Informatiebeveiligings- en privacy beleid van de Open Universiteit

Vaststelling & Wijziging

Het Informatiebeveiligingsbeleid beleid wordt jaarlijks geëvalueerd op initiatief van de security officer van de OU.

Project AVG18, document AVG18-3

Open Universiteit
www.ou.nl

document

identificatie	Informatiebeveiligings- en privacybeleid.v24.docx
status	Concept
auteur(s)	Timmermans, Peter
eigenaar	Directeur GSO
datum afdruk	18 mei 2018
opgeslagen	\\srv-hrl-03v\homedir$\tim\Mijn documenten\Informatiebeveiligingsbeleid\Informatiebeveiligings- en privacybeleid.v24.docx

wijzigingshistorie

versie	auteur	datum	wijziging	review
17	TIM	08-05-2015	Geheel nieuwe versie n.a.v. DigiD audit, gebruikmakend van het model van SURFibo.	KDR, OSP, HIL, JFE, RET
18	TIM	13-05-2015	Commentaar verwerkt en relevante beleidsprincipes uit het oude beleid toegevoegd. Rol van CIO beschreven.	RET
19	TIM	29-05-2015	N.a.v. KPMG rapport uitbesteding van dienstverlening en cloud opgenomen.	KDR, RET, RRI
20	TIM	12-06-2015	Commentaar van directeur GSO verwerkt.	KDR
21	TIM	24-06-2015	Commentaar directeur BD verwerkt. Inhoud van §5.4 vervangen door tekst uit het model. In § 5.6 de beschrijving bij Interne IT-auditor aangepast.	RED
22	TIM	03-07-2015	Commentaar Bedrijfsvoeringsoverleg verwerkt, tekstueel. Deze versie is 03-07-2015 vastgesteld door het CvB.	RED
23	Cerrix, TIM	22-1-2018	Binnen project AVG18 het informatiebeveiligingsbeleid geactualiseerd i.v.m. nieuwe ICT-besturingsmodel en met hulp van Cerrix (Ludo Cuijpers en Maurits Toet) is het privacybeleid toegevoegd. In dat verband ook de titel aangepast. In §3.2 is de Governance structuur in overeenstemming gebracht met het advies van de stuurgroep.	JFE, RED, HVW
24	Cerrix, TIM	15-05-2018	Vastgesteld door CvB na advies van UMT en OR.	

Bij het opstellen van het Informatiebeveiligingsbeleid van de Open Universiteit is gebruik gemaakt van het *Model Informatiebeveiligingsbeleid voor het Hoger Onderwijs* van de SURF Community voor Informatiebeveiliging en PRivacy SCIPR.

inhoudsopgave

0. Management Samenvatting 4
1. Inleiding 6
1.1 Algemeen 6
1.2 Doelgroep 7
1.3 Reikwijdte van het informatiebeveiligingsbeleid 7
1.4 Reikwijdte van het privacy beleid 7
1.5 Vervlechting informatiebeveiliging en privacy 8
2. Doelstelling 9
2.1 Afspraken 9
2.2 Beleidsuitgangspunten en –principes van informatiebeveiliging en privacy 9
3. Governance informatiebeveiligings- en Privacy beleid 13
3.1 Afstemming met samenhangende Risico's 13
3.2 Inpassing in I-governance 13
3.3 Documenten informatiebeveiliging en privacy 15
3.4 Controle, naleving en sancties 16
3.5 Bewustwording en training 16
3.6 Overleg 16
4. Compliance 18
4.1 Wet- en regelgeving 18
4.2 Afspraken in de cao 19
4.3 Vastgestelde beleidsdocumenten van de OU 19
5. Melding en afhandeling van incidenten 21
5.1 Datalekken 21
5.2 Andere informatiebeveiligingsincidenten (CERT) 21
Bijlage A. Rollen m.b.t. informatiebeveiliging en privacy 23
Bijlage B. Bronnen 26

0. Management Samenvatting

Informatie technologie (IT) en informatie management (IM) zijn niet meer weg te denken uit onze bedrijfsvoering. Bijna alle processen zijn afhankelijk van een goede en ongestoorde werking van IM en IT. Dat geldt net zo zeer voor het primaire proces als voor secundaire en ondersteunend processen zoals financieel management of personeelszaken. Zonder werkende IT geen onderzoek of onderwijs, geen facturering, geen uitbetaalde salarissen, geen werkende toegangscontrole, enzovoorts.

Daarom is evident dat het hoogste management zich verantwoordelijk weet voor IM en IT. De voorzitter van het College van bestuur (CvB) van de Open Universiteit (OU) heeft als gemandateerd portefeuillehouder voor Informatiebeveiliging en privacy de decaan PenOW en de directeur GSO aangewezen. De portefeuillehouder is daarmee verantwoordelijk voor de Informatiebeveiliging en het privacy beleid van de OU.

Informatiebeveiliging en privacy zijn direct gerelateerd aan de missie en prioriteiten van de organisatie. De mate waarin aandacht besteed wordt aan Informatiebeveiliging en privacy is afgeleid van de business impact die inbreuken op de informatiebeveiliging en privacy kunnen veroorzaken: aan het Informatiebeveiligings- en privacy beleid ligt dus altijd een business case ten grondslag. Met behulp van risicoanalyse kan een inschatting van de risico's en business cases worden gemaakt, om daar vervolgens een passende informatiebeveiliging en privacy -structuur en -maatregelen op te kunnen baseren.

Informatiebeveiliging en privacy gaan over alle IT- en informatiemiddelen en –processen. Bij informatiebeveiliging zijn met name de volgende 3 kwaliteitscriteria van belang:

Beschikbaarheid[1]
De mate waarin de beschikbaarheid en ongestoorde voortgang van de ict-dienstverlening gewaarborgd is.

Integriteit
De mate waarin de volledigheid, juistheid en tijdigheid van de IT-dienstverlening gewaarborgd is.

Vertrouwelijkheid
De mate waarin uitsluitend geautoriseerde personen gebruik kunnen maken van de gegevens of diensten.

Een aanvullend kwaliteitscriterium is **controleerbaarheid**: niet alleen "weten" of iets in orde is, maar dat ook achteraf kunnen "verifiëren".

In dit verband definiëren wij privacy als volgt:
Privacy
De mate waarin de verwerking van Persoonsgegevens voldoet aan de eisen die de wet daaraan stelt.

Ten overvloede: Informatiebeveiliging en privacy is géén primair of secundair proces, géén core business, maar als je er niets aan doet gaat het wel ten koste van de core business: Informatiebeveiliging en privacy zijn dus belangrijke business enablers. Het bestuur van de organisatie zorgt dan ook voor een goede governance, inclusief auditing en feedback, ook wel I-governance genoemd. Deze is cruciaal en management commitment is daarbij essentieel.

Dit informatiebeveiligings- en privacy beleid wordt daarom door het CvB van de OU vastgesteld en gedragen en geldt voor de gehele organisatie en allen die daarbij betrokken zijn in wat voor functie dan ook.

Betrokkenheid van het hoogste management is dus noodzakelijk, maar niet voldoende. Informatiebeveiliging en privacy zijn binnen de OU nadrukkelijk ieders verantwoordelijkheid. Dit wordt zowel uitgedragen langs formele weg, als via bewustwordingscampagnes en scholing. Het lijnmanagement heeft daarbij een speciale rol: zij hebben de taak om randvoorwaardelijk toe te zien op goede naleving van de afspraken rondom informatiebeveiliging en privacy.

Kortom, informatiebeveiliging en privacy werken het best wanneer de hele organisatie hierin participeert. Dat is een continu proces. Dit beleid is daarvoor het uitgangspunt. Beschreven worden niet alleen de voornoemde kwaliteitscriteria, maar ook:
- welke rollen ingevuld moeten zijn,

[1] Definities gebaseerd op NOREA, waarbij de nadruk op *maatregelen* is verwijderd.

