Beleid voor logische toegangsbeveiliging

Informatiebeveiliging

document	
identificatie	OU Beleid voor logische toegangsbeveiliging
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
0.1.1	TT2	27-05-2022	Initiële versie TT2	
0.2.1	MR1	11-05-2022	Feedback verwerkt en in Word beleidstemplate gezet	
0.3.0	CKO	03-05-2022	Review door CKO afgerond	
0.4.0	HIL	02-05-2022	Review door HIL afgerond	
0.5.0	MR1	19-05-2022	Tim en Martin samen nogmaals doorgelopen en bijgewerkt	TT2
0.5.1	MR1	23-05-2022	Reviewdata CKO en HIL in wijzigingshistorie toegevoegd	
0.5.2	MR1	25-05-2022	Feedback van CKO op accountcategorieën (par 4.1.2) verwerkt	
0.6.0	MR1	02-06-2022	Verwerken opmerkingen CKO en HIL	TT2
0.7.0	MR1	02-08-2022	Verwerken opmerkingen en voorgestelde wijzigingen RVB	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 review 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 implementeren van logische toegangsbeveiligingsmaatregelen en toegangscontroles, 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.

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 Identificeren van accounts

De volgende bepalingen zijn van toepassing:

1. Er is een periodiek bijgewerkt overzicht van:
    a. Alle geregistreerde accounts binnen de informatiesystemen
    b. De status per account [actief/niet actief (*disabled*)]
    c. De gebruiker(s) per account
    d. De eindverantwoordelijke voor een account
        i. Enkele gebruiker: de persoon zelf
        ii. Meerdere gebruikers: de voogd
    e. De permissies per account
2. Elk account valt onder 1 van de volgende categorieën:
    a. Algemeen account
    b. Named account – standaard gebruikersaccount
    c. Beheeraccount – geprivilegieerd account
    d. Serviceaccount/Systeemaccount – voor (geautomatiseerd) uitvoeren van processen zonder gebruikersinterface
    e. Noodaccount – enkel voor gebruik in noodsituaties

4.2 Aanmaken van een account

De volgende bepalingen zijn van toepassing:

1. Een account wordt enkel aangemaakt wanneer dit noodzakelijk is voor:
    a. Het functioneren van informatiesystemen; of
    b. De uitvoering van bedrijfsprocessen
2. Elk account valt onder ten minste 1 van de volgende categorieën gebruikers:
    a. Persoonlijk account: een account dat aan één gebruiker wordt uitgegeven. De Open Universiteit onderscheidt twee typen:
        i. Intern persoonlijk account: een account dat aan één medewerker wordt uitgegeven.

ii. Extern persoonlijk account: een account dat aan één externe gebruiker wordt uitgegeven. Dit betreft voornamelijk een:
    - Leverancier; of
    - Medewerker niet in loondienst (inhuur, uitzendkracht etc.).

b. Gedeeld account: een gedeeld account is een account waarbij meer dan één persoon het wachtwoord kent en/of hetzelfde verificatietoken gebruikt. Het gebruik van gedeelde accounts is alleen toegestaan als er een systeem- of bedrijfsbeperking is die het gebruik van afzonderlijke accounts verhindert. Ieder gedeeld account heeft een voogd: een medewerker die verantwoordelijk is voor het account.
c. Beheeraccount: accounts die aan een gebruiker worden gegeven en die het recht bieden om het besturingssysteem of de platforminstellingen te wijzigen, of accounts die wijzigingen in andere accounts mogelijk maken. Doorgaans een account dat meer toegang biedt en extra autorisatie vereist.
d. Ingebouwd beheeraccount: standaard geprivilegieerde accounts (bijv. root, administrator) zijn verbonden aan een bepaald systeem en kunnen niet worden verwijderd zonder de functionaliteit van het systeem te beïnvloeden. Doorgaans een account dat meer toegang biedt en extra autorisatie vereist.
e. Serviceaccount: Een serviceaccount wordt verstrekt voor een proces of applicatie. Het wordt gebruikt voor het uitvoeren van taken en diensten zonder gebruikersinteractie.
f. Gastaccount: account voor mensen die geen individueel account van de OU hebben. De reguliere term is gastaccount.
   Bijvoorbeeld: een eduroam account dat gevalideerd is door een collega-instelling.
g. Break glass account: Noodaccounts zijn bedoeld voor gebruik in een crisissituatie en kunnen alleen onder strikte voorwaarden en door het volgen van vooraf vastgestelde procedures worden aangemaakt en gebruikt. Ingebruikname van het account vindt plaats volgens een specifiek hiervoor ingestelde procedure. Noodaccounts moeten 24 uur na ingebruikname automatisch worden uitgeschakeld.
h. Tijdelijk account: Tijdelijke accounts zijn bedoeld voor kortdurend gebruik, kunnen alleen onder strikte voorwaarden worden aangemaakt en gebruikt en hebben een begin- en einddatum. Denk aan een incidenteel account voor een accountant, onderhoudsmonteur of eenmalige presentator. Deze accounts hebben strikt beperkte autorisaties en geven alleen toegang tot de noodzakelijk systemen.

