdeel van ieder project of iedere verandering met betrekking tot informatie, processen en IT-faciliteiten.
Achtergrond	Security by design betekent dat al tijdens de start van een project, het ontwerp van een nieuwe applicatie of ICT-omgeving en bij technische of functionele veranderingen rekening wordt gehouden met de beveiliging van gegevens en de continuïteit van de processen. Dit voorkomt (vaak dure) herstelwerkzaamheden achteraf.
Implicaties	Denk hierbij aan het vaststellen en toetsen van beveiligingseisen in projecten en het inregelen van autorisatieschema's. Zie bijlage B voor een overzicht van alle implicaties.

5	**Security by Default** Standaard beperkte toegang en veilige instellingen 
Kern	Gebruikers hebben alleen toegang tot informatie en IT-faciliteiten die zij nodig hebben voor hun werkzaamheden. Het openstellen van informatie is een bewuste keuze.
Achtergrond	Security by default betekent dat in elke configuratie die wordt geïmplementeerd de aanwezige security opties standaard aan staan. Dit voorkomt ongewenste en ongecontroleerde toegang tot (persoons)gegevens. Openstellen van informatie is daarmee altijd een bewuste keuze na een zorgvuldige afweging.
Implicaties	Denk hierbij aan het definiëren van standaard rollen en het standaard beperken van autorisaties en het standaard beschermen van alle externe communicatie met Security Socket Layer (SSL)-technologie. Zie Bijlage B voor een overzicht van alle implicaties.

5. Governance IB-beleid

5.1 Afstemming met samenhangende risico's

Bij governance moet aandacht zijn voor alle soorten risico's en hun onderlinge samenhang. Om die reden besteedt de OU op strategisch niveau veel aandacht aan afstemming van informatiebeveiliging, arboveiligheid, kennisveiligheid, fysieke veiligheid, bedrijfscontinuïteit en privacybescherming. Waar mogelijk en nodig vertaalt deze afstemming zich ook naar het tactische en operationele niveau.

Dit hoofdstuk gaat in op de governance van de informatieveiligheid en informatiebeveiliging (hierna IB-Governance genoemd) als onderdeel van de IT-Governance van de OU.

5.2 Rollen en hun inpassing in IB-Governance

Deze paragraaf beschrijft hoe de IB-Governance is georganiseerd, wie waarvoor verantwoordelijk is en aan wie wordt gerapporteerd. In de diverse rollen is onderscheid gemaakt in richtinggevend (strategisch), sturend (tactisch) en uitvoerend (operationeel).

De benaming van de specifieke rollen voor Informatiebeveiliging sluiten zoveel mogelijk aan bij het PvIB[17]:

	Informatieveiligheid (risicomanagement)	**Informatiebeveiliging** (ICT-beveiliging)
Strategisch/tactisch	Chief Information Security Officer	ICT-beveiligingsmanager
Tactisch/operationeel	Information Security Officer	ICT-beveiligingsspecialist

Tabel: rollen in informatiebeveiliging/-veiligheid

De IT-Governance bij de OU is ingericht volgens het zogenaamde Three Lines of Defence model[18] (ook wel '3LoD'). Dit model wordt algemeen toegepast als model om Governance, Risk en Compliance (GRC) te borgen in een organisatie. Het model beschrijft niet alleen de rollen binnen de organisatiestructuur, maar ook hun onderlinge samenwerking.

5.2.1 Eerste en tweede lijn

Het 3LoD-model heeft als uitgangspunt dat het lijnmanagement verantwoordelijk is voor haar eigen processen. De decanen,directeuren en dienstgemandateerden zorgen ervoor dat beveiligingsmaat-

[17] Beroepsprofielen Informatiebeveiliging: https://www.pvib.nl/kenniscentrum/documenten/beroepsprofielen-informatiebeveiliging-2-0
[18] https://www.icas.com/ca-today-news/internal-audit-three-lines-of-defence-model-explained

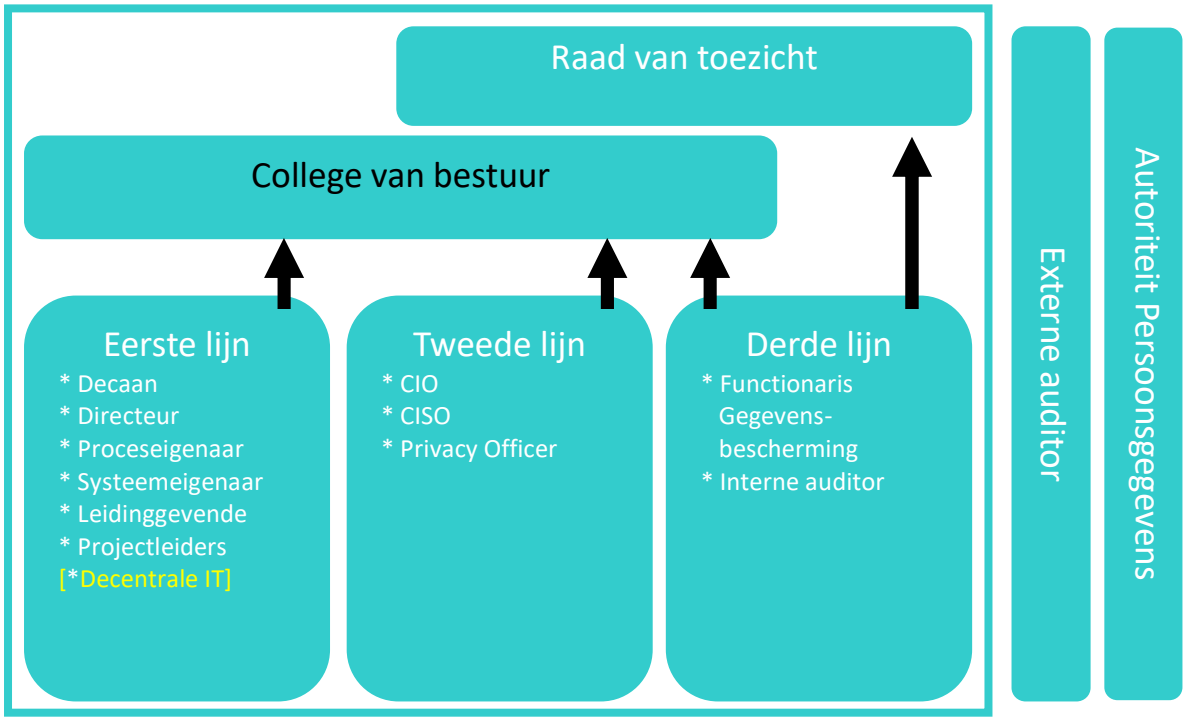
regelen ook werkelijk worden geïmplementeerd, dat awareness-programma's worden uitgevoerd, dat personeel wordt opgeleid, etc. Dit is de eerste lijn.

De tweede lijn ondersteunt de eerste lijn en het Collega van bestuur, adviseert en coördineert. Daarnaast bewaakt de tweede lijn of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. Ook beleidsvoorbereidende taken, het organiseren van de PDCA-cyclus, van integrale risicoanalyses en self-assessments en het opstellen van jaarplannen en rapportages zijn taken van de tweede lijn.

5.2.2 De derde lijn

De derde lijn controleert of het samenspel tussen de eerste en tweede lijn soepel functioneert en velt daarover een objectief, onafhankelijk oordeel en rapporteert mogelijkheden tot verbetering. Daarbij kijkt de derde lijn ook of er geen overlapping is en of er blinde vlekken bestaan.

De binnen de AVG verplichte Functionaris Gegevensbescherming (FG) en de internal auditor behoren typisch tot de derde lijn. Beiden opereren volledig los van alle andere organisatieonderdelen en rapporteren niet alleen aan het College van bestuur, maar ook aan de Raad van toezicht.



Schema: Three Lines of Defence

In bijlage E wordt de governance structuur een het 3LoD-model in detail beschreven. De Raad van toezicht, de externe auditor en de externe toezichthouder (Autoriteit Persoonsgegevens en Onderwijsinspectie) worden verder buiten beschouwing gelaten.

5.2.3 Eindverantwoordelijkheid

Juridisch gezien is het College van bestuur eindverantwoordelijk voor informatieveiligheid en daarmee ook voor informatiebeveiliging van de instelling. Specifieke onderdelen van deze verantwoordelijkheid worden via de mandaatregeling bij de decanen en directeuren verder belegd.

