# Beleid voor beveiliging bedrijfsvoering

Informatiebeveiliging

| document | |
|---|---|
| **identificatie** | OU Beleid voor beveiliging bedrijfsvoering |
| **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** | **au-teur** | **datum** | **wijziging** | **review** |
| 0.1.0 | TT2 | 24-06-2022 | Initiële versie T. Timmermans (ON2IT) | |
| 0.2.0 | MR1 | 04-07-2022 | Review door MR1 | TT2 |
| 0.3.0 | CKO | 12-07-2022 | Review door CKO | |
| 0.3.1 | TT2 | 01-09-2022 | Bijwerken structuur en opmaak | |
| 0.4.0 | MR1 | 14-09-2022 | Verwerken feedback en suggesties review HIL | TT2 |
| 0.4.1 | 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 beveiligingmaatregelen in operationele bedrijfsvoering, 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 Operationele procedures

De volgende bepalingen zijn van toepassing:

1. Er zijn operationele procedures omtrent informatiebeveiliging aanwezig die:
    a. Gedocumenteerd zijn als werkinstructies
    b. Periodiek herzien en indien nodig bijgewerkt worden
    c. Beschikbaar zijn voor personeel waarvoor dit relevant is

## 4.2 Wijzigingsbeheer en capaciteitsbeheer

De volgende bepalingen zijn van toepassing:

1. Veranderingen die van invloed zijn op de informatiebeveiliging dienen te worden beheerst. Dit omvat veranderingen in:
    a. Bedrijfsprocessen
    b. Fysieke ruimten waar informatie wordt opgeslagen of verwerkt
    c. Informatiesystemen
2. Er is een procedure voor wijzigingenbeheer waarin wordt beschreven:
    a. Registratie van wijzigingen
    b. Risicoafweging van mogelijke gevolgen van wijzigingen
    c. Goedkeuringsproces voor wijzigingen
3. Om prestaties van systemen te waarborgen zijn:
    a. Capaciteitseisen van systemen vastgesteld
    b. Voldoende middelen beschikbaar om te voldoen aan de gestelde capaciteitseisen

## 4.3 Malware

De volgende bepalingen zijn van toepassing:

1. Er wordt periodiek een risico-inventarisatie gedaan omtrent de dreiging en manifestatie van malware.
2. Er zijn preventieve, detecterende en reactieve maatregelen genomen voor het beschermen van informatie en informatiesystemen tegen malware.
3. Voor preventie van malware worden onder andere de volgende maatregelen genomen:
    a. Het downloaden en openen van bepaalde typen bestanden, waarvan bekend is dat deze mogelijk malware bevatten of verspreiden, wordt standaard technisch beperkt of geblokkeerd.
    b. Er worden trainingen aangeboden aan personeel over bewustwording van risico's over surfgedrag, het openen van onbekende links of bestanden en de aanwezigheid van kwetsbaarheden in software.
    c. Beveiligingsupdates worden geïnstalleerd of afgedwongen
4. Voor detectie van malware (preventief) wordt gebruik gemaakt van anti-malwaresoftware welke:
    a. Actief is op door de OU beheerde bedrijfsmiddelen
    b. Het bedrijfsmiddel scant op de aanwezigheid van verdachte bestanden of processen
    c. Verdachte bestanden in quarantaine kan plaatsen
    d. Verdachte processen kan blokkeren
    e. Regelmatig wordt voorzien van updates
    f. Niet kan worden gedeactiveerd door een eindgebruiker
    g. Meldingen van verdachte activiteiten of evenementen verstuurt richting een SOC voor analyse
5. Voor herstel van malware (reactief) is specialistische kennis beschikbaar voor het:
    a. Identificeren van de bron van malware
    b. Beperken van de impact van malware
    c. Beperken van de verspreiding van malware
    d. Uitroeien van de aanwezigheid van malware
    e. Identificeren van leerlessen en verbeteringen ter voorkoming van eenzelfde situatie

## 4.4 Back-ups

De volgende bepalingen zijn van toepassing:

1. Er zijn verschillende back-upniveaus vastgesteld voor informatiesystemen op basis van risico's omtrent:
    a. Het verlies van informatie (beschikbaarheid)
    b. Het niet toegang hebben tot informatie (beschikbaarheid)
    c. Het ongeautoriseerd aanbrengen van wijzigingen in informatie (integriteit)
    d. Het ongeautoriseerd inzien van informatie (vertrouwelijkheid)
2. Elk back-upniveau beschrijft:
    a. De frequentie waarop een nieuwe back-up wordt gemaakt
    b. De locatie waar de back-up wordt opgeslagen
    c. Het retentieschema voor back-ups
3. Back-ups worden opgeslagen op een andere locatie dan die van het informatiesysteem waar de back-up van wordt gemaakt.
4. Er vindt periodiek validatie plaats of back-ups correct en volledig zijn uitgevoerd.

## 4.5 Logging van activiteiten en gebeurtenissen

De volgende bepalingen zijn van toepassing:

1. Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, worden:
    a. Gegenereerd
    b. Bewaard
    c. Regelmatig beoordeeld
2. Logfaciliteiten en informatie in logbestanden worden beschermd tegen vervalsing, ongeautoriseerde toegang of verwijdering.

## 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