Beleid voor fysieke beveiliging

Informatiebeveiliging

document	
identificatie	OU Beleid voor fysieke beveiliging
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	19-05-2022	Initiële versie TT2	
0.2.0	TT2	19-05-2022	In de OU template voor beleidsdocumenten gezet	MR1
0.3.0	HIL	09-06-2022	Review HIL	
0.4.0	CKO	09-06-2022	Review CKO	
0.5.0	MR1	09-06-2022	Verwerken opmerkingen review HIL en CKO	TT2
0.5.1	TT2	12-08-2022	Bijwerken structuur en opmaak	
0.6.0	JAE	19-09-2022	Review 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 vaststellen van bepalingen omtrent de beveiliging van fysieke ruimtes, 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 fysieke ruimtes

De volgende bepalingen zijn van toepassing:

1. Er is een actueel overzicht van alle fysieke ruimtes die in beheer zijn van of in gebruik zijn door de OU, inclusief:
    a. Geografische locatie
    b. Omschrijving van het gebruik van de ruimte
    c. Categorieën gebruikers of bezoekers
    d. Status van locatie
        i. Vrij toegankelijk voor elke bezoeker
        ii. Beperkt toegankelijk voor een selectie van (groepen) bezoekers
    e. Contactpersoon of beheerder vanuit OU
2. Er is een verantwoordelijke aangewezen binnen OU voor het onderhouden van bovenstaand overzicht van fysieke ruimtes.
3. Er vindt periodieke controle plaats om te verifiëren dat het overzicht van fysieke ruimtes actueel en compleet is.

4.2 Toegang tot fysieke ruimtes

De volgende bepalingen zijn van toepassing:

1. Voor vrij toegankelijke fysieke ruimte gelden geen restricties of expliciete authenticatie van individuen.
2. Voor elke beperkt toegankelijke fysieke ruimte geldt dat:
    a. Er is vastgesteld dat enkel bepaalde (groepen) individuen toegang hebben
    b. Voorafgaand aan het betreden van de ruimte wordt rechtmatige toegang van het individu gecontroleerd door:
        i. Handmatige authenticatie door middel van een bewaker of receptionist; of

        ii. Automatische authenticatie door middel van een kaart, druppel, wachtwoord, toegangscode of biometrie
    c. Toegang wordt geregistreerd in logs die worden bewaard volgens een vooraf bepaalde retentieperiode
    d. Er zijn adequate fysieke en digitale beveiligingsmaatregelen genomen om ongeoorloofde toegang tot de ruimte tegen te gaan.
3. Er wordt periodiek gecontroleerd of de genomen beveiligingsmaatregelen en authenticatiemechanismen actief en effectief zijn.

4.3 Bezoekers van beperkt toegankelijke fysieke ruimtes

De volgende bepalingen zijn van toepassing:

1. Elke bezoeker wordt vooraf aan het bezoek:
    a. Geregistreerd als bezoeker voor een gespecificeerde periode
    b. Geïdentificeerd door middel van een geldig identiteitsbewijs
2. Elke bezoeker heeft een:
    a. Legitiem belang voor toegang tot de fysieke ruimte
    b. Gastheer of gastvrouw vanuit de OU welke verantwoordelijk is voor de acties en gedragingen van de bezoeker tijdens het verblijf
    c. Gastheer of gastvrouw vanuit de OU welke de bezoeker continu begeleidt tijdens het bezoek
3. Er wordt periodiek gecontroleerd of bezoekers voldoen aan bovenstaande eisen.

4.4 Maatregelen voor beschermen van informatie in fysieke ruimtes

De volgende bepalingen zijn van toepassing:

1. Bij het wegvallen van de primaire stroomtoevoer voor kritieke informatiesystemen is:
    a. Noodstroom beschikbaar als kortetermijnoplossing voor het kunnen blijven voorzien in ononderbroken stroomtoevoer en wordt periodiek onderhouden en getest
    b. Een secundaire stroomtoevoer is beschikbaar als lange termijn oplossing voor het kunnen blijven voorzien in ononderbroken stroomtoevoer en wordt periodiek onderhouden en getest
2. Apparatuur en bekabeling voor netwerkverbinding van en naar informatiesystemen is beschermd tegen schade, verstoring en vernietiging en wordt periodiek onderhouden en getest.
3. Brandblussers, gasblusinstallatie, sprinklerinstallaties, brandslangen, brandpreventiesystemen en branddetectieapparatuur zijn ononderbroken operationeel en worden periodiek onderhouden en getest.
4. Temperatuur- en vochtigheidsregulatiesystemen zijn ononderbroken operationeel en worden periodiek onderhouden en getest.

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