Beleid voor beheer van bedrijfsmiddelen

Informatiebeveiliging

document	
identificatie	OU Beleid voor beheer van bedrijfsmiddelen
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	13-04-2022	Initiële versie TT2	
0.2.0	MR1	19-04-2022	Bespreking MR1 en TT2	
0.3.0	HIL	02-05-2022	Review door HIL	
0.3.1	MR1	19-05-2022	Tekst in de OU template voor beleidsdocumenten gezet	CKO, HIL
0.4.0	CKO	02-06-2022	Review door CKO	
0.5.0	MR1	02-06-2022	Verwerken opmerkingen en suggesties HIL en CKO	TT2
0.7.1	TT2	12-08-2022	Bijwerken structuur en opmaak	
0.8.0	JAE	19-09-2022	Review door JAE	
0.9.0	TT2	28-09-2022	Verwerken opmerkingen door 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 omtrent het implementeren van informatiebeveiligingsmaatregelen voor bedrijfsmiddelen 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 bedrijfsmiddelen

De volgende bepalingen zijn van toepassing:

1. Er is een actueel overzicht van alle bedrijfsmiddelen die:
    a. Dienen als drager voor informatie waarvoor de OU verantwoordelijk is
    b. Toegang hebben tot informatie waarvoor de OU verantwoordelijk is
    c. Toegang hebben tot informatiesystemen
2. Van elk bedrijfsmiddel is vastgelegd:
    a. Verantwoordelijk eigenaar (natuurlijk persoon)
    b. Operationele gebruiker(s)
    c. Vastgesteld BIV-classificatieniveau
    d. Gegevensverantwoordelijke(n) vanuit OU
    e. Leverancier(s)
    f. Omschrijving van bedrijfsmiddel
    g. Status van bedrijfsmiddel
    h. Actieve informatiebeveiligingsmaatregelen
3. Er is een verantwoordelijke aangewezen binnen de OU voor het onderhouden van dit overzicht van bedrijfsmiddelen.
4. Er vindt periodieke controle plaats om te verifiëren dat dit overzicht van bedrijfsmiddelen actueel en compleet is.

4.2 Beveiligen van bedrijfsmiddelen

De volgende bepalingen zijn van toepassing:

1. Er zijn categorieën voor bedrijfsmiddelen gedefinieerd op het gebied van informatiebeveiliging, op basis van:
    a. Categorieën verwerkte informatie

   b. Benodigde toegang tot andere informatiesystemen
   c. Risico's met betrekking tot:
      i. Beschikbaarheid van informatie
      ii. Integriteit van informatie
      iii. Vertrouwelijkheid van informatie
2. Per categorie zijn minimaal vereiste maatregelen vastgesteld die:
   a. Ondubbelzinnig zijn
   b. Toetsbaar zijn
   c. Betrekking hebben op informatiebeveiliging
3. Bedrijfsmiddelen in de hoogste categorie worden gezien als 'kritieke' bedrijfsmiddelen.
4. Elk bedrijfsmiddel valt onder minimaal één categorie.
5. Elk bedrijfsmiddel implementeert informatiebeveiligingsmaatregelen in lijn met de categorie die van toepassing is.
6. De vereiste informatiebeveiligingsmaatregelen worden meegenomen als criteria in het selectieproces voor aanschaf van nieuwe bedrijfsmiddelen.
7. Elke bedrijfsmiddel moet worden getoetst op correcte en volledige implementatie van informatiebeveiligingsmaatregelen voorafgaand aan ingebruikname.
8. Er vindt periodieke controle plaats om te verifiëren dat de informatiebeveiligingsmaatregelen actief zijn en naar behoren functioneren.