- hoe informatiebeveiliging en privacy onderdeel wordt van de Planning & Control cyclus,
- hoe beveiligingsincidenten aangepakt worden (en hoe ze worden voorkómen),
- welke wettelijke randvoorwaarden van toepassing zijn.

Qua rolverdeling springen een aantal cruciale rollen eruit[2]: Functionaris voor de gegevensbescherming (FG), Security officer (SO) / Privacy officer (PO), Information security manager (ISM), CERT OU.

[2] De omschrijvingen van alle rollen staan in Bijlage A Rollen m.b.t. informatiebeveiliging en privacy

1. Inleiding

1.1 Algemeen

Onder Informatiebeveiliging en privacy wordt verstaan het treffen en onderhouden van een samenhangend pakket aan maatregelen om de kwaliteitscriteria beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening alsmede de privacy van de Persoonsgegevens te waarborgen.

Beschikbaarheid
De mate waarin de beschikbaarheid en ongestoorde voortgang van de ict-dienstverlening gewaarborgd is.

Integriteit
De mate waarin de volledigheid, juistheid en tijdigheid van de IT-dienstverlening gewaarborgd is.

Vertrouwelijkheid
De mate waarin uitsluitend geautoriseerde personen gebruik kunnen maken van de gegevens of diensten, al dan niet gereguleerd door (geautomatiseerde) procedures en/of technische maatregelen.

Privacy
De mate waarin de verwerking van Persoonsgegevens voldoet aan de eisen die de wet daaraan stelt. Die eisen hebben betrekking op het voldoen aan de volgende beginselen:

- Rechtmatigheid: verwerking van Persoonsgegevens is rechtmatig;
- Eerlijkheid: verwerking van Persoonsgegevens is behoorlijk;
- Transparantie: verwerking van Persoonsgegevens is transparant;
- Doelbinding: Persoonsgegevens worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden verzameld en vervolgens niet op onverenigbare wijze verwerkt;
- Dataminimalisatie: Persoonsgegevens zijn adequaat en ter zake dienend en blijven beperkt tot datgene wat minimaal nodig is voor de doeleinden waarvoor zij worden verwerkt;
- Juistheid: Persoonsgegevens zijn juist en worden zo nodig geactualiseerd;
- Opslagbeperking: Persoonsgegevens worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de Persoonsgegevens worden bewaard noodzakelijk is;
- Integriteit en vertrouwelijkheid: Persoonsgegevens worden door passende technische of organisatorische maatregelen op een dusdanige manier verwerkt dat een passende beveiliging gewaarborgd is;
- Verantwoordingsplicht: Persoonsgegevens worden verwerkt onder de verantwoordelijkheid van de verwerkingsverantwoordelijke, die ervoor zorgt en kan aantonen dat verwerking voldoet aan de bepalingen van de verordening.

Hierbij gaat het ook om de **Controleerbaarheid**: de mate waarin het mogelijk is om achteraf de waarden van de parameters waarin beschikbaarheid, integriteit, vertrouwelijkheid of privacy worden uitgedrukt, te verifiëren. Zulke parameters zijn bijvoorbeeld downtime, toegang en transacties.

Informatiebeveiliging en privacy is een beleidsverantwoordelijkheid van het CvB van de OU. Zoals overal in de maatschappij is ook bij de OU sprake van toenemende afhankelijkheid van IM en IT. Daarom is het van belang adequate maatregelen te treffen. Immers, onvoldoende informatiebeveiliging en privacy kan leiden tot onacceptabele risico’s voor het bedrijfsproces van de OU. Incidenten en inbreuken in bedrijfsprocessen kunnen leiden tot financiële schade en imagoverlies.

Informatiebeveiliging en privacy zelf is géén primair of secundair proces, géén core business, maar als je er niets aan doet gaat het wel ten koste van de core business: informatiebeveiliging en privacy zijn belangrijke business enablers.

De OU heeft de ambitie om met het onderhavige beleidsdocument informatiebeveiliging en privacy structureel naar een hoog niveau te brengen en daar te houden, door de onderwerpen governance (inclusief auditing en feedback), wet- en regelgeving, de organisatie van de beveiligingsfunctie en het informatiebeveiligings- en privacy beleid – ook in hun onderlinge relatie – duidelijk te beschrijven en vast te stellen.

1.2 Doelgroep

Het informatiebeveiligings- en privacy beleid bij de OU richt zich primair op het hoger management, de beveiligingsorganisatie en leidinggevenden. Het is van toepassing op alle medewerkers in loondienst, onderzoekers, studenten, belangstellenden, alumni, externe medewerkers, bestuurders, gasten, bezoekers en relaties. Kortom, op iedereen die – intern dan wel extern – op enige manier te maken heeft met (aspecten van) het bedrijfsproces bij de OU.

1.3 Reikwijdte van het informatiebeveiligingsbeleid

In deze paragraaf wordt beschreven wat de afbakening is van het toepassingsgebied van dit beleid.

Bij de OU wordt informatiebeveiliging breed geïnterpreteerd en betreft dus alle vormen van informatie, niet alleen digitale informatie. Er bestaat een belangrijke relatie en een gedeeltelijke overlap met risico's zoals *safety*[3], fysieke beveiliging en *business continuity*. Op strategisch niveau wordt aandacht geschonken aan deze raakvlakken en wordt zowel planmatig als inhoudelijk afstemming gezocht.

Het informatiebeveiligingsbeleid binnen de OU heeft betrekking op de doelgroep zoals beschreven in § 1.2 alsmede op alle instellingsonderdelen en dienstverlening. Tevens vallen onder het informatiebeveiligingsbeleid in beginsel alle door de OU beheerde clients van waaraf geautoriseerde[4] toegang tot (diensten van) het de OU netwerk verkregen kan worden. Hoewel de OU geen verantwoordelijkheid draagt ten aanzien van onbeheerde clients, valt het gebruik hiervan in combinatie met de ict-faciliteiten van de OU ook onder dit informatiebeveiligingsbeleid.

Bij het informatiebeveiligingsbeleid ligt de nadruk op die toepassingen die vallen onder de verantwoordelijkheid van de OU. Dit heeft zowel betrekking op beheerste informatie, die door de OU zelf is gegenereerd en wordt beheerd, als op niet- beheerste informatie, bijv. uitspraken van medewerkers in discussies op elektronische platforms van de OU, persoonlijke websites of pages op publieke fora, waarop de OU kan worden aangesproken.

1.4 Reikwijdte van het privacy beleid

Opslag en verwerking van Persoonsgegevens is noodzakelijk om te voldoen aan wettelijk voorgeschreven uitwisselingen van gegevens en voor de bedrijfsprocessen van de OU. Dit gebeurt met de grootste zorgvuldigheid omdat misbruik van Persoonsgegevens grote schade kan berokkenen aan Betrokkenen, maar ook aan de OU zelf. De OU beschermt de Persoonsgegevens die aan haar worden verstrekt en draagt zorg voor een zorgvuldig beheer en verwerking van die Persoonsgegevens. Het op een juiste manier verwerken van Persoonsgegevens is de verantwoordelijkheid van het CvB.

Het privacy beleid heeft betrekking op het beheer en verwerken van Persoonsgegevens van alle Betrokkenen bij de OU waaronder in ieder geval de doelgroep zoals beschreven in § 1.2 evenals op andere Betrokkenen waarvan de OU Persoonsgegevens beheert of verwerkt.

[3] Safety wordt als verzamelterm gebruikt voor de verschillende aspecten van personele veiligheid: Arbo en milieu, sociale veiligheid, bedrijfshulpverlening e.d.
[4] Ongeautoriseerde toegang is per definitie een beveiligingsincident – hiervoor geldt dat dit door de CERT functie van de OU afgehandeld wordt, zodra het incident bekend is.