5.2.4 Taken, bevoegdheden, verantwoordelijkheden

De diverse taken, bevoegdheden en verantwoordelijkheden zijn onderverdeeld in Strategisch, Tactisch en Operationeel niveau. Deze drie niveaus kenmerken zich door hun overlegstructuur.

Strategisch niveau	Tactisch niveau	Operationeel niveau
De Chief Information Security Officer (CISO) is een rol op strategisch (en tactisch) niveau. De CISO is verantwoordelijk voor het beleid en het ISMS-proces.	De rol ICT beveiligingsmanager en de rol eigenaar zijn tactisch (en operationeel). De (ICT beveiligingsmanager is verantwoordelijk voor de vertaling van de strategie en het beleid naar tactische (en operationele) plannen. Dit doet hij samen met de CISO (vanwege de uniformiteit), de systeem- en proceseigenaren.	Het operationele niveau is verantwoordelijk voor de implementatie van de informatiebeveiligingsmaatregelen en de afhandeling van incidenten. Dat gebeurt in overleg met de (technisch en functioneel) beheerders, relevante IT-functionarissen en met de tactische laag.

In de volgende tabel zijn de taken, bevoegdheden en verantwoordelijkheden per niveau samengevat. In de kolom Documenten zijn de meest toepasselijke beleidsdocumenten benoemd.

De actuele invulling voor de OU van rollen op functies c.q. functionarissen is te vinden in Bijlage F – Actuele invulling rollen Informatiebeveiliging.

Niveau	Wat?	Wie?	Overleg	Documenten
Richtinggevend (strategisch)	• Bepalen IB-strategie • Organisatie voor IB inrichten • IB planning en control vaststellen • Business continuity management • Communicatie naar management en organisatie	Bestuur (de portefeuillehouder Informatieveiligheid) op basis van advies CISO en CIO/directeur ITF	Bestuur stelt vast, de tweede lijn adviseert	• IB beleid • Privacybeleid • Gedrag- en Integriteitscode • ISMS • Classificatierichtlijn

Niveau	Wat?	Wie?	Overleg	Documenten
Sturend (tactisch)	Planning & Control IB: • voorbereiden normen en wijze van toetsen • evalueren beleid en maatregelen, ook van externe partijen bij contracten • begeleiding interne assessments en externe audits • communicatie naar proces- en systeemeigenaren en IT-ondersteuning	• Proceseigenaren • Systeemeigenaren • Data eigenaar • Informatie eigenaar. • CISO • ICT-beveiligingsmanager • Privacy Officer	Maandelijks HJI/ITF overleg	• Classificaties/Risicoanalyses en audits, inclusief DPIA's en SURFaudit • IB baselines (basismaatregelen) • Jaarplan en -verslag
Uitvoerend (operationeel)	• Implementeren IB-maatregelen. • Registreren en evalueren incidenten, inclusief datalekken • Communicatie eindgebruikers	• IT in samenwerking met proces- en systeemeigenaren • ICT-beveiligingsmanager • SOC[19] • OU-CERT[20] • Privacy Officer	Tweewekelijks overleg CISO – ICT-beveiligingsmanager Driemaandelijk OU-CERT-overleg	• SLA's (security-paragraaf) • Incidentregistratie inclusief evaluatie • OU-CERT charter

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

[19] SOC staat voor "Security Operations Center", meestal geleid door de ICT-beveiligingsmanager en inhoudelijk aangestuurd door CISO.
[20] <Computer Security Incident Response Team / Computer Emergency Response Team>

Strategisch	Tactisch	Operationeel
Op strategisch niveau wordt richtinggevend gesproken over governance en compliance, alsmede over doelen, scope en ambitie op het gebied van informatiebeveiliging, in samenhang met privacy. Dit gebeurt in het bestuur, geadviseerd door de CISO, de CIO en de FG en afgestemd op de IT-strategie en risicobereidheid van de OU.	Op tactisch niveau wordt de strategie vertaald naar plannen, maatregelen, te hanteren normen, evaluatiemethoden, e.d. Deze plannen en instrumenten zijn sturend voor de uitvoering. Dit tactisch overleg wordt gevoerd tussen de CISO, privacy officer en ICT-beveiligingsmanager. Waar nodig in overleg met overige betrokken functionarissen zoals de proces- of systeemeigenaren.	Op operationeel niveau worden de zaken besproken die de dagelijkse bedrijfsvoering aangaan in de zin van uitvoering en implementatie

Alle drie overlegtypes worden zoveel mogelijk ingepast in bestaande overlegvormen met hetzelfde karakter. Zo bespreekt men op strategisch niveau niet alleen informatiebeveiliging en privacy, maar ook andere risico's waarmee de OU te maken kan krijgen, zoals financieel, personeel en commercieel. Dit betekent dat informatiebeveiliging op de agenda staat van het College van bestuur. Op tactisch niveau zal het gesprek ook gaan over keuze van IT-functionaliteit en -services binnen de agenda van de Programmaboard Digitale Universiteit. Op operationeel niveau staat informatiebeveiliging op de agenda van overleggen tussen IT-ondersteuners, functioneel beheerders en IT-beheerders, maar ook op overleggen met key-users en projectteams.

Documenten
Voor informatiebeveiliging wordt bij de OU dezelfde (PDCA-)managementcyclus gevolgd, die ook voor andere onderwerpen geldt: visie/idee, beleid, analyse, plan implementatie, uitvoering, controle en evaluatie. Die cyclus wordt op de verschillende niveaus ondersteund door formeel vastgestelde documenten. In bijlage G is een overzicht opgenomen van de documenten die de OU voor informatiebeveiliging hanteert zoals genoemd in bovenstaande tabel.

5.3 Bewustwording en training

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging uit te sluiten. De mens zelf creëert de grootste risico's. Bij de OU werken we daarom voortdurend aan het vergroten van het beveiligingsbewustzijn van medewerkers om kennis van risico's te verhogen en veilig en verantwoord gedrag aan te moedigen. Onderdeel van het beleid zijn regelmatig terugkerende bewustwordingscampagnes voor alle medewerkers, studenten, derden en met name operationele beheerders. Verhoging van het beveiligingsbewustzijn is een verantwoordelijkheid van zowel de leidinggevenden, de CISO en de ICT-beveiligingsmanager. Bewustwording is een onderdeel van het introductieprogramma voor nieuwe medewerkers en studenten.

5.4 Controle, oefenen, naleving en sancties

Bij de OU is de Internal Auditor verantwoordelijk voor de (planning van) interne financieel georiënteerde audits en de CISO in afstemming met de ICT beveiligingsmanager voor de (planning van) IT audits en penetratietests.

De interne controles vinden jaarlijks plaats en worden naast de reguliere formele audits aangevuld met diverse incidentele activiteiten, zoals het nemen van steekproeven, het uitvoeren van penetra-

tietesten en het controleren van de feitelijke werking van de vastgestelde beveiligingsmaatregelen. Daarnaast worden vaardigheden en operationele procedures regelmatig getest in brainstormsessies of oefeningen. Voorbeelden hiervan zijn calamiteitenoefeningen[21].

De informatiesystemen (of -processen) van de OU worden intern geaudit. De audit richt zich op (1) de classificatie van de in het informatiesysteem vastgelegde gegevens (2), de inventarisatie van de risico's (3), de genomen beveiligingsmaatregelen en (4) de samenhang tussen 1, 2 en 3. Voor elk informatiesysteem wordt een audit frequentie vastgesteld aan de hand van de risicoclassificatie. Als een informatiesysteem wordt vervangen of als er belangrijke wijzingen plaatsvinden in de beveiliging, wordt er een audit uitgevoerd op basis van een nieuwe businessimpact en risicoanalyse. Naast de IT-controle als onderdeel van de jaarrekeningcontrole vindt jaarlijks de onafhankelijke SURF/VSNU audit plaats. Ook neemt de OU deel aan de jaarlijkse SURFbenchmark.

Het normenkader IBHO (zie hoofdstuk 3) wordt gebruikt als uitgangspunt voor interne en externe controles. Voor de audits van specifieke onderdelen of van informatiesystemen kunnen aanvullende, meer gedetailleerde, normen worden vastgesteld.

