Beleid voor naleving

Informatiebeveiliging

document	
identificatie	OU Beleid voor naleving
status	Definitief
auteur(s)	Martin Romijn - Chief Information Security Officer
eigenaar	Directeur ITF
opgeslagen	Teams-omgeving

accordering

acroniem	handtekening	datum
Cvb	Vastgesteld door het College van bestuur	26 september 2023

Open Universiteit
www.ou.nl

wijzigingshistorie				
versie	**auteur**	**datum**	**wijziging**	**review**
0.1.0	TT2	31-05-2022	Initiële versie TT2	
0.2.0	TT2	02-06-2022	Review MR1 en TT2	MR1
0.3.0	CKO	23-06-2022	Review door CKO	
0.4.0	HIL	23-06-2022	Review door HIL	
0.5.0	MR1	04-07-2022	Verwerken feedback en opmerkingen reviews CKO en HIL	
0.5.1	TT2	12-08-2022	Bijwerken structuur en opmaak	
0.6.0	JAE	19-09-2022	Review door JAE	
0.7.0	TT2	28-09-2022	Verwerken opmerkingen review JAE	MR1
0.7.1	MR1	05-06-2023	Verwijzing in paragraaf 6 vervangen door verwijzing naar intranet	
1.0	MR1	01-11-2023	Omgezet in definitieve versie en Pdf i.v.m. vaststelling door het College	

inhoudsopgave

1. Doel

Dit beleid heeft betrekking op het vastleggen van beleidsbepalingen omtrent de naleving van wettelijke en contractuele eisen op het gebied van informatiebeveiliging, met als doel data, informatie en informatiesystemen van de Open Universiteit (OU) op een adequate manier te beschermen.

2. Doelgroep

Dit beleid is bestemd voor iedereen – intern of extern – die te maken heeft met de bedrijfsprocessen van de OU.

3. Definities

Zie de begrippenlijst die in dezelfde map staat als dit document.

4. Beleidsbepalingen

De bepalingen in dit document zijn gebaseerd op:

1. Het document *Beleid verwerking persoonsgegevens en informatieveiligheid*, met daarin onder meer:
    a. Risico's die van toepassing zijn voor de OU
    b. Normen en toetsingskaders waaraan de OU moet voldoen
    c. Wet- en regelgeving waaraan de OU moet voldoen
2. Beslissingen door het College van bestuur

4.1 Identificeren van wettelijke en contractuele verplichtingen

De volgende bepalingen zijn van toepassing:

1. Er is een periodiek bijgewerkt overzicht van geldende wet- en regelgeving omtrent informatiebeveiliging waaraan de OU dient te voldoen.
2. Er is een periodiek bijgewerkt overzicht van geldende contractuele verplichtingen omtrent informatiebeveiliging waaraan de OU dient te voldoen.
3. Er vindt periodieke monitoring plaats voor het identificeren van (aanstaande) wijzigingen in toepasselijke wet- en regelgeving.
4. Er is een verantwoordelijke aangewezen voor het onderhouden van een actueel overzicht van geldende wet- en regelgeving en contractuele verplichtingen.

4.2 Beheren van licenties

De volgende bepalingen zijn van toepassing:

1. Er is een actueel overzicht van bedrijfsmiddelen waarvoor een licentie is vereist.
2. Er is een actueel overzicht van licenties inclusief:
    a. Naam en beschrijving van de licentie
    b. Status
    c. Activatiedatum
    d. Geldigheidsduur
    e. Verloopdatum
    f. Bewijs van aanschaf
    g. Indien actief: bedrijfsmiddelen gekoppeld aan de licentie
3. Er vindt periodiek controle plaats om vast te stellen dat gelicentieerde software en hardware in gebruik is met een geldige licentie.
4. Er is een verantwoordelijke aangewezen voor het licentiebeheer.

4.3 Onafhankelijke controle van informatiebeveiliging

De volgende bepalingen zijn van toepassing:

1. Er vindt periodieke controle plaats door een onafhankelijk aangesteld derdelijns specialist of auditor om de staat van de informatiebeveiliging van de OU en haar informatiesystemen vast te stellen.
2. Er vindt controle plaats door een onafhankelijk aangesteld specialist om de staat van de informatiebeveiliging van de OU en haar informatiesystemen vast te stellen na significante organisatorische of technische wijzigingen die mogelijk impact hebben op de status van informatiebeveiliging.
3. Na elke uitgevoerde controle volgt een rapport met constateringen en aanbevelingen.
4. Elke aanbeveling uit het rapport wordt door interne experts beoordeeld voor het vaststellen of deze wordt overgenomen door de OU.
5. Overgenomen aanbevelingen worden:
    a. Geregistreerd als actie
    b. Toegewezen aan een verantwoordelijke
    c. Voorzien van een risicoscore
    d. Voorzien van een deadline
6. Er is een verantwoordelijke aangewezen voor:
    a. Het aanstellen van een onafhankelijk specialist of auditor
    b. Het periodiek inplannen van een controle
    c. Het betrekken en inlichten van belanghebbenden

