Beleid voor acquisitie, ontwikkeling en onderhoud van informatiesystemen

Informatiebeveiliging

document	
identificatie	OU Beleid voor acquisitie, ontwikkeling en onderhoud van informatiesystemen
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	29-06-2022	Initiële versie T. Timmermans (ON2IT)	
0.2.0	MR1	11-07-2022	Review en aanpassingen door MR1	TT2
0.3.0	CKO	08-08-2022	Review door CKO	
0.4.0	MR1	17-08-2022	Verwerken opmerkingen en suggesties CKO	TT2
0.4.1	TT2	01-09-2022	Bijwerken structuur en opmaak	
0.5.0	MR1	14-09-2022	Verwerken opmerkingen en suggesties HIL	TT2
0.6.0	JAE	19-09-2022	Review door JAE	
0.7.0	MR1	22-09-2022	Verwerken opmerkingen en suggesties JAE	TT2
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 3
2. Doelgroep 3
3. Definities 3
4. Beleidsbepalingen 3
   4.1 Eisen voor veilige informatiesystemen 3
   4.2 Acquisitie van informatiesystemen 3
   4.3 Ontwikkelen van informatiesystemen 4
   4.4 Onderhouden van informatiesystemen 4
   4.5 Ontmantelen van informatiesystemen 5
5. Context 5
6. Naleving 5
7. Uitzonderingen 5
8. Wijzigingen 5
Bijlage 1: Structurele uitzonderingen op dit beleid 6

1. Doel

Dit beleid heeft betrekking op het vastleggen van beleidsbepalingen omtrent de acquisitie, ontwikkeling en onderhoud van informatiesystemen, 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 Eisen voor veilige informatiesystemen

De volgende bepalingen zijn van toepassing:

1. Er zijn eisen omtrent informatiebeveiliging opgesteld in een standaard voor veilige informatiesystemen die gelden voor:
    a. Aanschaf van informatiesystemen
    b. Ontwikkeling van informatiesystemen
    c. Uitbreiding van informatiesystemen
2. De eisen voor informatiesystemen zijn opgesteld op basis van:
    a. Beschikbaarheid van informatie
    b. Integriteit van informatie
    c. Vertrouwelijkheid van informatie
    d. Rol in kritieke bedrijfsprocessen
3. De eisen omtrent informatiebeveiliging gelden voor informatiesystemen:
    a. In eigen beheer
    b. In beheer door een derde partij

4.2 Acquisitie van informatiesystemen

De volgende bepalingen zijn van toepassing:

1. Als onderdeel van het selectieproces voor een informatiesysteem wordt getoetst op de eisen voor informatiesystemen zoals benoemd in de standaard waarnaar wordt verwezen in 4.1.
2. Indien er aan één of meerdere eisen niet wordt voldaan, moet dit worden geaccepteerd door de systeemeigenaar. Uitzonderingen moeten worden beoordeeld en vastgelegd zoals beschreven in hoofdstuk 7 van dit document.

4.3 Ontwikkelen van informatiesystemen

De volgende bepalingen zijn van toepassing:

1. Regels en richtlijnen over veilige systeemontwikkeling zijn vastgesteld in een standaard en worden toegepast in de gehele levenscyclus die bestaat uit de volgende fases:
    a. Planning
    b. Analyse
    c. Ontwerp
    d. Implementatie
    e. Testen en integratie
    f. Onderhoud
    g. Ontmantelen
2. Formele procedures voor het beheren van wijzigingen in systeemontwikkeling zijn vastgesteld en worden toegepast.
3. Bij veranderingen in systeemcomponenten worden kritische applicaties getest om te beoordelen of er geen nadelige impact is op informatiebeveiliging en bedrijfsactiviteiten.
4. Er is een afgeschermde omgeving voor systeemontwikkeling die los staat van de productieomgeving.
5. Er is een afgeschermde omgeving voor het uitvoeren van systeemacceptatietests die los staat van de productieomgeving.
6. Voor niet-productieomgevingen wordt gebruik gemaakt van:
    a. Willekeurige ‘dummy’ testgegevens welke geen productiegegevens bevatten; of
    b. Productiegegevens waarbij dezelfde beveiligingsmaatregelen en toegangsbeperkingen van toepassing zijn als voor de productieomgeving
7. Voorafgaand aan uitbestede systeemontwikkeling wordt gecontroleerd of de externe partij de eisen voor veilige systemen hanteert zoals benoemd in de standaard onder 4.1.
8. Bij uitbestede systeemontwikkeling wordt periodiek gevalideerd of de secure software development lifecycle (SDLC) wordt toegepast.
9. Bij het beëindigen of stoppen van uitbestede systeemontwikkeling wordt alle informatie die nodig is voor het voortzetten van onderhoud en systeemontwikkeling overgedragen aan:
    a. De OU; of
    b. Een andere door de OU ingeschakelde externe partij
10. Bij het beëindigen of stoppen van uitbestede systeemontwikkeling worden alle gegevens vernietigd indien de OU hier opdracht toe geeft.

4.4 Onderhouden van informatiesystemen

De volgende bepalingen zijn van toepassing:

1. Elk informatiesysteem en ondersteunende systeemcomponenten worden periodiek voorzien van onderhoud zodat het informatiesysteem:
    a. Adequaat kan blijven functioneren
    b. Wordt voorzien van beveiligingsupdates die kwetsbaarheden verhelpen
2. De mate van onderhoud aan een informatiesysteem is proportioneel tot de classificatie van informatie en de bijbehorende risico’s.
3. Er wordt periodiek gemonitord op de beschikbaarheid van beveiligingsupdates.
4. Beveiligingsupdates worden waar mogelijk en indien van toepassing:
    a. Automatisch geïnstalleerd
    b. Afgedwongen op beheerde bedrijfsmiddelen
    Bijvoorbeeld: het activeren van mobile device management (o.a. Microsoft Intune) op laptops.
5. Beveiligingsupdates worden geprioriteerd op basis van:
    a. Potentiële impact van kwetsbaarheden
    b. Kans op exploitatie van kwetsbaarheden
    c. Toepasselijkheid van kwetsbaarheden binnen de omgeving en configuratie

4.5 Ontmantelen van informatiesystemen

De volgende bepalingen zijn van toepassing:

1. Bij een te ontmantelen informatiesysteem wordt alle opgeslagen informatie:
    a. Overgezet naar een ander informatiesysteem
    b. Gearchiveerd conform geldende wet- en regelgeving
    c. Permanent verwijderd volgens een industrieconforme methode
2. Bij een te ontmantelen informatiesysteem worden alle permissies en koppelingen met andere informatiesystemen verwijderd of gedeactiveerd.
3. Een te ontmantelen informatiesysteem wordt permanent verwijderd van de locatie(s) waar deze is geïnstalleerd of opgeslagen.

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