De bevindingen van de interne en externe controles en mogelijke externe eisen met betrekking tot beveiliging, zijn input voor de nieuwe jaarplannen van de OU. Deze kunnen ook tot wijziging van het IB-beleid leiden.

Controle op de naleving vindt plaats door toezicht op praktische toepassing van informatiebeveiliging. Hierbij is het van belang dat leidinggevenden de medewerkers en studenten aanspreken op tekortkomingen. Voor het toezicht op de naleving van de AVG is de 'Functionaris Gegevensbescherming' (FG) verantwoordelijk.

Als uit de controles blijkt dat de naleving ernstig tekortschiet, dan kan de OU de betrokken verantwoordelijke medewerkers of studenten een sanctie opleggen. De sanctie wordt opgelegd binnen de kaders van de cao, arbeidsovereenkomsten, integriteitscode en de wettelijke mogelijkheden in bijvoorbeeld de Wet op het hoger onderwijs en wetenschappelijk onderzoek (WHW). Sanctionering behoort tot de eindverantwoordelijkheid van het College van bestuur en wordt volgens, de gedragscode computergebruik gemandateerd aan de verantwoordelijke leidinggevenden (decanen/directeuren). De Regeling disciplinaire maatregelen Open Universiteit Nederland is daarbij richtinggevend.

5.5 Financiering

Financiële middelen voor informatiebeveiliging worden structureel opgenomen in de diverse (project)begrotingen. De financiering van informatiebeveiliging wordt bij de OU centraal en decentraal geregeld.

Centraal
Algemene zaken, zoals het opstellen van een informatiebeveiligingsplan voor de instelling of een externe audit, worden uit de algemene middelen betaald die jaarlijks toegekend worden aan ITF. Instelling brede bewustwordingscampagnes en trainingen worden ook uit deze middelen betaald.

Decentraal
De beveiliging van informatiesystemen en processen, inclusief de kosten daarvan, zijn integraal onderdeel van verantwoord beheer van het betreffende informatiesysteem of proces. Beveiligingskosten van werkplekken maken integraal onderdeel uit van de werkplekkosten.

[21] Als voorbeeld gelden de (N)OZON oefening die jaarlijks door SURF worden gecoördineerd.

6. Melding en afhandeling van incidenten

Een incident is een gebeurtenis die de bedrijfsvoering negatief kan beïnvloeden. Incidentbeheer en -registratie gaat over het detecteren, vastleggen en afhandelen van incidenten. Belangrijk hierbij is dat medewerkers, studenten en derden herkennen wanneer er sprake is van een incident of inbreuk op de informatiebeveiliging en dit ook melden.

Van incidenten kan worden geleerd. Incidentregistratie en periodieke rapportage over opgetreden incidenten horen dan ook thuis in een volwassen informatiebeveiligingsomgeving.
Incidenten kan men bij de OU melden bij de ICT ServiceDesk: servicedesk@ou.nl. De OU heeft de contactgegevens van de ServiceDesk duidelijk gecommuniceerd naar haar medewerkers, studenten en derden.

Iedere medewerker, student en derde is verantwoordelijk voor het signaleren en melden van incidenten en inbreuken op de informatiebeveiliging, inclusief datalekken. Incidenten en inbreuken dienen direct gemeld te worden aan servicedesk@ou.nl.

De incidenten worden afgehandeld volgens het door de OU vastgestelde Incident management-proces, waar de afhandeling van datalekken een onderdeel van is. De OU-CERT Charter beschrijft het proces als het gaat over ernstige incidenten en incidenten buiten reguliere bedrijfstijden.

Er is een door het College van bestuur vastgesteld beleid voor Coordinated Vulnerability Disclosure. Daarmee geeft de OU mogelijke melders van kwetsbaarheden in de informatiesystemen een garantie dat de OU, onder voorwaarden, geen juridische stappen tegen hen onderneemt.

7. Vaststelling & wijziging

Het College van bestuur stelt, met instemming van de medezeggenschap, het IB-beleid vast dat de Chief Information Security Officer (CISO) voorstelt. Het IB-beleid volgt het instellings- en ICT-beleid. Het beleid wordt 1x per 3 jaar geëvalueerd en zo nodig bijgesteld. Minimaal 1 keer per 4 jaar, of na een substantiële verandering van het instellingsbeleid of belangrijke ontwikkelingen op cyberveiligheidsgebied, wordt het beleid herzien en opnieuw vastgesteld.

Dit beleid is vastgesteld door het College van bestuur van de Open Universiteit op 26 september 2023 met instemming van de Ondernemingsraad d.d. 20 september 2023 en na verkregen advies van de Studentenraad d.d. 18 september 2023.en kan worden aangehaald als “Beleid Informatieveiligheid van de OU”.

Bijlage A - Schematisch overzicht inrichting ISMS

Informatiebeveiliging is een continu proces. Kort gezegd: eerst moet worden vastgesteld wat nodig is, waarna maatregelen worden getroffen. Deze maatregelen worden vastgelegd in een jaarplan. De maatregelen kunnen veranderen (omdat bedreigingen en risico's veranderen, maar ook wet- en regelgeving is aan verandering onderhevig). Controle kan dan aanleiding geven tot bijsturing van de maatregelen. Daarnaast kan ook het totaalpakket van eisen, maatregelen en controle aan een herijking toe zijn en zal dus periodiek geëvalueerd moeten worden. Het gehele proces van informatiebeveiliging volgt dus een Plan-Do-Check-Act (PDCA)-cyclus (zie afbeelding).
De complete set van maatregelen, processen en procedures wordt vastgelegd in een Information Security Management System (ISMS) en biedt daarmee ondersteuning in het doorlopen van de PDCA-cyclus. De jaarlijkse planningen zijn te vinden zijn in de planning/control cyclus en meer in detail in het IT-Portfolio met de IT-jaarplannen.

Standaarden
De OU onderhoudt een ISMS op basis van de internationale ISO27001 standaard en gebruikt het CIS-20[22] framework als ondersteunend hulpmiddel om invulling te geven aan het ISMS.

Uitwerking
Na het vaststellen van de context van de organisatie (IB-beleid i.r.t. de externe en interne omgeving) en van de behoeften en verwachtingen van belanghebbende partijen en een scope-bepaling, wordt het ISMS opgesteld op basis van een PDCA-cyclus met de volgende fasen:

Plan	Do
In de planfase worden de volgende zaken gedefinieerd: • Beleid, context en scope • bedrijfsmiddelen (assets), mensen en financiële middelen • risico's en kansen • middelen en competenties • bewustzijn en communicatie • gedocumenteerde informatie	Bij de uitvoering van het ISMS gaat het om: • de operationele planvorming en beheersing • risicobeoordeling(en) • risicobehandeling
Check	**Act**
De checkfase omvat de evaluatie van de werking van het ISMS: • bewaking, meting, analyse en evaluatie • interne audit • management review	Op basis van de uitkomsten van de checkfase worden verbeteringen doorgevoerd

Door herhaling van de PDCA-cyclus werkt de organisatie doorlopend aan het verbeteren van het ISMS en is daardoor meer 'in control'.