4.4 Technische validatie van kritieke informatiesystemen

De volgende bepalingen zijn van toepassing:

1. Er vindt periodieke technische validatie plaats van de aanwezigheid en effectiviteit van beveiligingsmaatregelen te toetsen voor kritieke informatiesystemen.
2. Na elke uitgevoerde validatie volgt een rapport met constateringen en aanbevelingen.
3. Elke aanbeveling uit het rapport wordt door interne experts beoordeeld teneinde vast te stellen of deze wordt overgenomen door de OU.
4. Overgenomen aanbevelingen worden:
    a. Geregistreerd als actie
    b. Toegewezen aan een verantwoordelijke
    c. Voorzien van een risicoscore
    d. Voorzien van een deadline
5. Er is een verantwoordelijke aangewezen voor:
    a. Het eventueel inschakelen van een extern specialist
    b. Het periodiek inplannen van een technische validatie
    c. Het betrekken en inlichten van belanghebbenden

4.5 Beschermen van persoonsgegevens en privacy

De volgende bepalingen zijn van toepassing:

1. Er is een actueel verwerkingsregister dat:
    a. Informatie bevat over de persoonsgegevens die de OU verwerkt
    b. Informatie bevat over de verwerkingsactiviteiten van de OU
    c. Voldoet aan de eisen voor een verwerkingsregister zoals vastgesteld in de Algemene verordening gegevensbescherming (AVG)
2. Er is een actueel overzicht met afgesloten verwerkersovereenkomsten waarbij:
    a. De OU optreedt als verwerkingsverantwoordelijke
    b. De OU optreedt als (sub)verwerker
3. Er vindt periodieke validatie plaats om vast te stellen in hoeverre wordt voldaan aan wet- en regelgeving omtrent bescherming van persoonsgegevens.

5. Context

Dit beleid is gerelateerd aan meerdere documenten. Bijbehorende standaarden en procedures zijn momenteel in ontwikkeling. Vastgestelde standaarden komen beschikbaar op dezelfde locatie als dit beleidsdocument. Vastgestelde procedures komen beschikbaar op de interne omgeving van de verantwoordelijke afdeling.

6. Naleving

Wanneer dit beleid wordt geschonden kunnen disciplinaire maatregelen van toepassing zijn zoals nader beschreven in het op intranet aanwezige vigerende document Huisregels werknemers Open Universiteit. Dit is niet van toepassing wanneer er sprake is van een formeel vastgelegde uitzondering.

7. Uitzonderingen

Een uitzondering is een bekende en geaccepteerde situatie waarin dit beleid niet van toepassing is. We onderscheiden twee soorten uitzonderingen:

1. Structurele uitzonderingen zijn vastgelegd in de lijst van uitzonderingen in Bijlage 1.
2. Incidentele uitzonderingen moeten expliciet worden goedgekeurd en zijn enkel geldig voor een vooraf vastgelegde gebeurtenis of periode.

Een verzoek om uitzondering moet vooraf worden ingediend bij de ICT Servicedesk. Hierbij wordt gekeken naar de reikwijdte, rechtvaardiging en mogelijke risico’s die de uitzondering met zich meebrengt. Het Hoofd Operations en de Chief Information Security Officer beoordelen het verzoek en kunnen hierbij eventueel interne of externe experts om advies vragen. Een goedgekeurd verzoek wordt vastgelegd met bijbehorende motivatie in Bijlage 1. Aanvullende maatregelen kunnen nodig zijn om risico’s te beperken.

8. Wijzigingen

Het College van bestuur stelt, met instemming van de medezeggenschap, vast dat elke formeel goedgekeurde versie van dit beleid van kracht is. Het beleid wordt minimaal 1x per 3 jaar geëvalueerd en zo nodig bijgesteld, of eerder als dit nodig is vanwege belangrijke interne of externe ontwikkelingen op het gebied van informatiebeveiliging. Het formele goedkeuringsproces heeft geen betrekking op wijzigingen in Bijlage 1.

Bijlage 1: Structurele uitzonderingen op dit beleid