4.3 Ingebruikname van bedrijfsmiddelen

De volgende bepalingen zijn van toepassing:

1. Ingebruikname van een bedrijfsmiddel vindt enkel plaats nadat:
   a. Er is vastgesteld welke informatie verwerkt wordt
   b. Er is vastgesteld dat wordt voldaan aan de gestelde informatiebeveiligingsmaatregelen
   c. De vereiste licenties zijn aangeschaft en geldig zijn
2. Het principe van minste privileges wordt toegepast: toegang tot bedrijfsmiddelen wordt enkel verschaft aan diegenen die noodzakelijk toegang nodig hebben tot het bedrijfsmiddel voor het kunnen uitoefenen van taken en het leveren van diensten en/of producten.
3. Een bedrijfsmiddel met toegang tot niet-publieke informatie of informatiesystemen heeft de status 'actief'.
4. Voor elk actief bedrijfsmiddel is vastgelegd:
   a. Wanneer deze in gebruik is genomen
   b. Voor welke periode deze in gebruik is
5. Elke gebruiker van een bedrijfsmiddel gaat akkoord met gestelde eisen rondom het verantwoord gebruik van het bedrijfsmiddel voorafgaand aan ingebruikname.

4.4 Monitoren van bedrijfsmiddelen

De volgende bepalingen zijn van toepassing:

1. Per bedrijfsmiddel is een evaluatiecyclus vastgesteld.
2. Per evaluatiecyclus wordt opnieuw vastgesteld of:
   a. De omschrijving van het bedrijfsmiddel nog van toepassing is
   b. De toegewezen categorieën van verwerkte niet-publieke informatie en toegang tot informatiesystemen nog van toepassing zijn
   c. De vereiste informatiebeveiligingsmaatregelen nog actief en effectief zijn
3. Op elk bedrijfsmiddel zijn monitoringsmechanismen actief die proportioneel zijn tot:
   a. Risico's gerelateerd aan misbruik, diefstal of verlies
   b. Verwerkte niet-publieke informatie
   c. Toegang tot informatiesystemen
4. Monitoringsmechanismen kunnen bestaan uit:
   a. Proactieve real-time monitoring van activiteiten; of
   b. Reactieve monitoring door analyse van logs

4.5 Deactiveren van bedrijfsmiddelen

De volgende bepalingen zijn van toepassing:

1. Deactiveren van een bedrijfsmiddel vindt plaats nadat:
    a. Het bedrijfsmiddel tijdelijk of permanent geen actieve gebruiker heeft
    b. De licentie voor gebruik is verlopen of ingetrokken
    c. Het bedrijfsmiddel is opgegeven als vermist of gestolen
2. Het deactiveren van een bedrijfsmiddel zorgt ervoor dat deze niet langer toegang heeft tot:
    a. Niet-publieke informatie
    b. (Andere) informatiesystemen
3. Voor elk gedeactiveerd bedrijfsmiddel is vastgelegd:
    a. Wanneer deze is gedeactiveerd
    b. Voormalige eigenaren
4. Een gedeactiveerd bedrijfsmiddel heeft de status ‘inactief’
5. Bij fysieke bedrijfsmiddelen:
    a. Het wissen van opgeslagen informatie volgens een industrieconforme methode
    b. Het terugzetten naar standaard fabrieksinstellingen

4.6 Verwijderen van bedrijfsmiddelen

De volgende bepalingen zijn van toepassing:

1. Het verwijderen van een bedrijfsmiddel vindt plaats zodra:
    a. Deze tijdelijk of permanent gedeactiveerd is
    b. Hiertoe wordt besloten door de CISO of het Hoofd Operations
    c. Het bedrijfsmiddel bij verder gebruik een onaanvaardbaar risico met zich meebrengt
    d. Het bedrijfsmiddel end-of-life en/of end-of-support heeft bereikt waardoor het niet langer van beveiligingsupdates wordt voorzien
    e. Het bedrijfsmiddel defect is en niet te herstellen is
2. Het verwijderen van een bedrijfsmiddel bestaat uit:
    a. Intrekken van permissies voor toegang tot niet-publieke informatie en informatiesystemen
    b. Permanent verwijderen van de opgeslagen data volgens een industrieconforme methode
    c. Bij extern beheerde bedrijfsmiddelen:
        i. Een leverancier contractueel verplichten tot het permanent verwijderen van de opgeslagen data volgens een industrieconforme methode
        ii. Ontvangen bevestiging geslaagde permanente verwijdering van leverancier
    d. Bij fysieke bedrijfsmiddelen:
        i. Vernietigen van informatiedragende componenten door een gecertificeerde externe organisatie volgens een industrieconforme methode
3. Voor elk verwijderd bedrijfsmiddel is vastgelegd wanneer deze is verwijderd, inclusief bijbehorend bewijs.

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