[22] https://www.cisecurity.org/controls/cis-controls-list/

Bijlage B – Informatiebeveiligingsprincipes

1	**Risico-gebaseerd** Informatiebeveiliging is risico-gebaseerd 
Kern	We baseren de maatregelen op de mogelijke veiligheidsrisico's van onze informatie, processen en IT-faciliteiten.
Achtergrond	Het delen van kennis (openheid) is een belangrijke kernwaarde van het onderwijs- en onderzoekproces van de OU. Voor een goede risicoafweging bij het beschermen van informatie en het treffen van de juiste maatregelen, is het van belang om de waarde van informatie vast te stellen. Als de waarde van informatie bekend is, kan ook de juiste mate van beveiliging worden bepaald, één die past bij de risico's. Proportionaliteit daarin is gewenst, ook om de beschikbare financiële middelen efficiënt te gebruiken ('Fit for purpose').
Implicaties	• De risico's worden ingeschat en vastgesteld op basis van een risicoclassificatie (Bijlage C). • De OU stelt een Classificatierichtlijn vast. • Een gegevensbeschermingseffectbeoordeling (DPIA – Data Protection Impact Assessment) in het kader van de AVG maakt waar nodig onderdeel uit van de risicoanalyse. • Waar nodig worden maatregelen getroffen om het vastgestelde risico op Beschikbaarheid, Integriteit en Vertrouwelijkheid te brengen naar het geaccepteerde niveau. • Informatie heeft één eigenaar. • Eigenaren van informatie, informatiesystemen, applicaties en processen zijn verantwoordelijk voor de implementatie en operationele handhaving van maatregelen onder het principe van "Pas toe of leg uit". • Afwijkingen kunnen worden geaccepteerd binnen de risicobereidheid (risk-appetite) van de OU, uiteindelijk te bepalen door het bestuur. • Voor afwijkingen moet het risico-acceptatieproces worden gevolgd, met acceptatie door de gegevens-, proces- of systeemeigenaar. • De informatie-eigenaar (of eventueel ook de proces- of applicatie-eigenaar) tekent voor acceptatie van de risico's. • Maatregelen moeten zo worden ingericht dat hun effect controleerbaar is. • De hoogste risico's worden als eerste gemitigeerd. • Op basis van de risicoanalyse kan informatiebeveiliging voor gebruiksgemak kiezen. • Maatregelen moeten (qua kosten) in balans zijn met de vermindering van risico's (proportionaliteitsprincipe). • Informatie heeft één bron, waardoor eigenaarschap en "single point of truth" goed te duiden is. Hierdoor ontstaat ook een extra ketenverantwoordelijkheid voor de consequenties van wijzigingen bij de bron.

	• De OU blijft verantwoordelijk voor adequate bescherming van informatie bij gebruik van externe diensten voor informatieverwerking. • Waar van toepassing bevatten contracten de veiligheidseisen en de levering van externe toetsing (assurance) die laat zien dat maatregelen effectief zijn.

2	**Iedereen** Informatiebeveiliging is een verantwoordelijkheid van iedereen 
Kern	Iedereen is en voelt zich verantwoordelijk voor een juist en veilig gebruik van middelen en bevoegdheden.
Achtergrond	Iedereen is zich bewust van de waarde van informatie en handelt daarnaar. Deze waarde wordt bepaald door de mogelijke schade als gevolg van verlies van beschikbaarheid, integriteit of vertrouwelijkheid. Van zowel medewerkers, studenten als derden wordt verwacht dat ze bewust omgaan met informatie in welke vorm dan ook en dat ze actief bijdragen aan de veiligheid van de geautomatiseerde systemen en de daarin opgeslagen informatie. Het succes van beveiliging staat of valt met goede communicatie. Goede communicatie wordt daarom actief bevorderd, op en tussen alle niveaus in de instelling.
Implicaties	• Voor alle gebruikers van digitale informatievoorzieningen van de OU is een zogenaamde Acceptabel Use Policy (AUP) beschikbaar die is gepubliceerd via de website van de OU. Deze AUP is van toepassing op zowel studenten, medewerkers als derden. • Het veilig omgaan met informatie en informatiedragers is een onderdeel van de <aanstelling/arbeidsovereenkomst> van alle medewerkers. • Informatiebeveiliging krijgt aandacht bij indiensttreding van medewerkers en bij <Jaargesprekken/Periodieke overleggen> • Informatiebeveiliging krijgt aandacht in reguliere overleggen in afdelingen en projecten. • Medewerkers en studenten spreken elkaar aan op onveilige omgang met informatie en systemen. • Medewerkers en studenten melden (vermoedens van) kwetsbaarheden bij het CSIRT • Er is een door het bestuur vastgesteld Coordinated Vulnerability Disclosure beleid. • Schending van wetgeving, voorschriften en regels op gebied van informatiebeveiliging kan leiden tot sanctionerende maatregelen, door of namens het CvB.

3	**Altijd** Informatiebeveiliging is een continu proces 
Kern	Informatiebeveiliging zit in het DNA van al onze werkzaamheden.
Achtergrond	De omgeving verandert continu; cyberdreigingen nemen toe en af; processen veranderen, medewerkers en studenten veranderen etc. Eenmalig de maatregelen bepalen en implementeren is onvoldoende om een veilig klimaat te behouden. Informatiebeveiliging heeft alleen zin als dit een continu proces is van het nemen van maatregelen, bewustzijn en controles.
Implicaties	• Er wordt een Information Security management Systeem (ISMS, Bijlage A) ingericht waarmee door middel van een PDCA-cyclus alle aspecten van het IB-beleid adequaat worden opgevolgd. • Periodiek worden audits en assessments uitgevoerd die het mogelijk maken het beleid en de genomen maatregelen te controleren op effectiviteit (controleerbaarheid). • Bij instroom van nieuwe medewerkers en studenten is er aandacht voor de bewustwording van de risico's en de beveiligingsprocedures van de OU rond toegang en gebruik van IT-middelen. • Periodiek worden accounts met hoge privileges gevalideerd. • De OU organiseert regelmatig cybersecurity-awareness activiteiten voor de diverse doelgroepen: studenten, medewerkers, leidinggevenden en partners van de OU. • Bij aanpassingen in rollen, taken, en verantwoordelijkheden van een persoon worden ook de autorisaties daarmee in overeenstemming gebracht en aangepast. • Er wordt een proces ingericht om het dreigingsbeeld voor de OU te bepalen en periodiek bij te stellen. Nieuwe dreigingen leiden waar nodig tot aanpassing van maatregelen.

4	**Security by Design** Integrale aanpak informatiebeveiliging 
Kern	Informatiebeveiliging is vanaf de start een integraal onderdeel van ieder project of iedere verandering met betrekking tot informatie, processen en IT-faciliteiten.
Achtergrond	Security by design betekent dat al tijdens de start van een project, het ontwerp van een nieuwe applicatie of ICT-omgeving en bij technische of functionele veranderingen rekening wordt gehouden met de beveiliging van gegevens en de

	continuïteit van de processen. Dit voorkomt (vaak dure) herstelwerkzaamheden achteraf.
Implicaties	• Voor elk nieuw project/software-inkoop/innovatie worden de security-eisen (*non-functional requirements*) vanaf de start meegenomen. • Voor de livegang wordt de toepassing van de security-eisen getoetst en/of ge-test. • Bij elk IT-systeem of inrichting wordt ter bevordering van informatiebeveiliging het principe van 'minste rechten' gehanteerd. Dat betekent dat ernaar wordt ge-streefd om niet meer rechten te verlenen dan nodig zijn voor adequate functie- en bedrijfsuitoefening. • Toegang tot systemen is gebaseerd op autorisatieschema's. • Scheiding van verantwoordelijkheden wordt toegepast in processen en procedu-res. • In het ontwerp wordt meegenomen dat het gebruik van informatie en IT-faciliteiten herleidbaar is tot een verantwoordelijke gebruiker. • Er wordt een richtlijn "security in projecten" vastgesteld, gebaseerd op de maat-regelen die voortkomen uit de risicoclassificatie en maatregelen die mogelijk voortvloeien uit de gegevensbeschermingseffectbeoordeling (DPIA) in het kader van de AVG. • Bij procesontwerp worden maatregelen meegenomen die de continuïteit van het proces afdoende kunnen waarborgen.

5	**Security by Default** Standaard beperkte toegang en veilige instellingen 
Kern	Gebruikers hebben alleen toegang tot informatie en IT-faciliteiten die zij nodig hebben voor hun werkzaamheden. Het openstellen van informatie is een bewus-te keuze.
Achtergrond	Security by default betekent dat in elke configuratie die wordt geïmplementeerd de aanwezige security opties standaard aan staan. Dit voorkomt ongewenste en ongecontroleerde toegang tot (persoons)gegevens. Openstellen van informatie is daarmee altijd een bewuste keuze na een zorgvul-dige afweging.
Implicaties	• De beveiligingsbaseline van de standaardconfiguratie moet worden vastgelegd. (bv. het standaard beschermen van alle externe communicatie met SSL-technologie) • Het principe bij initiële inrichting van een informatiesysteem of een infrastructuur is "*gesloten, tenzij*". • Afwijking van de initiële inrichting volgt het principe "*Pas toe of leg uit.*" • Security wordt geborgd in een changemanagementproces. • Toegang tot informatie is rol-gebaseerd, waardoor gebruikers alleen toegang hebben tot informatie en IT-faciliteiten die zij nodig hebben voor hun werkzaam-heden (vastgelegd in een autorisatieschema). • Er worden enkele hoofdrollen geïdentificeerd op basis waarvan baseline-

	autorisaties worden toegekend. Te denken valt aan de hoofdrol student, medewerker, leverancier etc. Gebruikers krijgen standaard alleen deze rollen. • Logging- en auditprocessen worden zodanig ingeregeld dat toegang tot informatie en IT-faciliteiten herleidbaar is tot een verantwoordelijke gebruiker.