In het beleid ligt de nadruk op het vermijden van onrechtmatige verwerking van Persoonsgegevens. Zie voor de eisen van rechtmatige verwerking de definitie van privacy in §1.1. Waar is vastgesteld dat sprake is van rechtmatige verwerking, 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.

Uitgangspunt is dat de persoonlijke levenssfeer van de Betrokkene wordt gerespecteerd. De rechtmatig verwerkte Persoonsgegevens worden beschermd tegen onwettelijk en ongeautoriseerd gebruik dan wel misbruik. Die bescherming is gebaseerd op het fundamenteel recht van Betrokkenen op bescherming van hun Persoonsgegevens. Dit brengt met zich mee dat het beheer en verwerken van Persoonsgegevens bij de OU voldoet aan relevante wet- en regelgeving en dat Persoonsgegevens veilig zijn bij de OU.

1.5 Vervlechting informatiebeveiliging en privacy

Het waarborgen van de beschikbaarheid, de integriteit en de vertrouwelijkheid van de verwerkte Persoonsgegevens levert een essentiële bijdrage aan de realisatie van het privacy beleid.

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. Het door de OU gevoerde informatiebeveiligings- en privacy beleid wordt bekend gemaakt aan studenten, medewerkers, externen, etc.

Naast bovenstaande concrete doelstellingen is een meer algemeen doel het instellingsbreed creëren van bewustwording van het belang en de noodzaak van het beschermen van Persoonsgegevens, mede ter vermijding van risico’s als gevolg van het niet voldoen aan de relevante wet- en regelgeving.

2. Doelstelling

2.1 Afspraken

Als mission statement geldt:

> *Het Informatiebeveiligings- en privacy beleid bij de OU heeft als doel het waarborgen van de continuïteit van het bedrijfsproces[5] en het minimaliseren van de schade door het voorkómen van privacy- en beveiligingsincidenten en het minimaliseren van eventuele gevolgen van deze incidenten.*

Daarmee is informatiebeveiligings- en privacy beleid direct ondersteunend voor de missie en het proces van de instelling als geheel. De eindverantwoordelijkheid ligt bij de CvB-voorzitter.

Uit dit mission statement komen de volgende afgeleide doelstellingen voort:

- Kader: het beleid biedt een kader om (toekomstige) maatregelen in de informatiebeveiliging en privacy te toetsen en om de taken, bevoegdheden en verantwoordelijkheden in de instelling te beleggen.
- Normen: de basis voor de inrichting van het OU informatiebeveiligings- en privacy management is dit beleidsdocument, waarvoor ISO 27001 als voorbeeld diende. Formele certificering conform ISO 27001 wordt voor de OU niet als noodzakelijk gezien.
- Maatregelen: maatregelen worden genomen op basis van best practices in de SURF doelgroep, waarbij het op ISO 27002 gebaseerde Toetsingskader als uitgangspunt wordt genomen.
- Expliciet vastgestelde beveiligingsorganisatie: uitgangspunten en organisatie van informatiebeveiligings- en privacy functies zijn vastgelegd in dit beleid en worden gedragen door de hele instelling.
- Daadkrachtige procesbenadering: dit beleid beschrijft duidelijke keuzes in maatregelen, actieve controle op beleidsmaatregelen en de uitvoering daarvan, zodat die in de hele instelling worden toegepast.
- Compliance: het beleid biedt de basis om te voldoen aan de wettelijke voorschriften.

2.2 Beleidsuitgangspunten en –principes van informatiebeveiliging en privacy

Informatiebeveiligings- en privacy management wordt als proces ingericht. De OU kiest ervoor om de jaarlijkse planning en controlecyclus te baseren op “Plan, Do, Check, Act” (zie nevenstaande figuur). Hierin worden jaarlijks plannen gemaakt en uitgevoerd. De resultaten ervan worden geëvalueerd en vertaald naar nieuwe jaarplanningen. Deze planningen zullen op strategisch niveau zijn opgenomen in de OU planning, en meer in detail in de IT jaarplannen. Deze aanpak sluit aan bij het volwassenheidsniveau 4 van het Toetsingskader SURFaudit.

2.2.1 Beleidsuitgangspunten

1) De OU eist goede informatiebeveiliging en privacy en de bijbehorende bewustwording.
2) De OU is een instelling met een open karakter. Adequate beveiliging is daarbij wel een randvoorwaarde. Er wordt van medewerkers, studenten en derden verwacht dat ze zich qua techniek en ook qua houding ‘fatsoenlijk’ gedragen (eigen verantwoordelijkheid). Niet acceptabel is dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagoverlies. In paragraaf 3.3 wordt verwezen naar de relevante documenten die van toepassing zijn.
3) Het succes van informatiebeveiliging en privacy staat of valt met goede communicatie. Goede communicatie wordt daarom actief bevorderd, op en tussen alle niveaus in de instelling.
4) Het Informatiebeveiligings- en privacy beleid waarborgt de volgende kwaliteitscriteria:
   a) Beschikbaarheid
   b) Integriteit
   c) Vertrouwelijkheid

[5] Onderwijs en onderzoek worden nadrukkelijk als bedrijfsprocessen gezien.

d) Privacy.

2.2.2 Beleidsprincipes informatiebeveiliging en privacy

1. Informatiebeveiliging en privacy is ieders verantwoordelijkheid: van ieder individu wordt verwacht dat hij/zij communiceert met medewerkers, studenten en derden dat er van hen verwacht wordt dat ze actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie, waaronder Persoonsgegevens. Dat gebeurt in de aanstellingsbrief, tijdens RenO-gesprekken, met een gedragscode, met periodieke bewustwordingscampagnes, in contracten met tijdelijk personeel en leveranciers, enzovoorts. Het zo nodig opleggen van sancties na overtredingen maakt het geheel geloofwaardig.
2. Informatiebeveiliging en privacy is een lijnverantwoordelijkheid: dat betekent dat de leidinggevenden de verantwoordelijkheid dragen voor een goede informatiebeveiliging en privacy in hun organisatieonderdeel. Dit omvat ook de keuze van maatregelen en de uitvoering en handhaving ervan binnen de gestelde kaders.
3. Informatiebeveiliging en privacy is een continu proces: technologische en organisatorische ontwikkelingen binnen en buiten de OU maken het noodzakelijk om periodiek te bezien of men nog wel op de juiste wijze bezig is de beveiliging en de privacy te waarborgen. Audits maken het mogelijk het beleid en de genomen maatregelen te controleren op effectiviteit (controleerbaarheid).
4. Elk bedrijfsproces[6], elk informatiesysteem en elk gegeven en heeft een eigenaar. Binnen de OU kunnen alleen decanen en directeuren eigenaar zijn. Zij kunnen dit eigenaarschap (sub-)mandateren aan medewerkers. Om nodeloze complexiteit te vermijden, is de eigenaar van het bedrijfsproces in beginsel[7] ook eigenaar van de gebruikte informatiesystemen en gegevens. De proceseigenaar bepaalt welke gebruikers welke bevoegdheden hebben met betrekking tot dat bedrijfsproces. Als dat proces met een informatiesysteem wordt ondersteund, dan worden die bevoegdheden geïmplementeerd als autorisaties in dat informatiesysteem.
5. De OU is geen eigenaar van Persoonsgegevens. De OU krijgt deze Persoonsgegevens in bruikleen van de Betrokkene en gaat daar zorgvuldig mee om cf. de AvG. Persoonsgegevens worden uiterlijk bij het aanbreken van de vastgestelde vernietigingstermijn vernietigd.
6. De OU is in de zin van de AvG de Verantwoordelijke voor de Persoonsgegevens die zij verwerkt. Die rol is door het CvB gemandateerd aan:
   - de decanen van de faculteiten voor wat betreft de persoonsgegevens van proefpersonen in wetenschappelijk onderzoek van de eigen faculteit. De decaan PenOW treedt hierbij op als aanspreekpunt/ vertegenwoordiger van de decanen.
   - de directeur GSO voor wat betreft alle andere Persoonsgegevens.

