# Beleid voor informatiebeveiliging in bedrijfscontinuïteitsbeheer

Informatiebeveiliging

Aanbevolen om dit op te nemen als onderdeel van het overkoepelende beleid voor bedrijfscontinuïteit

| document | |
|---|---|
| **identificatie** | OU Beleid voor informatiebeveiliging in bedrijfscontinuïteitsbeheer |
| **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 | 01-07-2022 | Initiële versie T. Timmermans (ON2IT) | |
| 0.2.0 | MR1 | 11-07-2022 | Review door MR1 en TT2 | TT2 |
| 0.3.0 | CKO | 08-08-2022 | Review door CKO | |
| 0.3.1 | TT2 | 12-08-2022 | Bijwerken structuur en opmaak | |
| 0.4.0 | MR1 | 14-09-2022 | Verwerken feedback en suggesties review HIL | TT2 |
| 0.5.0 | JAE | 19-09-2022 | Review door JAE | |
| 0.6.0 | TT2 | 28-09-2022 | Verwerken opmerkingen review JAE | MR1 |
| 0.6.1 | 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 ..... 3
2. Doelgroep ..... 3
3. Definities ..... 3
4. Beleidsbepalingen ..... 3
  4.1 Continuïteit van informatiebeveiliging ..... 3
  4.2 Testen van bedrijfscontinuïteit ..... 3
5. Context ..... 3
6. Naleving ..... 4
7. Uitzonderingen ..... 4
8. Wijzigingen ..... 4
Bijlage 1: Structurele uitzonderingen op dit beleid ..... 5

# 1. Doel

Dit beleid heeft betrekking op het vastleggen van beleidsbepalingen omtrent de informatiebeveiligingsaspecten in bedrijfscontinuïteitsbeheer, 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 Continuïteit van informatiebeveiliging

De volgende bepalingen zijn van toepassing:

1. Er is een bedrijfscontinuïteitsplan (BCP) dat tot stand komt door uitvoering van een expliciete risicoafweging om zo bedrijfskritische processen en bedrijfsmiddelen te identificeren.
2. In het bedrijfscontinuïteitsplan (BCP) is de continuïteit van informatiebeveiliging tijdens incident- en crisissituaties opgenomen, bestaande uit:
    a. Beschikbaarheid van informatie
    b. Integriteit van informatie
    c. Vertrouwelijkheid van informatie

## 4.2 Testen van bedrijfscontinuïteit

De volgende bepalingen zijn van toepassing:

1. Het bedrijfscontinuïteitsplan wordt periodiek getest op geldigheid en bruikbaarheid door middel van een bedrijfscontinuïteitsoefening.
2. Na elke bedrijfscontinuïteitsoefening vindt een evaluatie plaats om de continuïteit van informatiebeveiliging te verifiëren en beoordelen.
3. Geconstateerde verbeteringen worden binnen een vooraf vastgestelde periode doorgevoerd.

# 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