Bijlage C – Risicobereidheid en Classificatie

Bij de OU zijn alle gegevens, processen, informatiesystemen en applicaties waarop dit informatiebeveiligingsbeleid van toepassing is, geclassificeerd. Deze classificatie is afhankelijk van de te verwerken gegevens en wordt bepaald op basis van de risicobereidheid (risk appetite) van de UM aan de hand van risicoanalyses en schade categorieën. Het classificatieproces is vastgelegd in een door het CvB vastgestelde Classificatierichtlijn[23].

Het niveau van de beveiligingsmaatregelen is afhankelijk van een vastgestelde risicoklasse.
Deze bijlage geeft een overzicht van de vastgestelde risicobereidheid, de gehanteerde schade categorieën en het vastgestelde classificatieproces.

Risicobereidheid

Met een risicoanalyse kan de mogelijke schade worden geëvalueerd die een dreiging kan toebrengen aan specifieke informatie (bijv. misbruik door oneigenlijke toegang, ongeautoriseerde toegang) en wat de kans is dat die schade optreedt. Het gebruik van standaard risicoanalysehulpmiddelen is vaak een tijdrovend en abstract traject.
Niet alle risico' s hoeven gemitigeerd te worden. De OU is bereid om sommige risico' s te accepteren. De risicobereidheid in onderstaande tabel kan gezien worden als een risicoanalyse op basis van algemene waarden in plaats van concrete risico's.

De risicobereidheid van de OU is in onderstaand schema weergegeven.

Risico		**Schade**			
		Verwaarloosbaar	Enig	Ernstig	Ontwrichtend
Kans	Minimaal	Acceptabel	Acceptabel	Acceptabel	Acceptabel
	Klein	Acceptabel	Acceptabel	Acceptabel	Niet acceptabel
	Reëel	Acceptabel	Acceptabel	Niet acceptabel	Niet acceptabel
	Hoog	Acceptabel	Niet acceptabel	Niet acceptabel	Niet acceptabel

Tabel 1: Risicobereidheid

[23] Zie Https://www.maastrichtuniversity.nl/informatiebeveiliging.

Schadecategorieën

Schade kan onderverdeeld worden in verschillende categorieën. De hieronder voorgestelde schadecategorieën geven een indicatie van het belang van de informatie. Gekoppeld aan de risicobereidheid worden maatregelen geselecteerd die de kans op inbreuken op de veiligheid terugdringen tot een voor de organisatie acceptabel niveau.

De schade categorieën bij de OU zijn als volgt bepaald:

	INDICATIE SCHADECATEGORIEËN			
IMPACT	**Imago**	**Onderwijs**	**Onderzoek**	**Financieel**
VERWAARLOOSBAAR	Een klein aantal negatieve berichten in lokale media (inclusief sociale media)	Hooguit verstoring van een beperkt aantal activiteiten op een instituut of vakgroep.	Geen of korte onderbrekingen in lopend onderzoek, voornamelijk reeds publieke of niet-gevoelige data	Directe schade ligt tussen 0 en €10.000
ENIG	Negatieve berichtgeving in de media gedurende een paar dagen (inclusief sociale media)	Verstoring van een deel van het onderwijs (zoals een deel van instituut of vakgroep)	Niet openbare onderzoeksgegevens, langdurige onderbreking of invalidatie van onderzoek	Directe schade tussen €10.000 en €250.000
ERNSTIG	Aanhoudende negatieve berichtgeving in de lokale media (inclusief sociale media). Details maatschappelijk gevoelige werkzaamheden (zoals dierproeven).	Langdurige verstoring van een groot deel van het onderwijs op een of meer instituten.	Publicatiebeperkingen, reputatieschade aan onderzoeker of instelling, patenten of contractuele afspraken	Directe schade tussen €250.000 en €1.500.000
ONTWRICHTEND	Aanhoudende negatieve berichtgeving in de landelijke/internationale media (inclusief sociale media).	Merendeel van het onderwijs wordt langdurig onmogelijk op een of meer instituten	Op één of meer instituten is een groot deel van het onderwijs onmogelijk. Verregaande contractuele verplichtingen, uitsluiting toekomstige subsidies of levensbedreigend onderzoek	Directe schade is groter dan €1.500.000

Tabel 2: Indicatie schadecategorieën

Classificatie aan de hand van 3 kwaliteitsaspecten en 3 risico klassen

De data en/of informatie-eigenaar bepaalt de schadecategorie op basis van de maximale schade/waarde van de data. De waarde van een aantal datatypen is al vastgesteld voor de hele organisatie (tabel 2).

De eigenaar houdt bij het bepalen rekening met **drie kwaliteitsaspecten**:

Beschikbaarheid (B)	Is de informatie/functie aanwezig/bruikbaar/leesbaar op alle noodzakelijke momenten en met de juiste performance.
Integriteit (I)	Is de informatie/functie betrouwbaar/compleet/onaangetast?
Vertrouwelijkheid (V)	Hebben alleen rechthebbenden toegang tot de informatie/functie?

Naast bovenstaande drie kwaliteitsaspecten zijn bij het bepalen van maatregelen de volgende 2 aspecten van belang:

Controleerbaarheid
Hierbij gaat het om de controleerbaarheid[24] van de maatregelen die genomen zijn om deze kwaliteitsaspecten te borgen.

Privacybescherming
De aspecten Integriteit en Vertrouwelijkheid zijn ook van belang om de Privacy rechten van Betrokkenen te kunnen waarborgen bij de verwerking van persoonsgegevens. De hieruit voortvloeiende risico's worden bepaald in een zogenaamde Gegevensbeschermingseffectbeoordeling (GBEB, ook wel DPIA[25] genoemd) in het kader van de AVG.

Voor de feitelijke classificatie wordt per kwaliteitsaspect gekozen voor een indeling in **3 risico klassen**: **Laag, Midden en Hoog**. De indeling in 3 klassen maakt het eenvoudig om per kwaliteitsaspect een indeling in een klasse te maken en daar dan voor de hele instelling generieke maatregelen aan te koppelen.

De onderstaande tabel geeft een handvat voor het inschatten de risicoklasse aan de hand van een generieke impactindicatie per kwaliteitsaspect.

CATEGORIE	BESCHIKBAARHEID	INTEGRITEIT	VERTROUWELIJKHEID
LAAG	algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan 1 week brengt geen merkbare (meetbare) schade toe aan de belangen van de instelling, haar medewerkers of haar studenten of klanten	het bedrijfsproces staat enkele integriteitsfouten toe.	informatie die toegankelijk mag of moet zijn voor alle of grote groepen medewerkers of studenten. Vertrouwelijkheid is gering. Daar waar informatie openbaar is, is inzage geen issue, beheer (ten behoeve van de integriteit) wel.
MIDDEN	algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan 1 dag brengt merkbare	het bedrijfsproces staat zeer weinig integriteitsfouten toe. Bescherming van	informatie die alleen toegankelijk mag zijn voor een beperkte groep gebruikers. De informatie is vertrouwelijk.

[24] Controleerbaarheid: de mate waarin het mogelijk is om achteraf parameters die van belang zijn voor beschikbaarheid, integriteit of vertrouwelijkheid te verifiëren. Zulke parameters zijn bijvoorbeeld *downtime*, toegang en transacties.
[25] Data Protection Impact Assessment

	schade toe aan de belangen van de instelling, haar medewerkers of haar studenten of klanten	integriteit is absoluut noodzakelijk.	
HOOG	algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan 1 uur brengt merkbare schade toe aan de belangen van de instelling, haar medewerkers of haar studenten of klanten	het bedrijfsproces staat geen integriteitsfouten toe	dit betreft zeer vertrouwelijke informatie, alleen bedoeld voor specifiek benoemde personen, waarbij onbedoeld bekend worden buiten deze groep grote schade kan toe brengen.