   Andere bedrijfsprocessen en systemen kunnen die Persoonsgegevens slechts raadplegen en verrijken met schriftelijke toestemming van de Verantwoordelijke en de FG.
7. De OU is in beginsel eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert de OU informatie, waarvan het intellectueel eigendom toebehoort aan derden. Medewerkers, studenten en derden worden goed geïnformeerd over de regelgeving voor het (her)gebruik van deze informatie.
8. Waardering van informatie: iedereen behoort de waarde van informatie te kennen en daarnaar te handelen. Deze waarde wordt bepaald door de schade die kan optreden als gevolg van verlies van beschikbaarheid, integriteit en vertrouwelijkheid. Het classificatiekader is leidend bij de bepaling van de waarde.
9. De privacy en de beveiliging van de informatievoorziening worden primair gerealiseerd door algemene maatregelen die onafhankelijk zijn van de individuele gebruiker. Door de maatregelen in hoge mate dwingend op te leggen en dus niet afhankelijk te laten zijn van de discipline van de gebruiker, kan een minimum niveau van informatiebeveiliging en privacy worden gegarandeerd.

[6] Voor de afbakening van de bedrijfsprocessen baseert de OU zich op de *Hoger Onderwijs Referentie Architectuur* (HORA).
[7] Er is een uitzondering gemaakt voor het eigenaarschap van Persoonsgegevens. Dat is gemandateerd aan de decaan PenOW en de directeur GSO.

10. Bij elke mutatie van de informatievoorziening – al dan niet in projectverband – zoals infrastructurele wijzigingen of de aanschaf of wijziging van systemen, wordt reeds in het vroegst mogelijke stadium rekening gehouden met informatiebeveiliging. Voor zover de betreffende systemen Persoonsgegevens verwerken, wordt bij nieuwe systemen privacy by design / default toegepast en wordt bij mutaties in bestaande systemen minstens een Privacy Impact Assessment (PIA) uitgevoerd.
11. Bij elke IT-inrichting wordt ter bevordering van informatiebeveiliging en privacy het principe van least privileges gehanteerd, wat wil zeggen dat er steeds naar wordt gestreefd om niet meer dan die rechten te verlenen die noodzakelijk zijn voor adequate functie- en bedrijfsuitoefening.
12. De OU streeft ernaar om alle gegevens en systemen waarop dit informatiebeveiligings- en privacy beleid van toepassing is te classificeren. Daarbij wordt gekeken naar de aspecten beschikbaarheid, integriteit en vertrouwelijkheid. Voor elk van deze aspecten wordt een klein aantal klassen gedefinieerd. Het niveau van de te treffen beveiligingsmaatregelen is afhankelijk van deze klassen. De huidige stand van zaken qua classificatie is te vinden in het document AVG18-7 Classificatiekader OU.
13. Ict-voorzieningen aan externen worden alleen o.g.v. een Service Level Agreement (SLA) geleverd. Indien de OU ict-voorzieningen levert aan een andere organisatie, wordt met die andere organisatie een SLA afgesloten door de OU. Om misverstanden over de te leveren voorzieningen te voorkomen worden voorzieningen tijdig en expliciet beschreven. Dat kan alleen als de leverancier van de voorziening (de OU) en de klant (de externe organisatie) daarbij betrokken zijn.
14. Uitbesteding. Waar de OU (delen van) haar informatievoorziening door externe partijen laat verzorgen, ziet zij er op toe dat deze externe partijen binnen de kaders van dit informatiebeveiligings- en privacy beleid handelen. De proceseigenaar ziet er op toe dat dit in een overeenkomst met de externe partijen wordt vastgelegd. In deze overeenkomst wordt opgenomen dat de OU het recht heeft om te (laten) controleren of de externe partij inderdaad conform dit informatiebeveiligings- en privacy beleid handelt. Indien de uitbestede informatievoorziening Persoonsgegevens bevat, is ook beleidsprincipe 27 van toepassing. De genoemde overeenkomst wordt per 25 mei 2018 aangeduid als Verwerkersovereenkomst.
15. Elke Verwerking van Persoonsgegevens is gebaseerd op de AvG.
16. Persoonsgegevens worden alleen verwerkt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de Verwerking geformuleerd.
17. Bij een Verwerking van Persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt tot de Persoonsgegevens die strikt noodzakelijk zijn voor het specifieke doeleinde. De gegevens dienen met het oog op dat doel toereikend, ter zake dienend en niet bovenmatig te zijn.
18. Verwerking van Persoonsgegevens gebeurt op de minst ingrijpende wijze en staat in redelijke verhouding tot het beoogde doeleinde.
19. Er worden maatregelen getroffen om zoveel mogelijk te waarborgen dat de te verwerken Persoonsgegevens juist en actueel zijn.
20. Persoonsgegevens worden adequaat beveiligd volgens de geldende beveiligingsnormen.
21. Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.
22. Persoonsgegevens worden niet langer verwerkt dan noodzakelijk is voor de doeleinden van de Verwerking, hierbij worden de van toepassing zijnde bewaar- en vernietigtermijnen in acht genomen.
23. Iedere Betrokkene heeft recht op inzage respectievelijk verbetering, aanvulling, verwijdering of afscherming van de in de afzonderlijke Verwerkingen hem betreffende Persoonsgegevens, en heeft het recht van verzet.
24. De OU kan aan Betrokkenen op transparante wijze verantwoording afleggen over welke gegevens er allemaal verzameld worden en over de verwerkingen daarvan en de daarbij gehanteerde principes.

25. Bij alle registraties op vrijwillige basis wordt aan de Betrokkene altijd, voor bijvoorbeeld het plaatsen van foto's op social media of publicaties, aantoonbare toestemming (zogenaamde Opt-in) gevraagd en daarnaast krijgt de Betrokkene de mogelijkheid om zijn toestemming weer in te trekken (de zogenaamde Opt-out).
26. Om de privacy te kunnen waarborgen, wordt elk persoonsgegeven op de OU op één plaats bewaard tenzij de OU daar toestemming heeft gegeven om daarvan af te wijken.
27. Opslag van Persoonsgegevens buiten het eigen rekencentrum. Waar de OU Persoonsgegevens opslaat buiten het eigen rekencentrum (al dan niet in de cloud) wordt uitsluitend gebruik gemaakt van diensten waarmee de OU een Verwerkersovereenkomst heeft afgesloten. Die Verwerkersovereenkomst waarborgt dat de Persoonsgegevens cf. de AvG en de regels van de Autoriteit Persoonsgegevens worden verwerkt. De FG ziet daarop toe.

3. Governance informatiebeveiligings- en Privacy beleid

Het goed, efficiënt en verantwoord leiden van een instelling wordt vaak aangeduid met de term governance. Het omvat vooral ook de relatie van de instelling met de belangrijkste belanghebbenden zoals de proceseigenaren, medewerkers, studenten, klanten en derden. Een goede governance zorgt er voor dat alle belanghebbenden hun rechten en plichten kennen.

In dit hoofdstuk worden diverse rollen onderscheiden. Het aantal rollen is als regel groter dan het aantal personen dat die rollen vervult.

3.1 Afstemming met samenhangende Risico's

Onderdeel van governance is dat aan alle soorten risico's en hun onderlinge verwevenheid passende aandacht geschonken wordt. Het is om die reden dat bij de OU op strategisch niveau zowel aandacht geschonken wordt aan informatiebeveiliging en privacy, als aan safety, fysieke beveiliging en business continuity. Immers, samenwerking op het gebied van deze risico's is een noodzakelijke voorwaarde voor goede governance. Dit wordt bevorderd door de planningscyclus voor deze gebieden zo veel mogelijk parallel te laten verlopen. Daardoor kan de gewenste kruisbestuiving optreden. Waar mogelijk en nodig wordt deze afstemming ook vertaald naar het tactische en operationele niveau.