3. Elk account heeft een noodzaak welke het bestaan legitimeert
4. Elk account heeft één eindverantwoordelijke, in de vorm van een eigenaar of voogd

4.3 Toewijzen van permissies aan een account

De volgende bepalingen zijn van toepassing:

1. Het principe van minste bevoegdheden wordt toegepast, waarbij elk account enkel permissies heeft die noodzakelijk zijn voor het uitvoeren van de toegewezen taken
2. Er vindt periodieke controle plaats op correcte implementatie van het principe van minste bevoegdheden
3. Het gebruik van geprivilegieerde accounts is beperkt tot een minimum
4. Een niet-geprivilegieerde gebruiker kan geen geprivilegieerde taken uitvoeren in informatiesystemen

4.4 Gebruiken van een account

De volgende bepalingen zijn van toepassing:

1. Elke natuurlijke persoon ondergaat verificatie van identiteit voorafgaand aan ingebruikname van een account
2. Elke gebruiker van een actief account is akkoord met de voorwaarden zoals vastgelegd in het *Reglement computergebruik medewerkers Open Universiteit*

4.5 Controleren en monitoren van een account

De volgende bepalingen zijn van toepassing:

1. Activiteiten van een account worden gelogd voor zover:
    a. Dit technisch mogelijk is in systemen
    b. Wordt voldaan aan wet- en regelgeving
2. Er vindt periodieke controle plaats op de toegekende permissies voor geprivilegieerde accounts
3. Beheerders worden op hoogte gesteld van gedetecteerde afwijkingen in permissies
4. Beheerders ondernemen adequaat en spoedig acties op gedetecteerde afwijkingen

4.6 Deactiveren van een account

De volgende bepalingen zijn van toepassing:

1. Een account wordt gedeactiveerd zodra:
    a. Dit niet langer noodzakelijk is voor het functioneren van informatiesystemen
    b. Dit niet langer noodzakelijk is voor de uitvoering van bedrijfsprocessen
    c. De gebruiker niet langer in dienst is
    d. De gebruiker niet langer geïdentificeerd kan worden of onherleidbaar is
    e. De gebruiker niet langer betrokken is bij de (processen van de) Open Universiteit
    f. Er sprake is van langdurige inactiviteit
    g. De voogd aangeeft dat een account niet langer nodig is
    h. Er (vermoedelijk) sprake is van misbruik, fraude of oneigenlijk gebruik
    i. Besloten is door het College van Bestuur
    j. Besloten is door individuen of instanties zoals bevoegd door het College van Bestuur

4.7 Verwijderen van een account

De volgende bepalingen zijn van toepassing:

1. Een account wordt permanent verwijderd zodra:
    a. Het is gedeactiveerd en er geen zicht is op heractiveren
    b. Verplicht door wet-en regelgeving
    c. Bevolen door wettelijk bevoegde instanties

4.8 Verantwoordelijkheden in accountbeheer

De volgende bepalingen zijn van toepassing:

1. Het principe van scheiding van taken wordt toegepast: mogelijk conflicterende taken in het beheren van accounts worden uitgevoerd als gescheiden activiteiten om misbruik of kwaadaardige acties te voorkomen
   Bijvoorbeeld: een beheerder moet zichzelf of anderen niet ongezien en ongeautoriseerd extra rechten kunnen toekennen of in staat zijn om logs van eigen activiteiten te verwijderen of wijzigen.
2. De aanwezige scheiding van taken is:
    a. Gedefinieerd
    b. Technisch afgedwongen in mechanismen van informatiesystemen, voor zover technisch mogelijk
    c. Procesmatig afgedwongen in de uitvoering van bedrijfsprocessen

4.9 Toegang tot informatiesystemen

De volgende bepalingen zijn van toepassing:

Elk informatiesysteem met (toegang tot) niet-publieke informatie:

1. Vereist expliciete en geldige autorisatie voorafgaand aan het verschaffen van toegang
2. Maakt gebruik van gestandaardiseerde of geautomatiseerde mechanismen voor autorisatie, voor zover ondersteund
3. Maakt gebruikt van logging voor het vastleggen van succesvolle en gefaalde autorisatie, voor zover ondersteund
4. Dwingt een limiet af van opeenvolgende ongeldige aanmeldingspogingen door een gebruiker binnen een vastgestelde periode
5. Dwingt toegang af door middel van een versleutelde verbinding
6. Vergrendelt automatisch toegang van account zodra deze het limiet van opeenvolgende ongeldige aanmeldpogingen bereikt
7. Ontgrendelt toegang van vergrendeld account:
    a. automatisch na een vastgestelde periode
    b. handmatig door een actie vanuit een beheeraccount
8. Beeindigt automatisch een gebruikerssessie na een vastgestelde periode, waarna nieuwe autorisatie vereist is
9. Staat voor niet (volledig) geautoriseerde gebruikers of accounts:
    a. Geen gebruik toe
    b. Slechts zeer beperkt gebruik toe, waarbij documentatie aanwezig is die dit beschrijft en deze keuze verantwoordt

Aanvullend van toepassing voor elk door de organisatie beheerd apparaat met (toegang tot) niet-publieke informatie:

1. Bevat een unieke fysieke en digitale identificatiekenmerk welke niet kan worden gewijzigd of gemanipuleerd
2. Bevat een vergrendelingsmechanisme dat niet kan worden uitgeschakeld-
3. Kan enkel worden gebruikt indien ontgrendeld door de expliciet toegewezen gebruiker(s) en account(s)
4. Is geregistreerd conform het document *Beleid voor beheer van bedrijfsmiddelen*
5. Heeft conform het document *Beleid voor gebruik van cryptografie* geïmplementeerd:
    a. Versleuteling van netwerkverkeer
    b. Versleuteling van volledige lokale opslag
6. Vereist authenticatie conform het document *Standaard voor authenticatiemechanismen*
7. Beperkt strikt het gebruik van lokale beheerdersrechten en -privileges

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