Tabel 3: Inschatten van de schade

Ten aanzien van alle aspecten BIV kunnen in bijzondere gevallen, bijvoorbeeld als gevolg van externe eisen, zwaardere klassen worden vastgesteld door het bestuur. De CISO zorgt ervoor dat zulke bijzondere klassen als uitzondering worden aangemerkt en behandeld.

Hiermee wordt de risico-classificatie vastgesteld. Het feitelijke risico wordt bepaald door de impact te vermenigvuldigen met de káns dat de schade optreedt. Door afdoende mitigerende maatregelen te nemen, kunnen kans en impact gereduceerd worden, en daarmee het risico gemitigeerd.

De uitkomst van de classificatie is daarmee bepalend voor de maatregelen die genomen moeten worden om de informatie adequaat te beveiligen.
De OU heeft een informatiebeveiligingsbaseline vastgesteld als minimale set maatregelen. Aan de hand van de classificatie worden aan de baseline maatregelen van toepassing verklaard conform de centraal vastgestelde maatregelentabel.

Bijlage D – Wet- en regelgeving

Deze bijlage geeft een overzicht van de belangrijkste aan informatieveiligheid gerelateerde wet- en regelgeving met specifieke aandachtspunten voor de OU. Voor een gedetailleerd overzicht met relevante wet- en regelgeving wordt verwezen naar de bijlage met wet- en regelgeving bij het Information Security Management System (ISMS).

1. **Wet op het Hoger onderwijs en Wetenschappelijk onderzoek (WHW)**
   De OU heeft een kwaliteitszorgsysteem conform de InstellingsToets Kwaliteitszorg (ITK). Hierin is (onder meer) het zorgvuldig omgaan met gegevens in de studentenadministratie en met de studieresultaten gewaarborgd. Daarnaast worden integriteitscodes voor wetenschappelijk onderzoek nageleefd en toegepast.

2. **Algemene Verordening Gegevensbescherming (AVG)**
   De instelling heeft een separaat gegevensbeschermingsbeleid vastgesteld waarin naleving van de AVG wordt geborgd. Naleving van het informatiebeveiligings- en privacybeleid inclusief de daarin vermelde technische en organisatorische maatregelen zorgen samen voor het voldoen aan de AVG.

3. **Wettelijke bewaartermijnen/Archiefwet**
   De OU houdt zich aan de wettelijke voorschriften ten aanzien van bewaartermijnen, zoals die zijn vastgelegd in specifieke wetgeving (zoals de Belastingwet en in het arbeidsrecht) en in de Archiefwet en het Archiefbesluit. De OU hanteert daarbij het Basisselectiedocument[26] van de sector universiteiten. Dit selectiedocument gaat over alle informatie zoals die bijvoorbeeld is vastgelegd in (gedigitaliseerde) documenten, informatiesystemen, websites en e-mail. Dit is onderdeel van de jaarlijkse externe accountantsrapportages.

4. **Auteurswet**
   De OU respecteert auteursrechten en handelt daarnaar.

5. **Telecommunicatiewet**
   Omdat de doelgroep van de OU voldoende afgebakend is worden de netwerkvoorzieningen van de OU niet aangemerkt als een openbaar netwerk in de zin van de Telecommunicatiewet.

6. **Wet Computercriminaliteit III**
   De Wet Computercriminaliteit richt zich op de strafrechtelijke probleemgebieden in relatie tot het computergebruik. De wet bestaat uit artikelen die op diverse plekken zijn toegevoegd aan het Wetboek van Strafrecht. De extra artikelen houden zich bezig met:
   - Vernieling en onbruikbaar maken.
   - Aftappen van gegevens.
   - Denial of service, verstikkingsaanval.
   - Computervredebreuk.
   - Diensten afnemen zonder betalen.
   - Malware, kwaadaardige software.

   Naleving van dit Informatiebeveiligingsbeleid, met name van de beveiligingsmaatregelen en het te verwachten gedrag zorgen ervoor dat de OU een adequaat basisniveau van beveiliging heeft tegen deze dreigingen. Indien er aanvallen op de OU plaatsvinden die de beveiliging significant doorbreken en die vallen onder de Wet Computercriminaliteit, zal het bestuur van de OU aangifte doen.

[26] https://www.nationaalarchief.nl/archiveren/kennisbank/selectielijst-universiteiten-en-universitair-medische-centra-2020

7. **Overige codes en landelijke afspraken**

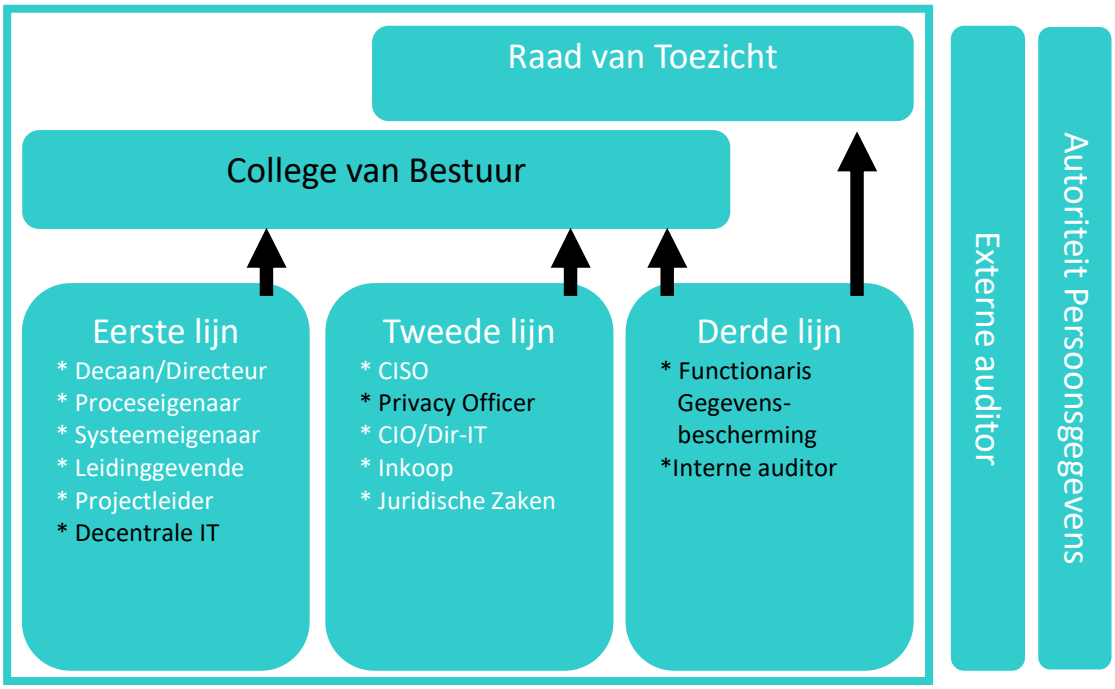
Het informatiebeveiligingsbeleid bij de OU is gebaseerd op het SURF Normenkader en de instelling is deelnemer in de UNL[27] . De OU is in dit kader gehouden aan de volgende codes en landelijke afspraken:

- Code goed bestuur universiteiten.
- Nederlandse gedragscode wetenschappelijke integriteit.
- Juridisch Normenkader Hoger Onderwijs.
- Basisselectie document universiteiten.
- Basisselectie document WO.
- FAIR-principes.

[27] Universiteiten van Nederland

Bijlage E – Rollen de IB-governance

In deze bijlage worden de diverse rollen in het 3LoD model verder “top down” beschreven en hun onderlinge samenhang is samengevat in een tabel. De Raad van Toezicht, Externe Audit en Autoriteit Persoonsgegevens worden buiten beschouwing gelaten.



Schema: Three Lines of Defence, vertaald naar Onderwijs

College van bestuur
Het bestuur is verantwoordelijk voor de informatiebeveiliging binnen de OU en stelt het beleid en de governance op het gebied van informatieveiligheid vast. Informatieveiligheid komt zo vaak als nodig en minimaal 1x per jaar op de agenda van het bestuur. Het bestuur wijst een van haar leden aan als portefeuillehouder informatieveiligheid.

