Beleid voor leveranciersbeheer

Informatiebeveiliging

document	
identificatie	OU Beleid voor leveranciersbeheer v1.0.docx
status	Definitief
auteur(s)	Martin Romijn - Chief Information Security Officer
eigenaar	Directeur ITF
opgeslagen	Teams-omgeving (intern)

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	04-05-2022	Initiële versie	TT2, EGW
0.2.0	TT2	04-05-2022	Bespreking MR1 en TT2	
0.5.1	MR1	19-05-2022	Tekst in de OU template voor beleidsdocumenten gezet	CKO, HIL
0.6.0	MR1	09-06-2022	Verwerken opmerkingen en wijzigingen na review CKO en HIL	
0.7.1	TT2	12-08-2022	Bijgewerkte structuur en opmaak	
0.8.0	JAE	19-09-2022	Review door JAE	
0.9.0	TT2	28-09-2022	Verwerken opmerkingen review JAE	MR1
0.9.1	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 afspraken met externe leveranciers omtrent het implementeren van informatiebeveiligingsmaatregelen en het controleren op de naleving hiervan, 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 Overzicht van leveranciers

De volgende bepalingen zijn van toepassing:

1. Er is een actueel overzicht van alle leveranciers met toegang tot informatie waarvoor de OU verantwoordelijk is, inclusief:
    a. Categorieën verwerkte informatie
    b. Informatiesystemen waar de leverancier toegang tot heeft
    c. Overeenkomsten en contracten
    d. Omschrijving van geleverde diensten en/of producten
    e. Status van leverancier:
        i. Potentieel, levert momenteel geen diensten en/of producten maar gaat dit mogelijk doen
        ii. Huidig, levert momenteel diensten en/of producten
        iii. Voormalig, heeft eerder diensten en/of producten geleverd
    f. Contactgegevens
    g. Contactpersoon vanuit OU
    h. Afspraken omtrent informatiebeveiligingsmaatregelen
2. Er is een verantwoordelijke aangewezen binnen de OU voor het onderhouden van dit overzicht van leveranciers.
3. Er vindt periodieke controle plaats om te verifiëren dat dit overzicht van leveranciers actueel en compleet is.

4.2 Doorlichting van potentiële leveranciers

De volgende bepalingen zijn van toepassing:

1. Elke potentiële leverancier is onderdeel van een doorlichtingsproces.

2. Er is een verantwoordelijke aangewezen binnen de OU voor het doorlichtingsproces.
3. Het doorlichtingsproces bestaat uit het vaststellen van:
    a. Contactgegevens
    b. Reputatie en bedrijfsgeschiedenis
    c. Financiële stabiliteit
    d. Te leveren diensten en/of producten
    e. Categorieën van te verwerken of benodigde informatie
    f. Het risicoprofiel
    g. Aanwezigheid van externe certificeringen omtrent informatiebeveiliging
    h. Afspraken omtrent informatiebeveiligingsmaatregelen
4. Er zijn risicoprofielen voor leveranciers vooraf gedefinieerd op het gebied van informatiebeveiliging, op basis van:
    a. Categorieën verwerkte informatie
    b. Benodigde toegang tot informatiesystemen
    c. Risico's met betrekking tot:
        i. Beschikbaarheid van informatie
        ii. Integriteit van informatie
        iii. Vertrouwelijkheid van informatie
5. Elke leverancier valt onder één risicoprofiel.
6. Per risicoprofiel zijn minimaal vereiste maatregelen vastgesteld die:
    a. Ondubbelzinnig zijn
    b. Toetsbaar zijn
    c. Betrekking hebben op informatiebeveiliging
7. Elke leverancier implementeert maatregelen passend bij het risicoprofiel dat van toepassing is.
8. Elke leverancier implementeert maatregelen volgens een algemeen erkende norm voor informatiebeveiliging, zoals ISO 27001, Baseline Informatiebeveiliging Overheid of ISAE 3400/3402, en kan dit aantonen middels:
    a. Een bewijs van accreditatie, certificaat of verklaring van een onafhankelijke auditor; of
    b. Het naar waarheid invullen van een beoordelingsformulier en het op verzoek kunnen aanleveren van bijbehorende bewijsstukken
9. De CISO en Privacy Officer beoordelen elk ingevuld beoordelingsformulier als:
    a. Aanvullende informatie nodig, een herbeoordeling volgt
    b. Afgekeurd, de leverancier voldoet niet aan de gestelde eisen
    c. Goedgekeurd, de leverancier voldoet aan de gestelde eisen
10. Elke leverancier moet het doorlichtingsproces succesvol afronden voor het mogen leveren van diensten en/of producten.
11. Elke leverancier voldoet aan wettelijke eisen omtrent het beveiligen van informatie.
12. Elke leverancier ondertekent een:
    a. Geheimhoudingsverklaring
    b. Overeenkomst waarin wordt vastgelegd welke diensten en/of producten worden geleverd en tegen welke voorwaarden
    c. Verwerkersovereenkomst indien persoonsgegevens worden verwerkt en de leverancier kan worden aangemerkt als verwerker volgens de Algemene Verordening Gegevensbescherming (AVG).