In dit hoofdstuk wordt verder ingegaan op de governance van de informatiehuishouding (verder I-governance te noemen) en de positionering van informatiebeveiliging daarin.

3.2 Inpassing in I-governance

In deze paragraaf wordt beschreven hoe informatiebeveiliging en privacy als onderdeel van I-governance zijn georganiseerd en wie waarvoor verantwoordelijk is. Van belang daarbij is om onderscheid te maken naar richtinggevend of strategisch, sturend of tactisch en uitvoerend niveau. Wat betreft de benaming van rollen wordt zoveel mogelijk aangesloten bij het PvIB[8].

Niveau	Wat?	Wie?[9]	Overleg	Documenten
Richtinggevend	Bepalen strategie voor privacy en informatiebeveiliging.	CvB, op advies van UMT na instemming van de OR Portefeuillehouder	UMT	Informatiebeveiligings- en privacy beleid
	Organisatie inrichten t.b.v. informatiebeveiliging en privacy. Informatiebeveiliging en privacy planning en control vaststellen. Business continuity management. Communicatie naar management en organisatie.	Portefeuillehouder	UMT	Informatiebeveiliging en privacy *baselines* (basismaatregelen) *Business continuity plan*

[8] Functies in de informatiebeveiliging. Platform informatiebeveiliging (PvIB), 2006.
[9] De hier genoemde rollen worden toegelicht in Bijlage A Rollen m.b.t. informatiebeveiliging en privacy.

Niveau	Wat?	Wie?[9]	Overleg	Documenten
Sturend	Planning & Control informatiebeveiliging en privacy: • Voorbereiden normen en wijze van toetsen • Evalueren beleid en maatregelen • Begeleiding audits • Communicatie naar eigenaren	Interne auditor, hierbij ondersteund door SO/PO. Indien nodig wordt een IT-auditor ingehuurd.	Interne auditor (eventueel externe IT-auditor) en FG (FG is mede ondertekenaar)	Risicoanalyses en audits
	Opstellen Jaarverslag en Jaarplan	SO/PO, gehoord de FG en interne auditor, in opdracht van de directeur Bestuursdienst		Jaarverslag en –plan
	Toetsen projectvoorstellen op de toepassing van het Informatiebeveiligings- en privacy beleid	Informatie manager	IT-Beraad	Goedgekeurde projectvoorstellen
Uitvoerend	Implementeren informatiebeveiliging en privacy maatregelen Communicatie eindgebruikers	FenI i.s.m. eigenaren proces- en Persoonsgegevens en in overleg met SO/PO ISM's	Operationeel overleg	SLA's (*security* paragraaf)
	Registreren, evalueren en (doen) oplossen incidenten	CERT-coördinator / SO	CERT overleg	Incidentregistratie incl. evaluatie
	Registreren, evalueren en (doen) oplossen datalekken	Coördinator onderzoeksteam	Onderzoeksteam	Verslagen van afhandeling van datalekken.
	Na overleg met het CvB melden datalekken bij de AP	FG en SO/PO		Verslagen van meldingen van datalekken.

Tabel 1 Samenvatting van de governance structuur

De financiering van informatiebeveiliging wordt bij de OU als volgt geregeld:

- Algemene zaken, zoals het opstellen van een informatiebeveiligings- en privacy plan voor de instelling of een externe audit, worden uit de algemene middelen betaald. Algemene instelling brede bewustwordingscampagnes en trainingen worden eveneens uit deze middelen betaald.
- De beveiliging van informatiesystemen, inclusief de kosten daarvan, zijn integraal onderdeel van verantwoord beheer van het betreffende informatiesysteem. Beveiligingskosten van werkplekken maken integraal onderdeel uit van de werkplekkosten. Voorlichting en training voor specifieke toepassingen of doelgroepen worden uit infrastructurele budgetten betaald.

Hoe en waar de financiering ook geregeld is, de ervaring leert dat rekening gehouden moet worden met onvoorziene kosten voortvloeiende uit het Informatiebeveiligings- en privacy beleid.

3.3 Documenten informatiebeveiliging en privacy

Voor informatiebeveiliging en privacy wordt bij de OU dezelfde managementcyclus gevolgd, die ook voor andere onderwerpen geldt.

1. Dit Informatiebeveiligings- en privacy beleid:
   Het Informatiebeveiligings- en privacy beleid ligt ten grondslag aan de aanpak van informatiebeveiliging en privacy binnen de OU. In het Informatiebeveiligingsbeleid worden de randvoorwaarden en uitgangspunten vastgelegd en wordt richting gegeven aan de vertaling van het beleid in concrete maatregelen. Om er voor te zorgen dat het beleid gedragen wordt binnen de instelling en die er ook naar handelt, wordt het uitgedragen door (of namens) de CvB-voorzitter. Het informatiebeveiligings- en privacy beleid wordt opgesteld door de SO/PO en met advies van de Informatie manager en FG in het UMT vastgesteld door het CvB.

2. Jaarplan/verslag:
   Elk jaar leveren de SO/PO een jaarverslag en een jaarplan voor het volgende jaar in bij de portefeuillehouder. Het jaarplan is mede gebaseerd op de resultaten van de periodieke controles / audits. Er wordt o.a. ingegaan op incidenten, resultaten van risicoanalyses (incl. genomen maatregelen) en andere initiatieven die het afgelopen jaar hebben plaatsgevonden. Dergelijke verslagen kunnen geconsolideerd worden in de bestuurlijke Planning & Control-cyclus. Waar nodig wordt apart aandacht besteed aan specifieke systemen/applicaties.

3. Baseline van IT informatiebeveiligings- en privacy maatregelen (basisniveau maatregelen):
   Deze baseline beschrijft de maatregelen die minimaal nodig zijn om de OU breed een minimaal niveau van informatiebeveiliging en privacy te kunnen waarborgen. Dit vloeit voort uit het beleid of uit besluiten die door het CvB genomen zijn. Deze basismaatregelen worden dus overal in de instelling getroffen. De baseline wordt opgesteld door de SO/PO en goedgekeurd door de portefeuillehouder. Wanneer er systemen zijn die na een risicoanalyse hogere beveiligings- en privacy eisen nodig hebben, dan worden aanvullende maatregelen genomen.

4. Policies:
   Gedragscodes en richtlijnen voor medewerkers, studenten en derden, al dan niet voor specifieke doelgroepen, op het gebied van informatiebeveiliging. Met name:
   - Reglement computergebruik medewerkers en studenten Open Universiteit voor het veilig gebruik van IT-voorzieningen, e-mail en Internet;
   - Reglement bescherming persoonsgegevens Open Universiteit;
   - Richtlijn Authenticatie.

Daarnaast is informatiebeveiliging een vast onderdeel van de volgende documenten:

5. Business Continuity Plan:
   Business Continuity Management (BCM) is de benaming van het proces dat potentiële bedreigingen voor een instelling identificeert en bepaalt wat de impact op de “operatie” van de instelling is als deze bedreigingen daadwerkelijk manifest worden. Het product van BCM bestaat uit een samenhangend stelsel van maatregelen, die zowel preventief, detectief, correctief als repressief werkzaam zijn. Disaster Recovery is derhalve onderdeel van BCM.

   Het Business Continuity Plan wordt opgesteld op initiatief van de Business Continuity Manager, in samenwerking met de portefeuillehouder, de SO en de proceseigenaren.

6. Service Level Agreements (SLA’s):
   Voor diensten van een externe leverancier worden afspraken in een contract vastgelegd. In deze contracten zit standaard een informatiebeveiligings- en privacy paragraaf, waarin de verantwoordelijkheden van de leverancier zijn opgenomen.

7. Inhuur- en uitbestedingscontracten:
   Bij de inhuur van personeel, maar ook bij de inkoop van middelen (met name hardware, software en applicatie/cloud platforms), wordt expliciet aandacht aan informatiebeveiliging en privacy besteed, onder andere door dit beleid ook toe te passen op externen, en door beveiliging en privacy standaard onderdeel van de inkoopvoorwaarden te maken.