De inhoudelijke verantwoordelijkheid voor zover het de digitale informatiebeveiliging betreft is door de portefeuillehouder belegd bij de CISO. Deze heeft de opdracht om op de digitale informatiebeveiliging van de gehele instelling toe te zien. De niet-digitale informatiebeveiliging is belegd bij de proceseigenaren.

Functionaris Gegevensbescherming (FG of Data Protection Officer)
De FG houdt binnen de OU toezicht op de toepassing en naleving van de AVG, zoals beschreven in het privacybeleid. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de instelling.

Interne auditor
De interne auditor is onderdeel van de interne audit-organisatie en controleert jaarlijks het goed en betrouwbaar functioneren van de interne organisatie. Dit omvat o.a. de structuur en verantwoordelijkheden van de organisatie, monitort het proces van risico management en beoordeelt subsidiedecla-

raties. De interne auditor rapporteert aan de portefeuillehouder in het bestuur, in afstemming met de Directeur Finance en control. Daarnaast rapporteert de interne auditor aan stakeholders zoals decanen en directeuren.

Chief Information Security Officer (CISO)
De CISO is een rol op strategisch (en tactisch) niveau. Hij adviseert en rapporteert onafhankelijk en direct aan het bestuur. De CISO stelt het IB-beleid op, helpt bij een juiste vertaling daarvan naar instellingsonderdelen, ziet toe op de (uniforme) naleving ervan en rapporteert over lacunes, inconsistenties en onvolkomenheden. De CISO kan zowel gevraagd als ongevraagd advies geven. De manager Operations is de hiërarchisch leidinggevende van de CISO. De CISO kan onderzoek doen, onderzoek laten uitvoeren (audits), informatie opvragen en deze in principe ook krijgen.

ICT-beveiligingsmanager
De ICT-beveiligingsmanager vervult een rol bij de vertaling van de strategie naar tactische (operationele) en technische plannen en maatregelen. Dit doet hij samen met de CISO en met de systeem- en proceseigenaren. Tevens adviseert de ICT-beveiligingsmanager over specifieke informatiebeveiligingsmaatregelen, bijvoorbeeld in projecten, bij acquisities van software of hardware, etc. De ICT-beveiligingsmanager heeft de directeur ITF als hiërarchisch leidinggevende.

Privacy Officer (PO)
De Privacy Officer houdt zich binnen de OU centraal bezig met de toepassing en naleving van de AVG. In sommige gevallen in samenwerking met de Information Security Manager en CISO, bijvoorbeeld bij het analyseren van (mogelijke) datalekken. Andere voorbeelden van samenwerking zijn het beoordelen van risico's en maatregelen in het geval van een Gegevensbeschermingseffectbeoordeling (DPIA) of bij het afsluiten van verwerkersovereenkomsten in het kader van de AVG.

Eigenaar bedrijfsproces
Een bedrijfsproces is een zich herhalende keten van activiteiten gericht op de klant en afgestemd op de organisatie.

De eigenaar van een bedrijfsproces is de persoon die de bevoegdheid heeft om te bepalen hoe een bedrijfsproces verloopt, en de verantwoordelijkheid heeft ervoor te zorgen dat het bedrijfsproces aan de klantverwachtingen en bedrijfsbeleid en -doelstellingen blijft voldoen, vandaag en in de toekomst.
Voorbeeld: het financiële bedrijfsproces: de eigenaar van het financiële bedrijfsproces is de eigenaar van het financiële informatiesysteem, de financiële data (ook van financiële data die in een ander informatiesysteem dan het financiële informatiesysteem gebruikt worden).

Per bedrijfsproces is er één eigenaar.

Eigenaar data (datadomein)
Een eigenaar van data zorgt ervoor dat de gegevens volgens de geldende in- en externe regels worden verwerkt in het daarvoor bestemde informatiesysteem.
Voorbeeld: financiële domein: ook financiële data in een ander informatiesysteem dan het financiële systeem (bijv. binnen digitale campus) vallen onder eigenaarschap van de eigenaar van het financiele domein.
Bij gebruik van data in een systeem van een ander domein moeten de data eigenaren afspraken vastleggen welke data met wel doel in welk informatiesysteem verwerkt worden (leverancier – afnemer relatie)
Per domein is er één eigenaar.

Eigenaar informatie
Het verschil tussen data en informatie: data bestaat uit gegevens en informatie bestaat uit data die in een bepaalde c.q. relevante context geplaatst worden en daardoor betekenis en waarde hebben gekregen. Vanuit data wordt er iets waargenomen zonder dat er een betekenis aan de gegevens zit.

Met andere woorden:
Data zelf zijn de ruwe, onverwerkte gegevens in bijvoorbeeld datasets. Informatie is gestructureerde data in een nuttige c.q. relevante context.

Een eigenaar van informatie is de eigenaar van een bepaalde rapportage die informatie maakt van (ruwe) data. De eigenaar van informatie [als afnemer] moet afspraken maken met de data-eigenaar c.q. data-eigenaren [de data-leverancier(s)]. Deze afspraken moeten gebaseerd zijn op: wat-wie-welke-voor welk doel?

Er is één eigenaar per rapportage.

Eigenaar informatiesysteem
Een eigenaar van een informatiesysteem is verantwoordelijk voor het creëren en uitdragen van de productvisie en –strategie, eventueel via een gemandateerde product owner.

Een eigenaar van een informatiesysteem:

- Moet ervoor zorgdragen dat het informatiesysteem geschikt blijft voor haar functie, conformeren aan beleid van de OU en eventuele wettelijke verplichtingen.
- Kan een deel van zijn taken en bevoegdheden mandateren aan product owner(s) c.q. medewerkers.
- Is beslissingsbevoegd voor dat informatiesysteem en voor de toegang tot het informatiesysteem. Wijzigingen in het informatiesysteem of in de toegangsrechten tot het informatiesysteem vereisen de instemming van de eigenaar. De eigenaar controleert of het informatiesysteem en de toegangsrechten tot het informatiesysteem aan zijn eisen voldoen.
- Moet ervoor zorgdragen dat gegevens [in het informatiesysteem - data] volgens de geldende regels worden verwerkt. Verzorgt het budget voor de instandhouding van het informatiesysteem en voor de realisatie en controle van eventuele wijzigingen.

Er is één eigenaar per informatiesysteem.

Leidinggevende (inclusief onderwijsverantwoordelijken)
Naleving van het IB-beleid is onderdeel van het integrale bedrijfsproces. Iedere leidinggevende heeft de taak om:

- ervoor te zorgen dat hun medewerkers c.q. studenten op de hoogte zijn van (de voor hen relevante aspecten van) het beveiligingsbeleid;
- toe te zien op de naleving van het beveiligingsbeleid door medewerkers en studenten;
- periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen;
- als aanspreekpunt beschikbaar te zijn voor alle personeel gerelateerde informatiebeveiligingszaken.

Bijlage F – Actuele Invulling rollen informatiebeveiliging

Rollen uit informatiebeveiligingsbeleid	Binnen OU ingevuld door
College van bestuur	Frank van der Duijn Schouten (interim voorzitter) Theo Bastiaens (rector magnificus)
Portefeuillehouder Informatiebeveiliging (CvB)	Frank van der Duijn Schouten
Business Continuity Manager (BCM)	Hilde Janssen
Information Security Officer (CISO)	Martin Romijn
ICT-beveiligingsmanager	Hilde Janssen – t.a.v. Operations Maarten Scholl – t.a.v Innovatie & development
Privacy Officer (PO)	Mark Adriolo
Functionaris Gegevensbescherming (FG)	Saskia van der Westen
Interne auditor	Harold van Breugel
CIO / Directeur ITF	Jan Jansen
Belangrijkste proceseigenaren	Vertegenwoordiger / product owner expertisecentrum Vertegenwoordiger / product owner onderwijsservices Vertegenwoordiger / product owner bedrijfsvoering Vertegenwoordiger / product owner CPO Vertegenwoordiger onderzoek namens alle faculteiten: AZ Vertegenwoordiger / product owner IT Vertegenwoordiger onderwijs namens alle faculteiten
Decanen/directeuren	Zie https://mijn.ou.nl/group/mdw/organisatie

Bijlage G – Documenten informatiebeveiliging

Voor informatiebeveiliging wordt bij de OU dezelfde (PDCA-)managementcyclus gevolgd, die ook voor andere onderwerpen geldt. De (PDCA-)managementcyclus bestaat uit visie/idee, beleid, analyse, plan implementatie, uitvoering, controles en evaluatie.