4.3 Onboarden van leveranciers

De volgende bepalingen zijn van toepassing:

1. Onboarding van een leverancier vindt enkel plaats na het succesvol afronden van het doorlichtingsproces.
2. Het principe van minste privileges wordt toegepast: de leverancier ontvangt enkel toegang tot informatie en informatiesystemen die absoluut noodzakelijk zijn voor het kunnen leveren van de diensten en/of producten.
3. Per leverancier wordt bijgehouden tot welke informatie en informatiesystemen deze toegang heeft.

4. In informatiesystemen worden accounts en gebruikers van leveranciers expliciet aangemerkt als extern.

Monitoren van bestaande leveranciers

De volgende bepalingen zijn van toepassing:

1. Per risicoprofiel is een evaluatiecyclus vastgesteld.
2. Per evaluatiecyclus wordt opnieuw vastgesteld of:
    a. De omschrijving van geleverde diensten en/of producten nog van toepassing is
    b. Het toegewezen risicoprofiel nog van toepassing is
    c. De leverancier nog steeds voldoet aan de vastgestelde maatregelen
    d. Er zich wijzigingen hebben voorgedaan bij de leverancier met mogelijk invloed op informatiebeveiliging
3. Elke leverancier zal OU proactief informeren indien er sprake is van een mogelijke invloed op informatiebeveiliging als gevolg van:
    a. Een wijziging in de geleverde diensten en/of producten; of
    b. Een wijziging in de organisatiestructuur van de leverancier; of
    c. Het niet langer aanbieden of ondersteunen van de geleverde diensten en/of producten
    d. Het kwijtraken of niet langer kunnen behouden van het bewijs van accreditatie, certificaat of verklaring van een onafhankelijke auditor
4. Elke leverancier zal OU informeren indien er sprake is van een vermoedelijk of daadwerkelijk datalek.
5. Er vindt periodieke controle plaats om te verifiëren dat toegang tot informatie en informatiesystemen niet wordt misbruikt.

4.4 Offboarden van leveranciers

De volgende bepalingen zijn van toepassing:

1. Het offboarden van een leverancier vindt plaats zodra de leverancier:
    a. Stopt met het leveren van diensten en/of producten; of
    b. Niet langer voldoet aan de gestelde beveiligingsmaatregelen en hier geen verbeteringsplan voor kan aantonen
    c. Wordt afgekeurd door de directeur ITF of het College van Bestuur
2. Bij offboarden van een leverancier dient:
    a. Toegang tot informatie en informatiesystemen volledig te worden ingetrokken
    b. De leverancier de eerder verwerkte en/of ontvangen informatie te vernietigen
3. Er vindt controle plaats om te verifiëren dat:
    a. Toegang tot informatie en informatiesystemen volledig is ingetrokken
    b. De leverancier de eerder verwerkte en/of ontvangen informatie heeft vernietigd

5. Context

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.

6. Naleving

Wanneer dit beleid wordt geschonden kunnen disciplinaire maatregelen van toepassing zijn zoals nader beschreven in het op intranet aanwezige document *Huisregels werknemers Open Universiteit U2020/5500 JNI (versie 8 oktober 2020)*. 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