3.4 Controle, naleving en sancties

Bij de OU is de interne auditor verantwoordelijk voor de interne audits en voor de controle op de uitvoering van de informatiebeveiligings- en privacy jaarplannen. Daar waar externe IT expertise nodig is wordt een IT-auditor ingehuurd. De SO/PO en de ISM's ondersteunen daarbij.

Interne audits vinden jaarlijks plaats en hebben bij voorkeur een divers karakter (brainstorms, steekproeven, penetration testing, testen van policies, informatiebeveiliging/CERT firedrills).

De bedrijfskritische informatiesystemen van de OU worden intern geaudit. Deze audits richten zich op de classificatie van de in het informatiesysteem vastgelegde gegevens (Persoonsgegevens en andere gegevens), op de inventarisatie van de risico's, op de genomen beveiligingsmaatregelen en op de samenhang tussen deze drie onderwerpen. Elk informatiesysteem wordt tenminste eens per twee jaar geaudit. Indien een informatiesysteem wordt vervangen of indien zich significante wijzigingen voordoen in de implementatie van de beveiliging, wordt op dat moment een audit uitgevoerd.

De externe controle wordt in een cyclus van 4 jaar uitgevoerd door een onafhankelijke partij. Dit is qua tijdsplanning gekoppeld met het accountantsonderzoek en wordt zoveel mogelijk gecoördineerd met de normale Planning & Control cyclus.

De bevindingen van de externe controles, evenals mogelijke externe eisen t.a.v. beveiliging, zijn input voor de nieuwe jaarplannen van de OU. Deze kunnen ook tot wijziging van dit beleid leiden.

De naleving bestaat uit concreet toezicht op de dagelijkse praktijk van het informatiebeveiligings- en privacy management proces. Van belang hierbij is dat leidinggevenden (inclusief onderzoeks- en onderwijsverantwoordelijken) de medewerkers en studenten aanspreken in geval van tekortkomingen.

Mocht de naleving ernstig tekort schieten, dan kan de OU de betrokken verantwoordelijke medewerkers of studenten een sanctie opleggen, binnen de kaders van arbeids- en studieovereenkomsten en de wettelijke mogelijkheden. Dit is primair een verantwoordelijkheid van de verantwoordelijke leidinggevenden en het CvB.

3.5 Bewustwording en training

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging en privacy uit te sluiten. De mens zelf creëert de grootste risico's. Daarom wordt bij de OU het bewustzijn voortdurend aangescherpt, zodat kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Onderdeel van het beleid zijn regelmatig terugkerende bewustwordingscampagnes voor medewerkers (o.a. operationele beheerders), studenten en derden. Verhoging van het beveiligingsbewustzijn is zowel een verantwoordelijkheid van de leidinggevenden, als de SO/PO en de ISM's; uiteindelijk is de CvB-voorzitter hiervoor verantwoordelijk. Dit alles laat onverlet dat elke beveiliging faalt als deze niet gedragen wordt door de medewerkers – elke OU medewerker is mede verantwoordelijk voor goede beveiliging. Dit is een cruciaal onderdeel van bewustwording en wordt randvoorwaardelijk ondersteund in het personeelsbeleid.

3.6 Overleg

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

Op **strategisch** niveau wordt richtinggevend gesproken over governance en compliance, alsmede over doelen, scope en ambitie op het gebied van informatiebeveiliging en privacy. Dit gebeurt in het UMT, geadviseerd door de SO/PO.

Op **tactisch** niveau wordt de strategie vertaald naar plannen, te hanteren normen, evaluatiemethoden, e.d. Deze plannen en instrumenten zijn sturend voor de uitvoering. Dit tactisch overleg wordt in het IT-Beraad gevoerd met advies van betrokken functionarissen zoals SO/PO, CERT-coördinator en proceseigenaren.

Op **operationeel** niveau worden de zaken besproken die het dagelijkse bedrijfsproces aangaan in de zin van uitvoering en implementatie.

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

4. Compliance

4.1 Wet- en regelgeving

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

Wet op het Hoger onderwijs en Wetenschappelijk onderzoek (WHW)
Aan de WHW ontleent de Open Universiteit zijn bestaan als rechtspersoon naar publiek recht. De WHW bevat de regels waaraan de OU moet voldoen. Op de WHW is het Uitvoeringsbesluit WHW gebaseerd waarin meer concrete bepalingen zijn opgenomen met betrekking tot studenten, personeel alsmede de berekening van de rijksbijdrage.

Wet Bescherming Persoonsgegevens (Wbp)
De OU heeft de wettelijke privacy vereisten met betrekking tot beveiliging ingebed in dit beleid. Handelen conform dit beleid leidt in beginsel tot voldoen aan de beveiligingsvereisten uit de wet.

Algemene Verordening Gegevensbescherming (AvG)[10]
De AvG is sinds 25 mei 2016 van kracht en moet op 25 mei 2018 volledig zijn geïmplementeerd door de OU. Op de laatst genoemde datum vervalt de Wet bescherming persoonsgegevens (WBP). De AvG is Europese regelgeving en geldt voor de gehele Europese Economische ruimte. Onder AvG wordt tevens begrepen de Uitvoeringswet Algemene verordening gegevensbescherming.

Daarnaast is er een Verordening met betrekking tot de eerbiediging van het privéleven en de bescherming van Persoonsgegevens in elektronische communicatie. Deze verordening die op 25 mei 2018 in werking treedt zal voorzien in de nadere omschrijving en aanvulling daarvan voor elektronische communicatiegegevens die als Persoonsgegevens worden aangemerkt.

Wet op de ondernemingsraden

Op grond van de Wet op de ondernemingsraden behoeft het College van bestuur instemming van de ondernemingsraad voor elk door hem voorgenomen besluit tot vaststelling, wijziging of intrekking van een regeling omtrent het verwerken van alsmede de bescherming van de persoonsgegevens van de in de onderneming werkzame personen.

Archiefwet
De OU houdt zich aan de wettelijke voorschriften ten aanzien van bewaartermijnen, zoals die in de Archiefwet zijn vastgelegd. In het Basis selectiedocument zijn de vernietigingstermijnen[11] van diverse typen informatie vastgelegd.

Auteurswet
De OU respecteert auteursrechten en handelt daarnaar.

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. Een onderdeel hiervan, de zogenaamde Cookiewet, is wél van toepassing op de websites van de OU.

Wet Computercriminaliteit
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 (WvS). De extra artikelen houden zich bezig met:

- Vernieling en onbruikbaar maken
- Aftappen van gegevens
- Denial of service, verstikkingsaanval
- Computervredebreuk
- Wat is computercriminaliteit

[10] In Engelstalige documenten wordt de AVG aangeduid als de General Data Protection Regulation (GDPR).
[11] De OU heeft (2017) een contract met het bedrijf AllBedigit dat ons adviseert m.b.t. die vernietigingstermijnen.

- Diensten afnemen zonder betalen
- Malware, kwaadaardige software

Aansluitvoorwaarden SURFfederatie / SURFnet
De OU heeft verschillende overeenkomsten met SURFnet die ons o.a.:
- verbieden om anonieme toegang tot internet te faciliteren
- verplichten om adequaat te reageren op klachten van SURFcert over misbruik van voorzieningen dat afkomstig is uit de OU,
- verplichten om met ons identity management systeem integere gegevens te leveren aan de SURFfederatie.

Als ultieme sanctie kan SURFnet de internetverbinding van de OU tijdelijk afsluiten.

Het naleven van dit informatiebeveiligings- en privacy beleid en het implementeren van basismaatregelen zorgen ervoor dat de OU een basisniveau van beveiliging heeft. Indien er aanvallen op de OU plaatsvinden die die beveiliging significant doorbreken en die vallen onder de Wet Computercriminaliteit, doet de OU in beginsel aangifte. De CERT-coördinator en SO/PO adviseren hierover aan de portefeuillehouder.

