Beleid voor veilig personeel

Informatiebeveiliging

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

accordering

acroniem	**handtekening**	**datum**
JNI		6 -12 – 2022
HIL		
OSP		
Cvb	Vastgesteld door het College van bestuur na positief advies van de medezeggenschap.	26 september 2023

Open Universiteit
www.ou.nl

wijzigingshistorie				
versie	**auteur**	**datum**	**wijziging**	**review**
0.1.0	TT2	07-06-2022	Initiële versie TT2	
0.2.0	MR1	09-06-2022	Review door MR1 en TT2	
0.3.0	HIL	29-06-2022	Review door HIL	
0.4.0	CKO	04-07-2022	Review door CKO	
0.5.0	MR1	04-07-2022	Verwerken feedback en opmerkingen reviews HIL en CKO	TT2
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	Review door JNI en OSP	
0.8.0	MR1	06-12-2022	Verwerken opmerkingen review JNI en OSP	MR1
0.9.0	MR1	08-12-2022	Verwerken finale feedback JNI	OSP
0.9.1	MR1	05-06-2023	Verwijzing in paragraaf 6 vervangen door verwijzing naar intranet	
0.9.2	MR1	03-10-2023	Paragraaf 4.2.1 woord “nieuwe” medewerkers verwijderd op basis van advies daarover van de studentenraad.	JAE
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 risicobehandeling en veiligheid van personeel voor, tijdens en na dienstverband, 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.

Voor de betekenis van gebruikte termen wordt primair gebruik gemaakt van de definities uit het Cybersecurity woordenboek 2021. Daar waar de termen niet in het woordenboek voorkomen, wordt maximaal aangesloten bij de terminologie zoals deze door ITIL wordt gebruikt.

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 Aanvang van dienstverband

De volgende bepalingen zijn van toepassing:

1. Bij alle kandidaten voor een dienstverband wordt voorafgaand aan indiensttreding door of in opdracht van de leidinggevende een screening uitgevoerd die past bij de te ontvangen bevoegdheden en verantwoordelijkheden van de functie.
2. Nieuw personeel accepteert voorafgaand aan de start van werkzaamheden een geheimhoudingsclausule die:
    a. Het personeelslid verplicht om verantwoord om te gaan met vertrouwelijke informatie
    b. Maatregelen beschrijft bij schending van geheimhouding
    c. Vastlegt hoelang geheimhouding na beëindiging van dienstverband van kracht blijft

    De geheimhoudingsbepaling maakt deel uit van de vigerende CAO die op alle medewerkers van toepassing is.
3. Nieuwe medewerkers ontvangen bij indiensttreding informatie over informatiebeveiliging.

4.2 Tijdens dienstverband

De volgende bepalingen zijn van toepassing:

1. Er is een omgeving ingericht voor medewerkers voor verstrekken van informatie over informatiebeveiliging.
2. Er is een verantwoordelijke aangewezen voor het toewijzen van medewerkers aan de omgeving.
3. Er is een verantwoordelijke aangewezen voor het periodiek herzien en bijwerken van de inhoud op de omgeving.
4. Er is een klokkenluidersregeling die iedereen in staat stelt om anoniem en veilig situaties, problemen of misstanden ten aanzien van informatiebeveiliging te melden.
5. Elke medewerker wordt toegewezen aan trainingen en oefeningen om het bewustzijn ten aanzien van informatiebeveiliging te vergroten op basis van functie, capaciteiten en verantwoordelijkheden.

6. Elke medewerker die is toegewezen aan trainingen en oefeningen om het bewustzijn ten aanzien van informatiebeveiliging te vergroten, is verplicht deel te nemen aan deze activiteiten en deze succesvol af te ronden binnen de daarvoor vastgestelde termijn.
7. Er zijn voldoende financiële middelen beschikbaar voor het kunnen volgen van trainingen en opleidingen ten aanzien van informatiebeveiliging.
8. Er zijn disciplinaire maatregelen en sancties opgesteld voor het overtreden van verplichtingen of verboden ten aanzien van informatiebeveiliging.

4.3 Beëindiging van dienstverband

De volgende bepalingen zijn van toepassing:

1. Voorafgaand aan beëindiging van het dienstverband:
    a. Verwijdert de betreffende medewerker persoonlijke informatie, inclusief privé e-mail, van informatiedragers van de OU. De OU faciliteert daar niet bij
    b. Zorgt de betreffende medewerker ervoor dat alle zakelijke informatie correct intern is overgedragen en opgeslagen om verlies van informatie te voorkomen
    c. Controleert de leidinggevende van de medewerker of informatie correct intern is overgedragen en opgeslagen om verlies van informatie te voorkomen
    d. Het account, inclusief alle daaraan gekoppelde informatie, vervalt na de uitdiensttreding.
2. Er wordt opgetreden tegen overtredingen van verantwoordelijkheden en contractuele verplichtingen met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband, zoals geheimhouding na uitdiensttreding.

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