In het kader van informatiebeveiliging hanteert de OU de volgende documenten:

1. *Het IB-beleid*
   Het IB-beleid ligt ten grondslag aan de aanpak van (digitale) informatiebeveiliging binnen de OU. Het beleid wordt opgesteld door de CISO en vastgesteld door het bestuur.

2. *Beschrijving van het Information Security Management System (proces en vastlegging)*

3. *Classificatierichtlijn, DPIA, regelingen en werkinstructies*

4. *Jaarplan/verslag*
   De CISO levert, in lijn met de PDCA-cyclus, jaarlijks een verslag over het afgelopen jaar en een jaarplan voor het volgende jaar op aan het bestuur. Het jaarverslag is mede gebaseerd op de resultaten van de periodieke controles/audits. Er wordt o.a. ingegaan op incidenten, resultaten van risicoanalyses (inclusief genomen maatregelen) en andere initiatieven die het afgelopen jaar hebben plaatsgevonden. Het jaarplan wordt in ieder geval afgestemd met het Privacy jaarplan wat door de FG wordt opgesteld.
   De verslagen worden geconsolideerd in de bestuurlijke Planning & Control-cyclus. Waar nodig wordt apart aandacht besteed aan specifieke systemen/applicaties.
   Het jaarplan wordt getoetst op de beschikbaarheid van resources (mensen en middelen), afgezet tegen de risico's die gemitigeerd moeten worden.

5. *Baseline van informatiebeveiligingsmaatregelen*
   Deze baseline beschrijft de maatregelen die minimaal nodig zijn om het voor de OU vastgestelde minimale niveau van informatiebeveiliging te kunnen waarborgen. Dit vloeit voort uit het beleid of uit aanvullende besluiten die door het bestuur genomen zijn. Deze basismaatregelen moeten overal in de instelling worden genomen. De baseline wordt gemaakt door de (C)ISM('s) in overleg met de CISO en vastgesteld in het tactisch IB-overleg. Wanneer er processen of systemen zijn die na een classificatie of andere risicoanalyse (bijvoorbeeld een DPIA) hogere beveiligingseisen nodig hebben, dan worden er aanvullende maatregelen genomen.

6. *Policies*
   Gedragscodes en richtlijnen op het gebied van informatiebeveiliging voor medewerkers, studenten en derden (al dan niet voor specifieke doelgroepen), zoals:
   - Privacybeleid.
   - Gedragscode computergebruik (Acceptable Use Policy), voor het veilig gebruik van IT-faciliteiten, e-mail en internetgebruik door medewerkers, studenten en derden.
   - RFC-2350 voor de lokale OU-CERT (zie hoofdstuk 6. Melding en afhandeling van incidenten (OU-CERT))
   - Beleid Coordinated Vulnerability Disclosure.

Naast bovenstaand organisatorisch beleid zijn de volgende detail beleidsonderwerpen beschreven:

- Beleid voor acquisitie, ontwikkeling en onderhoud van systemen
- Beleid voor beheer van bedrijfsmiddelen
- Beleid voor beveiliging bedrijfsvoering
- Beleid voor communicatiebeveiliging
- Beleid voor cryptografie
- Beleid voor fysieke beveiliging
- Beleid voor informatiebeveiliging in bedrijfscontinuïteitsbeheer
- Beleid voor leveranciersbeheer
- Beleid voor logische toegangsbeveiliging
- Beleid voor naleving
- Beleid voor veilig personeel

Daarnaast is informatiebeveiliging een vast onderdeel van de volgende documenten:

7. *Dienstenovereenkomsten (DVO's, SLA's), inhuur- en uitbestedingscontracten en eventueel bijbehorende verwerkersovereenkomsten*
   Bij de inhuur van personeel en bij de inkoop van middelen (met name hardware, software, applicatie/cloud platforms en diensten), wordt expliciet aandacht aan informatiebeveiliging besteed. Dit wordt gedaan door o.a. het IB-beleid toe te passen op externen en door beveiliging standaardonderdeel van de inkoopvoorwaarden te maken. Afspraken worden in een contract(en) met de leverancier vastgelegd. Het contract bevat standaard een informatiebeveiligingsparagraaf waarin de verantwoordelijkheden van de leverancier zijn opgenomen. De basis hiervoor is het SURF Juridisch Normenkader Cloudservices Hoger Onderwijs[28] die een informatiebeveiliging bijlage bevat.

8. *Business Continuity Plan*
   Het Business Continuity Plan wordt opgesteld op initiatief van de Business Continuity Manager en in samenwerking met het bestuur, de CISO, de proceseigenaren, CIO/Directeur ITF en het afdelingshoofd Operations.

28 https://www.surf.nl/binaries/content/assets/surf/nl/kennisbank/2013/juridisch-normenkader-cloudservices-hoger-onderwijs.pdf

Bijlage H – Inrichting van het OU-CERT

Het doel van het OU-Computer Emergency Response Team (OU-CERT) is het voorkomen van informatiebeveiligingsincidenten en ze te bestrijden als ze zich toch voordoen. Het doel is de continuïteit van de OU te ondersteunen en haar reputatie te beschermen. Het OU-CERT houdt zich ook bezig met beveiligingsincidenten buiten de OU als daar eigen medewerkers in enige rol bij betrokken zijn. In zulke gevallen wordt als dat mogelijk is, gebruikgemaakt van de diensten van SURFcert, die wereldwijd in verbinding staat met andere Computer Security Incident Response Teams (CSIRT's).

De leden van het OU-CERT zijn in die rol benoemd door het bestuur en opereren in haar opdracht.

Het OU-CERT stelt een handvest op waarin doelgroep, opdracht, bevoegdheden, escalaties, werkwijze (inclusief omgang met vertrouwelijkheid) en samenstelling zijn uitgewerkt. Daarin wordt o.a. vastgelegd dat het OU-CERT voor de OU als geheel werkzaam is en haar opdracht direct van het bestuur van de OU krijgt. Ook worden directe escalaties naar het bestuursniveau (via de CISO) vastgelegd. Dit is onderdeel van het algemene calamiteitenprotocol van de OU. Ook worden directe contacten vastgelegd met de afdelingen c.q. personen die binnen de OU zorgdragen voor juridische kwesties en contacten met de pers.

Het OU-CERT is gerechtigd om tijdelijk computersystemen of netwerksegmenten te laten isoleren om haar taak goed te kunnen uitvoeren.

Incidentbeheer en -registratie hebben betrekking op de wijze waarop medewerkers, studenten en derden inbreuken op de informatiebeveiliging melden en de wijze waarop deze worden afgehandeld. Van incidenten kan worden geleerd. Incidentregistratie en periodieke rapportage over opgetreden incidenten horen dan ook thuis in een volwassen informatiebeveiligingsomgeving. Incidenten kunnen bij de OU worden gemeld bij Servicedesk@ou.nl / cert@ou.nl[29] [30]. De OU heeft de contactgegevens van dit meldpunt duidelijk gecommuniceerd naar haar medewerkers, studenten en derden.

Elke medewerker, student en derde is zelf verantwoordelijk voor het signaleren en melden van incidenten en inbreuken op informatiebeveiliging, inclusief datalekken. Incidenten en inbreuken dienen direct gemeld te worden aan het OU-CERT-meldpunt.

Om incidenten op de juiste manier te kunnen afhandelen, worden ze in het relevante operationeel overleg besproken. In het geval het bedrijfsproces, financiën of de goede naam van de OU in gevaar zijn, wordt het incident ook met het bestuur besproken. Als er vanuit het (uitbestede) Security Operations Center of eigen waarneming verontrustende trends worden geconstateerd, dan speelt de OU hierop in door het treffen van extra maatregelen of het creëren van bewustwording binnen de organisatie.

[29] Computer Security Incident Response Team / Computer Emergency Response Team. Zie https://www.ou.nl/security voor meer informatie.
[30] <Servicedesk>@<ou.nl>, tel. +31 45 576 23 06