4.2 Afspraken in de cao

Cao Nederlandse Universiteiten (2 juli 2016 t/m 30 juni 2017)
De artikelen 1.16 Geheimhouding en 1.17 Aansprakelijkheid en schadeloosstelling zijn van belang voor het Informatiebeveiligings- en privacy beleid van de OU.

4.3 Vastgestelde beleidsdocumenten van de OU

Reglement bescherming persoonsgegevens Open Universiteit[12] (Jan Engels, 2016)
Vertaling van de Wet Bescherming Persoonsgegevens (Wbp) naar het privacy beleid van de Open Universiteit.

http://www.intranet.ou.nl/eCache/INT/30/232.html

Reglement computergebruik medewerkers Open Universiteit[13] (Peter Timmermans en Judith Niesters, 2015)
Reglement waardoor de OU regels wil stellen omtrent het gewenste gebruik van bedrijfsmiddelen. Het streven daarbij is een goede balans aan te brengen tussen enerzijds verantwoord en veilig gebruik van internet en ict-faciliteiten en anderzijds de privacy van de medewerker.

http://www.intranet.ou.nl/INTRANET/Docs/Organisatie/BU/PO/reglement_computergebruik.pdf

Reglement computergebruik studenten Open Universiteit[14] (Peter Timmermans en Judith Niesters, 2015)
Reglement waardoor de OU regels wil stellen omtrent het gewenste gebruik van bedrijfsmiddelen. Het streven daarbij is een goede balans aan te brengen tussen enerzijds verantwoord en veilig gebruik van internet en ict-faciliteiten en anderzijds de privacy van de medewerker.

Privacyverklaring Open Universiteit (Jan Engels, 2017)
Document waarin voor de medewerkers van de OU het gebruik van Persoonsgegevens, beveiliging, verstrekken van Persoonsgegevens aan derden, verzoek tot wijzigen van gegevens en de contactgegevens van de FG worden vermeld.

Beleid m.b.t. het verstrekken van persoonsgegevens aan OU medewerkers (Peter Timmermans en Jan Engels, 2017)
Het betreft het verstrekken van Persoonsgegevens in het kader van onderzoek, bedrijfsvoering en andere situaties.

Eigenaarschap van bedrijfsmiddelen (Peter Timmermans en Hilde Janssen, 2015)
Kaders voor eigenaarschap van informatiesystemen, informatie en infrastructuur.

Beleid aanschaf software of informatiediensten (Hilde Janssen en Peter Timmermans, 2017)

[12] Vastgesteld door het CvB.
[13] Vastgesteld door het CvB
[14] Vastgesteld door het CvB

Beleid oor de inkoop van software en het afsluiten van overeenkomsten voor het leveren van diensten op het gebied van informatieverwerking.

Aanpak van datalekken (Peter Timmermans, 2016)
Bestrijden van onrechtmatige verwerking van Persoonsgegevens die onder de verantwoordelijkheid van de OU vallen.

Disclaimer Open Universiteit (Jan Engels, 2017)
Aansprakelijkheid websites, e-mail nieuwsbrieven en overige uitingen die gecommuniceerd worden door de OU.

Classificatiekader Open Universiteit (Ludo Cuijpers, 2017)
Beschrijving BIV classificatie en benoemen beheersmaatregelen (controls)

Diverse documenten

- RFC-2350 voor CERT OU. Zie: www.ou.nl/Security
- Richtlijn authenticatie: Hoofdstuk 3.1 Soorten toegangscodes in het document Uitvoeringsregels informatiebeveiliging http://www.intranet.ou.nl/INTRANET/Docs/Ict/Informatiebeveiliging/Uitvoeringsregels%20informatiebeveiliging.pdf
- Operationeel model CERT OU
- Informatiebeveiligingsbaseline van de Open Universiteit.
- Calamiteitenplan (Concept) zie: R:\Afdelingen\GSO\AenB\FenI\ICT_voorzieningen\Systeembeheer\CalamiteitenPlan-haw-nieuwe opzet-V02.doc

5. Melding en afhandeling van incidenten

5.1 Datalekken

De OU heeft een procedure opgesteld voor de omgang met (vermoedens van) datalekken. In die procedure is beschreven dat datalekken moeten worden gemeld bij de Servicedesk van de OU. Deze procedure is vastgesteld door het CvB. De beschrijving van deze procedure vatt in twee delen uiteen. Het deel van de procedure dat van belang is voor alle medewerkers van de OU staat op Intranet in het ICT ABC onder de lemma's *Datalekken – Meldplicht* en *Meldplicht datalekken*. Onder beide lemma's is dezelfde informatie beschikbaar.

In het document *Aanpak datalek* is beschreven welke functies zijn betrokken bij de verdere afhandeling van het datalek en welke acties – afhankelijk van de specifieke omstandigheden van het datalek – daartoe noodzakelijk zouden kunnen zijn.

5.2 Andere informatiebeveiligingsincidenten (CERT)

5.2.1 Registratie informatiebeveiliging incidenten

Incidentbeheer en -registratie hebben betrekking op de wijze waarop geconstateerde dan wel vermoede inbreuken op de informatiebeveiliging en privacy door medewerkers, studenten en derden gemeld worden en de wijze waarop deze worden afgehandeld.

Het is van belang om te leren van incidenten. Incidentregistratie en periodieke rapportage over opgetreden incidenten horen thuis in een volwassen informatiebeveiligingsomgeving. De OU maakt daartoe gebruik van een CERT-meldpunt (e-mail aan cert@ou.nl) en heeft bekend gemaakt hoe dat is te benaderen. In de openbare meldingen en rapportages van CERT OU worden eventuele daders en slachtoffers van informatiebeveiligings- en privacy incidenten geanonimiseerd.

Elke medewerker en derde is zelf verantwoordelijk voor het signaleren en melden van incidenten en inbreuken op informatiebeveiliging en privacy. Incidenten en inbreuken worden direct gemeld aan het CERT-meldpunt.

De incidenten worden afgehandeld en worden in het relevante operationeel overleg besproken en – als bedrijfsproces, financiën of goede naam in gevaar zijn – ook op bestuurlijk niveau. Bij constatering van verontrustende trends kan hierop meteen worden ingespeeld, bijvoorbeeld door het nemen van extra maatregelen of een bewustwordingscampagne.

5.2.2 Doelen

Het doel van de CERT is instelling brede preventie en curatieve zorg voor informatiebeveiliging en privacy incidenten om zodoende informatiebeveiligings- en privacy incidenten te voorkomen en deze te bestrijd en als ze zich voordoen. Daarmee ondersteunt CERT OU de continuïteit van de OU en beschermt haar reputatie. CERT OU houdt zich ook bezig met beveiligings- en privacy incidenten buiten de OU als daar eigen medewerkers of studenten in enige rol bij betrokken zijn. In zulke gevallen wordt in principe gebruik gemaakt van de diensten van SURFcert, die wereldwijd in verbinding staat met andere CERT's.

De leden van het CERT zijn benoemd door het College van Bestuur en opereren in diens opdracht. Het CERT is gerechtigd het isoleren van computersystemen of netwerksegmenten te gelasten.

Het CERT heeft de volgende opdracht:

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

Het CERT van de OU behandelt meldingen vertrouwelijk en verstrekt alleen informatie over beveiliging en privacy incidenten als dat noodzakelijk en relevant is voor de oplossing van een incident.

De dienstverlening van het CERT van de OU is gedocumenteerd en door het College van Bestuur bekrachtigd.

CERT OU heeft een charter opgesteld waarin doelgroep, opdracht, bevoegdheden, escalaties, werkwijze (inclusief omgang met vertrouwelijkheid) en samenstelling zijn uitgewerkt.

