Beleid voor communicatiebeveiliging

Informatiebeveiliging

document	
identificatie	OU Beleid voor communicatiebeveiliging
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	23-04-2022	Initiële versie	
0.2.0	TT2	25-04-2022	Review MR1 en TT2	
0.3.0	CKO	16-06-2022	Review CKO	
0.4.0	HIL	16-06-2022	Review HIL	
0.5.0	TT2	16-06-2022	Verwerken opmerkingen en suggesties CKO en HIL	MR1
0.5.1	TT2	01-09-2022	Bijwerken structuur en opmaak	
0.5.2	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 het beveiligen van systeem- en netwerkcommunicatie, 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 Beheer van netwerken

De volgende bepalingen zijn van toepassing:

1. Er is een actueel overzicht van netwerken die worden beheerd door de OU.
2. Elk netwerk heeft een eindverantwoordelijke.
3. Elk netwerk heeft een beheerder die verantwoordelijk is voor het beheer van het netwerk en onderhouden van documentatie hiervan.
4. Netwerkverkeer wordt geïnspecteerd voor het kunnen:
    a. Toestaan van het verkeer
    b. Blokkeren van het verkeer
5. Verdacht netwerkverkeer kan na inspectie mogelijk worden gemarkeerd voor nadere inspectie.

4.2 Segmenteren en beveiligen van netwerken

De volgende bepalingen zijn van toepassing:

1. Elk netwerk is opgedeeld in fysieke of virtuele microperimeters op basis van functionele processen.
2. Voor elke microperimeter wordt inkomend en uitgaand verkeer standaard geblokkeerd.
3. Voor elke microperimeter is inkomend en uitgaand verkeer enkel toegestaan waarvoor is vastgelegd volgens de Kipling-methode:
    a. Wie heeft toegang nodig
    b. Wat is de bestemming van het verkeer
    c. Waar moet toegang worden toegestaan
    d. Wanneer is toegang toegestaan
    e. Waarom is toegang vereist
    f. Hoe kan toegang worden verkregen
4. Voor elke microperimeter is inkomend en uitgaand verkeer enkel toegestaan na expliciete verificatie door inspectie van het verkeer.

5. Verkeer tussen microperimeters op hetzelfde netwerk:
    a. Wordt beschouwd als zijnde communicatie afkomstig vanuit een extern of onbekend netwerk
    b. Is standaard geblokkeerd
    c. Is enkel toegestaan na expliciete verificatie door inspectie van het verkeer
6. Een door de OU beheerd netwerk bevat niet inherent meer permissies dan een extern, niet door de OU beheerd netwerk.
7. Inkomend en uitgaand verkeer van microperimeters wordt gelogd en weggeschreven naar een read-only omgeving.
8. Logs van inkomend en uitgaand verkeer van microperimeters wordt geïnspecteerd op afwijkend of niet-toegestaan gedrag.
9. Encryptie van data in transit is vereist voor het uitwisselen van informatie tussen informatiesystemen op het netwerk, volgens het *Beleid voor gebruik van cryptografie*.
10. Er vindt periodieke controle plaats om te verifiëren dat:
    a. Het overzicht met alle door de OU beheerde netwerken actueel is
    b. Alle door de OU beheerde netwerken de vereiste beveiligingsmaatregelen hebben geïmplementeerd
11. Elk draadloos netwerk:
    a. Heeft beperkingen in het gebruik van het draadloos netwerk:
        i. Gedefinieerd
        ii. Technisch afgedwongen
    b. Vereist expliciet authenticatie voor aan het verschaffen van toegang tot het draadloos netwerk
    c. Vereist voor het verschaffen van toegang tot het netwerk expliciet autorisatie van:
        i. Accounts, individueel of in groepen
        ii. Gebruikers, individueel of in groepen
        iii. Mobiele apparaten, individueel of in groepen
    d. Bevat mechanismen voor het detecteren van mogelijk ongeauthoriseerde activiteiten
    e. Ondersteunt conform het document *Beleid voor gebruik van cryptografie*:
        i. Versleuteling van netwerkverkeer
        ii. Versleuteling van verbonden apparaten
    f. Is geconfigureerd en geïmplementeerd als separaat netwerksegment

4.3 Uitwisselen van informatie

De volgende bepalingen zijn van toepassing:

1. Het uitwisselen van informatie is onderhevig aan door de OU vastgestelde informatiebeveiligingseisen, ongeacht de vorm van uitwisseling (zoals mondeling, digitaal of op papier).
2. Het uitwisselen van niet-publieke informatie tussen partijen vindt plaats op basis van:
    a. De vereisten per classificatieniveau zoals vastgelegd in het *Informatiebeveiligingsbeleid*
    b. Het ‘need-to-know’ principe, waarbij niet meer informatie wordt uitgewisseld dan noodzakelijk wordt geacht door de verstrekker
    c. De vereisten voor het gebruik van encryptie zoals vastgelegd in het *Beleid voor gebruik van cryptografie*
    d. Het verifiëren van de ontvangende partij door de verzendende partij voorafgaand aan het verstrekken van de informatie
3. Eenieder dient melding te maken bij de ITF Servicedesk indien er verdenkingen of aanwijzingen zijn dat:
    a. Er sprake is van ongeautoriseerd uitwisselen van niet-publieke informatie
    b. De informatie verloren is gegaan tijdens het uitwisselen
    c. De informatie is gelekt naar ongeautoriseerde partijen tijdens het uitwisselen
4. Er zijn contractuele afspraken gemaakt over het uitwisselen van niet-publieke informatie met:
    a. Medewerkers
    b. Studenten en klanten
    c. Leveranciers
    d. Andere partijen waarmee niet-publieke informatie uitgewisseld gaat worden

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