Beleid voor gebruik van cryptografie

Informatiebeveiliging

document	
identificatie	OU Beleid voor gebruik van cryptografie
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	04-05-2022	Initiële versie	
0.2.0	MR1	04-05-2022	Review door MR1	TT2
0.3.0	MR1	19-05-2022	Tekst in de OU template voor beleidsdocumenten gezet	CKO, HIL
0.4.0	CKO	23-05-2022	Review door CKO	
0.5.0	HIL	01-06-2022	Review door HIL	
0.6.0	MR1	09-06-2022	Verwerken opmerkingen en suggestie CKO en HIL	TT2
0.6.1	TT2	12-08-2022	Bijwerken structuur en opmaak	
0.7.0	JAE	19-09-2022	Review door JAE	
0.8.0	TT2	28-09-2022	Verwerken opmerkingen JAE	MR1
0.8.1	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 encryptie en decryptie van data, 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 Encryptie van data at rest

De volgende bepalingen zijn van toepassing:

1. Encryptie van data at rest is vereist voor het opslaan van niet-publieke informatie, volgens de classificaties zoals omschreven in het *Informatiebeveiligingsbeleid*.
2. Hardwarematige encryptie van data at rest is vereist voor niet-publieke informatie die zich bevindt op een geïntegreerde of externe harde schijf
3. Softwarematige encryptie van data at rest is vereist voor niet-publieke informatie die zich bevindt:
    a. In een bestand
    b. In een database
4. Er wordt gebruik gemaakt van door de OU goedgekeurde algoritmen zoals vastgelegd in de *Standaard voor gebruik van cryptografie* voor:
    a. Applicaties die worden beheerd door de OU
    b. Applicaties die worden beheerd door een derde partij die door de OU is erkend als leverancier van een informatiesysteem
5. Er vindt periodieke controle plaats om te verifiëren dat encryptie van data at rest is toegepast voor niet-publieke informatie en bijbehorende informatiesystemen.

4.2 Encryptie van data in transit

De volgende bepalingen zijn van toepassing:

1. Encryptie van data in transit is vereist voor het uitwisselen van niet-publieke informatie tussen systemen, volgens de classificaties zoals omschreven in het *Informatiebeveiligingsbeleid*.
2. Encryptie van data in transit vindt plaats door middel van:
    a. Encryptie van lokaal netwerkverkeer
    b. Encryptie van internetverkeer
3. Er wordt gebruik gemaakt van door de OU goedgekeurde algoritmen zoals vastgelegd in de *Standaard voor gebruik van cryptografie* voor:

   a. Applicaties die worden beheerd door de OU
   b. Applicaties die worden beheerd door een derde partij die door de OU is erkend als leverancier van een informatiesysteem
4. Er vindt periodieke controle plaats om te verifiëren dat encryptie van data in transit is toegepast voor niet-publieke informatie en bijbehorende informatiesystemen.

4.3 Decryptie van data

De volgende bepalingen zijn van toepassing:

1. Decryptie van data vereist het gebruik van een geldige cryptografische sleutel.
2. Decryptie van data is toegestaan voor:
   a. Het gebruik van data door eindgebruiker(s)
   b. Het inspecteren van data(stromen) voor beveiligingsdoeleinden
   c. Het inspecteren van data(stromen) in overeenstemming met wettelijke verplichtingen

4.4 Cryptografische sleutels

De volgende bepalingen zijn van toepassing:

1. Cryptografische sleutels worden gegenereerd, opgeslagen en beheerd in een beveiligde omgeving.
2. Cryptografische sleutels worden periodiek ververst.
3. Toegang tot de opslag van cryptografische sleutels is strikt beperkt tot geautoriseerde individuen.
4. Activiteiten worden vastgelegd door middel van logs in het geval van:
   a. Opvragen of cryptografische sleutels
   b. Wijzigen van cryptografische sleutels
   c. Verwijderen van cryptografische sleutels
5. Gegenereerde logs worden:
   a. Niet-manipuleerbaar opgeslagen
   b. Minimaal bewaard voor een vooraf vastgestelde periode

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