Bijlage A. Rollen m.b.t. informatiebeveiliging en privacy

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

Rol	Beschrijving
Bestuur (CvB)	Is verantwoordelijk voor de informatiebeveiliging en privacy binnen de OU en stelt het beleid op het gebied van informatiebeveiliging en privacy vast.
Onderne-mingsraad (OR)	De OR heeft op grond van de WOR advies- en instemmingsrecht op verschillende dossiers. Bij het informatiebeveiliging en privacy beleid is van belang dat de OR op het gebied van de bescherming van persoonsgegevens op grond van art. 27 lid 1 sub k instemmingsrecht heeft ten aanzien van de bescherming van persoonsgegevens van de in de OU werkzame personen.
Business Continuity Manager (BCM)	Draagt zorg voor het definiëren, doen opzetten en controleren van processen die de continuïteit van de instelling(sprocessen) waarborgen. Deze functie is significant breder dan alleen IT beveiliging. Binnen de OU wordt deze rol vervuld door de Clustercoördinator Facilitaire en ict-voorzieningen.
CERT-coördinator	Wordt benoemd door de CvB-voorzitter op advies van de portefeuillehouder, de SO/PO en de Clustercoördinator Facilitaire en ict-voorzieningen. Hij is verantwoordelijk voor information security incident management binnen de instelling, en is in dat kader ook bevoegd het tijdelijk isoleren van computersystemen of netwerksegmenten te gelasten. De CERT-coördinator werkt voor het uitvoeren van deze taken samen met andere CERT-leden. Binnen de OU fungeert de Beleidsmedewerker ICT security als CERT-coördinator.
CERT OU	Het computer emergency response team van de OU, de brandweer van de informatiebeveiliging en privacy, die net als de “gewone” brandweer zowel preventief als curatief opereert.
Eigenaar	Degene die verantwoordelijk en bevoegd is en over het betreffende budget beschikt. Binnen de OU kunnen alleen decanen en directeuren eigenaar zijn. Zij kunnen dit eigenaarschap (sub-)mandateren aan medewerkers. In dit Informatiebeveiligings- en privacy beleid zijn vooral de eigenaren van de persoonsgegevens en van de bedrijfsprocessen van belang. **Persoonsgegevens** De decanen van de faculteiten zijn eigenaren van de persoonsgegevens van proefpersonen in wetenschappelijk onderzoek van de eigen faculteit. De decaan PenOW treedt hierbij op als aanspreekpunt/vertegenwoordiger van de decanen. De directeur GSO is eigenaar van alle andere Persoonsgegevens. **Bedrijfsprocessen** De eigenaar van een bedrijfsproces (proceseigenaar) is in principe eigenaar van de gegevens (m.u.v. persoonsgegevens) die in dat bedrijfsproces worden verwerkt en van de informatiesystemen waarmee dat gebeurt.
Functionaris gegevensbescherming (FG)	Houdt binnen de OU toezicht op de toepassing en naleving van de AvG. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de instelling. Het CvB heeft een van de Juridisch adviseurs benoemd in de rol van FG.
Informatiedomein vertegenwoordiger (IDV)	Een OU medewerker die als vertegenwoordiger van een informatiedomein (bedrijfsproces) optreedt in relevante gremia, zoals het IT-beraad.

Rol	Beschrijving
Informatie manager	Beleidsmedewerker die UMT en CvB adviseert over de informatiebehoeften van de organisatie en hoe aan die behoeften te voldoen. Toetst projectvoorstellen op de toepassing van het Informatiebeveiligings- en privacy beleid
Information Security Manager (ISM)	OU medewerkers die op tactisch (en operationeel) niveau opereren en daarmee de verbindende schakel vormen tussen het strategische niveau waarop de SO opereert en de dagelijkse inrichting en uitvoering van informatiebeveiliging en privacy in de bedrijfsfuncties. Binnen de OU wordt die rol ingevuld door de Informatiedomein vertegenwoordigers (IDV's).
Interne auditor	De interne auditor controleert jaarlijks het goed en betrouwbaar functioneren van de interne IT-organisatie. Dit omvat o.a.: de structuur en verantwoordelijkheden van die IT-organisatie, de hardware, de systeem software en -applicaties, het interne- en (indien aanwezig) externe netwerk, veiligheids- en calamiteiten systemen. De rol van interne IT-auditor wordt ingevuld door de interne auditor.
IT-beraad	Overlegorgaan waarin de IDV's van de verschillende informatiedomeinen zitting hebben alsmede de informatiemanager, de resource manager en een Enterprise Architect. Dit overlegorgaan initieert (project-)voorstellen vanuit een visie en meerjarenbeleid. De informatiemanager heeft binnen het IT-beraad de rol en positie om : a) de beleidskaders helder positioneren; b) vanuit die helderheid te zorgen dat het IT-beraad besluiten neemt binnen de beleidskaders.
Leidinggevende	Naleving van het informatiebeveiligingsbeleid is onderdeel van het integrale bedrijfsproces. Iedere leidinggevende heeft de taak om: – er voor te zorgen dat hun medewerkers c.q. studenten op de hoogte zijn van (de voor hen relevante aspecten van) het informatiebeveiligings- en privacy beleid; – toe te zien op de naleving van het informatiebeveiligings- en privacy beleid door medewerkers en studenten; – periodiek het onderwerp informatiebeveiligings- en privacy beleid onder de aandacht te brengen in werkoverleggen; – als aanspreekpunt beschikbaar te zijn voor alle personeel gerelateerde informatiebeveiligings- en privacy beleid zaken. De leidinggevende kan hierin ondersteund worden door de SO/PO.
Privacy Officer (PO)	Een rol op strategisch en tactisch niveau. De privacy officer heeft direct toegang tot de portefeuillehouder en is zelf geen lijnverantwoordelijke. adviseert de Verantwoordelijken voor de Persoonsgegevens m.b.t. de verwerking van deze Persoonsgegevens binnen de kaders van de AvG. De privacy officer ondersteunt de FG bij dienst taken maar heeft niet de bevoegdheden van de FG.
Security Officer (SO)	Een rol op strategisch en tactisch niveau. De security officer heeft direct toegang tot de portefeuillehouder en is zelf geen lijnverantwoordelijke. Hij adviseert – gevraagd en ongevraagd – de portefeuillehouder en andere Verantwoordelijken, waakt over informatiebeveiliging, stelt lastige vragen, ondersteunt audits en formuleert beleid en aanbevelingen. Deze rol is belegd bij de Beleidsmedewerker ICT security, binnen de afdeling Beleid en strategieontwikkeling bedrijfsvoering van de Bestuursdienst.
Verantwoordelijke	In de zin van de AvG is de Verantwoordelijke degene die het doel en de middelen van de verwerking van Persoonsgegevens bepaalt. Die verantwoordelijkheid kan alleen gedragen worden als de Verantwoordelijke ook de Eigenaar van die persoonsgegevens is. Andere bedrijfsprocessen en systemen kunnen Persoonsgegevens slechts raadplegen en verrijken met schriftelijke toestemming van de Verantwoordelijke en de FG.

Bijlage B. Bronnen

1. HORA: Toolbox Hoger Onderwijs Referentie Architectuur Zie: ttp://www.wikixl.nl/wiki/hora/index.php/Hoofd-pagina
2. ISO 27001 : NEN-ISO/IEC 27001:2013 nl Zie: http://www.nen.nl/NEN-Shop/Norm/NENISOIEC-270012013-nl.htm
3. ISO 27002 : NEN-ISO/IEC 27002:2013 nl Zie: http://www.nen.nl/NEN-Shop/Norm/NENISOIEC-270022013-nl.htm
4. Normenkader SURFaudit: http://www.surf.nl/diensten-en-producten/surfaudit/normenkader-surfaudit/index.html - volledige versie te verkrijgen via SURFibo lidmaatschap, zie http://www.surf.nl/over-surf/samenwerking/nationale-samenwerking/surfibo/index.html
5. RFC-2350. Zie: http://www.ietf.org/rfc/rfc2350.txt